

PARTNERS

INFORMAZIONE E FORMAZIONE PER IL CANALE A VALORE



Innovare i servizi per rimanere competitivi

INCHIESTA

MARKET REVIEW

PROTEZIONE
DEGLI ENDPOINT:
EDR, XDR, MDR



LE SOLUZIONI
DEL MERCATO

FOCUS IT-OT: L'INTEGRAZIONE CHE GUIDA L'INDUSTRIA 4.0

CANALE

- ▶ I MANAGED PRINT SERVICES SECONDO BROTHER
- ▶ C.I.E. UNIFICA LA RETE E LA GESTISCE DAL CLOUD

SICUREZZA

- ▶ OPENTEXT: CONTRASTARE IL RANSOMWARE CON LA CYBER RESILIENZA
- ▶ WATCHGUARD: L'XDR PER AFFRONTARE LA SICUREZZA

SOMMARIO

GENNAIO 2024 • N. 60

EDITORIALE

I 10 trend per il 2024 nell'ICT B2B

INCHIESTA

Servizi Ict, AI e Cloud il motore per il 2024

14. CANALE

I managed print services secondo Brother

C.I.E. unifica la rete e la gestisce dal cloud

19. INTERVISTA

Achab: le infrastrutture ICT nelle PMI italiane: sfide e soluzioni

22. CYBERSECURITY

La cybertempesta perfetta: visioni della sicurezza nel 2024

OpenText: contrastare il ransomware con la cyber resilienza

WatchGuard: la potenza dell'XDR per affrontare le nuove sfide di sicurezza

36. INTERVISTA

Vectra AI: sconfiggere i falsi positivi senza andare in cloud



39. FOCUS TECNOLOGIE

IT-OT: l'integrazione che guida l'industria 4.0

45. MARKET REVIEW

Soluzioni per la protezione degli endpoint: EDR, XDR, MDR

Le soluzioni del mercato

PARTNERS

Anno XI - numero 60
Gennaio 2024

Direttore responsabile: Riccardo Florio

In redazione: Riccardo Florio, Paola Rosa

Grafica: Paola Rosa

Hanno collaborato: Maurizio Ferrari, Stefano Uberti Foppa, Fabrizio Pincelli, Mercedes Oledieu, Leo Sorge

Redazione:

REPORTEC srl | Via Gorizia 35/37
20099 Sesto San Giovanni (MI);
Tel 02 24304434 | www.reportec.it |
redazione@reportec.it

Editore:

Reportec Srl, C.so Italia 50 | 20122 Milano

Diffusione: 35.000 copie digitali

Iscrizione al tribunale di Milano n° 515 del 13 ottobre 2011.

Immagini: Dreamstime.com

Proprietà: Reportec Srl, C.so Italia 50, 20122 Milano

Tutti i diritti sono riservati

Tutti i marchi sono registrati e di proprietà delle relative società

Reportec è una società fondata da:
Gaetano Di Blasio, Riccardo Florio, Giuseppe Saccardi



RICCARDO FLORIO
DIRETTORE RESPONSABILE

I 10 trend per il 2024 nell'ICT B2B

Il 2024 è da poco iniziato ed è già possibile individuare i trend che caratterizzeranno l'ICT B2B nel 2024. In un periodo definito dall'innovazione e dall'efficienza, il cloud e l'Intelligenza artificiale emergono come protagonisti in un contesto di ridotta spesa dei consumatori e crescenti preoccupazioni per la recessione. Le imprese, quindi, si stanno orientando verso un aumento degli investimenti in tecnologie digitali.

Vediamo più in dettaglio i dieci trend chiave.

- 1. L'ascesa del cloud computing e dell'AI** - Il 2024 vedrà un'accelerazione nell'adozione del cloud computing e dell'intelligenza artificiale. Le imprese si stanno orientando verso queste tecnologie per sfruttare la loro flessibilità, scalabilità e potenzialità di analisi dei dati. A fronte della volontà di agire in molti cercheranno all'esterno qualcuno che gli suggerisca cosa fare.
- 2. Strategie in evoluzione** - Le aziende devono essere pronte a rispondere rapidamente alle fluttuazioni del mercato e alle tendenze emergenti. È fondamentale concentrarsi su strategie che ottimizzino le risorse e riducano i costi operativi, come l'adozione di modelli "cloud first" per rimanere agili e resilienti in un panorama economico in continuo cambiamento.



3. **Resilienza e cybersecurity** - La sicurezza diventerà una priorità ancora più critica nel 2024, soprattutto con l'aumento del lavoro remoto e della dipendenza dalle tecnologie digitali. Anche l'AI generativa rappresenta un tema che apre verso nuovi rischi e che a più ampio termine richiederà di rivedere i modelli di detection and response. È importante anche che le aziende si assicurino che le loro soluzioni cloud siano dotate di robusti meccanismi di sicurezza per proteggere dati sensibili e rafforzare la fiducia dei clienti.
4. **Migliorare la comprensione del cliente** - In un mercato in rapida evoluzione, comprendere le esigenze e le aspettative del cliente diventa fondamentale. Questo richiede un'analisi approfondita dei dati per creare profili cliente dettagliati, che aiutino a personalizzare l'offerta e migliorare l'efficacia delle strategie di marketing.
5. **Comunicazione efficace nel mercato ICT B2B** - Nel 2024, i contenuti di marketing dovranno essere curati con attenzione per parlare direttamente ai clienti IT. È importante che le informazioni tecniche siano bilanciate con messaggi chiari e accessibili, in modo da coinvolgere un pubblico ampio e diversificato, che vada oltre i soli professionisti IT.
6. **Engagement omnicanale** - L'importanza di una strategia di marketing omnicanale continua a crescere. Raggiungere i clienti ovunque si trovino, su diverse piattaforme digitali è essenziale per un engagement efficace e la personalizzazione dei contenuti per ciascun canale assicura un'esperienza coerente e coinvolgente per il cliente.



7. **Ritorno degli eventi in presenza** - Il 2024 vedrà un ulteriore ritorno agli eventi in presenza, che rappresentano un'opportunità unica di networking e di stabilire connessioni personali e presentare soluzioni innovative.
8. **Formazione e aggiornamento professionale** - Con l'evoluzione continua delle tecnologie, la formazione continua del personale è essenziale. Gli investimenti nella formazione garantiscono che il personale sia aggiornato sulle ultime tecnologie e pratiche del settore, contribuendo a migliorare l'efficienza interna e a fornire un servizio clienti più informato e competente.
9. **Collaborazioni e partnership** - Nel 2024, la collaborazione e la creazione di partnership strategiche saranno cruciali. Lavorare insieme a diverse aziende può aprire nuove opportunità di mercato e stimolare l'innovazione perché le collaborazioni possono portare a soluzioni più efficaci e a una maggiore penetrazione del mercato.
10. **Verso un futuro sostenibile** - La responsabilità ambientale diventa un fattore sempre più importante. Le imprese B2B ICT devono considerare l'impatto ambientale delle loro operazioni e prodotti e investire in tecnologie sostenibili. Questo migliora anche l'immagine aziendale e ne rafforza la posizione sul mercato.



Servizi Ict, Ai e Cloud il motore per il 2024

L'anno appena iniziato sarà quello della consacrazione dell'Intelligenza Artificiale, ma anche quello della mancanza di competenze. I principali attori del mercato tracciano il loro percorso

di Maurizio Ferrari

L'anno che verrà è il titolo di una famosa canzone di Lucio Dalla, in una strofa afferma "...che il nuovo anno porterà una trasformazione e tutti quanti stiamo già aspettando...". Trasformazione che gli operatori del canale stanno facendo; trasformazione che porta il nome di Intelligenza Artificiale, di cybersecurity, di risposta alla carenza di competenze, di capacità di muoversi tra il mondo virtuale dell'iperconvergenza e quello on premise, di gestire il variegato mondo dell'Internet of Things e del cloud in tutte le sue declinazioni. A livello europeo, secondo una ricerca Context, nel 2024 le vendite IT at-

traverso il canale dovrebbero tornare a crescere del 2,6% su base annua dopo un difficile 2023 che ha pagato la spinta "drogata" dal Covid agli investimenti ICT degli scorsi anni.

Gli analisti di Context hanno approfondito le principali tendenze del mercato e i dati di vendita degli ultimi trimestri e secondo il loro lavoro il fatturato per il 2024 sarà compreso tra -0,5% e 6,5% (il 2,6% è la previsione centrale), in crescita rispetto al -6% previsto per il 2023.

Secondo Context saranno diversi i fattori che favorirebbero una migliore performance nel 2024, tra

questi nuovi prodotti e casi d'uso basati sull'Intelligenza Artificiale, oltre a un ciclo di aggiornamento dei prodotti e servizi ritardato nell'anno precedente.

Molto dipenderà però dal quadro macroeconomico che si verrà a creare nei primi mesi dell'anno e dalla capacità delle condizioni economiche di stimolare la domanda dei consumatori e gli investimenti delle imprese. *«Il 2023 è stato un anno di correzione dopo la crescita alimentata da Covid degli ultimi anni – ha dichiarato Adam Simon, Ceo di Context –. È stato un anno difficile per la distribuzione e per tutto il settore ICT, in quanto le aziende hanno perso la fiducia negli investimenti. Tuttavia, c'è una luce alla fine del tunnel. Il secondo trimestre del 2024 sarà il trimestre della svolta. Prevediamo che i tassi di crescita del volume e del valore convergeranno, per poi continuare nella seconda metà dell'anno, aiutati da confronti positivi su base annua».*

Servizi gestiti, ascesa dinamica e continua

I servizi gestiti saranno un'arma in più per il canale che grazie a questi può intercettare le esigenze dei clienti, diventando partner nel business e non solo mero fornitore di prodotti hardware e software. Una tendenza che trova conferma nello studio commissionato da Cisco e condotto da Canalys che **evidenzia come i partner di canale ICT che si sono concentrati sui servizi gestiti nel 2023 dovrebbero**

far registrare una crescita significativa. A livello mondiale, nonostante il clima di incertezza che ha spinto verso il basso gli investimenti, le previsioni per i managed service fanno segnare una crescita mondiale del 12,7%, per un valore totale di 472 miliardi di dollari.

Una crescita che supera quella stimata del 3,5% della spesa IT complessiva.

La mancanza di personale competente sul mercato è alla base di questa crescita. **Le organizzazioni, non trovando persone formate, si affidano a partner** capaci di offrire soluzioni complete attraverso i servizi gestiti, acquisendo così le competenze e il supporto tecnologico necessario al proprio business. Secondo diversi analisti, come Gartner, McKinsey e Accenture, **il 2024 sarà l'anno dell'Intelligenza Artificiale**, e di conseguenza dei dati, perché senza una significativa mole di dati da analizzare l'Intelligenza Artificiale non funziona al meglio. I servizi e le soluzioni basate su di essa entreranno in modo prepotente in diversi punti dell'organizzazione aziendale, dalla cybersicurezza ai customer service, dal marketing all'ingegneria del software.

Come sarà il 2024?

Lo abbiamo chiesto ai principali attori di questo mercato; ognuno ha indicato quali saranno, secondo loro, gli elementi che potranno fare la differenza e come pensano di affrontare le sfide del 2024.

Il primo ad alzare la mano, in questo tavolo virtuale, è **Simone Cavazzoni, general manager di Quanture**, che pone l'accento sulla Intel-



ligenza Artificiale. *«Nel 2024, l'AI generativa sarà uno dei trend più dibattuti. La recente disponibilità di Microsoft Copilot per tutte le Pmi rappresenta un passo significativo nell'adozione di questa nuova tecnologia in Italia. In questo nuovo scenario i servizi gestiti saranno cruciali per colmare la mancanza di competenze ICT dei team interni delle aziende, mentre machine learning e realtà aumentata saranno sempre più richiesti nel settore OT e nelle aziende produttive. Cybersecurity e Sostenibilità saranno altri temi chiave del 2024. La recente escalation degli attacchi cibernetici richiederà piani strutturati di Disaster Recovery e il potenziamento delle difese aziendali. La sostenibilità sarà un argomento non più rimandabile, visto le scadenze imposte dalla direttiva europea "CsrD". Non solo andranno ripensate le strategie aziendali ma, andranno ottimizzati anche i processi di business. Il nostro ruolo è quello di abilitare queste tecnologie emergenti per guidare le imprese verso una nuova era digitale».*

Michele Puccio, country manager Italia di Arrow Enterprise Computing Solutions, invece, vede nel cloud e nei servizi "as-a-service" la strada da percor-



rere. *«Arrow è un distributore IT a valore aggiunto che promuove l'innovazione nel proprio canale di riferimento, aiutando vendor e IT provider a crescere, grazie a expertise, soluzioni vincenti, piattaforme digitali e servizi su misura che possono essere offerti agli utenti. Arrow negli anni si è trasformato in vero "advisor strategico" con competenze orientate al business, in grado di coordinare un network di provider capaci di mettere a fattor comune le specificità ed elevare il valore della partnership, un ruolo che sarà ulteriormente accentuato nel 2024. Inoltre, con lo spostamento del mercato verso tutto ciò che è "as-a-service", Arrow continuerà a rendere disponibili nuovi strumenti di valutazione e gestione del cloud attraverso la piattaforma ArrowSphere, per aiutare i partner di canale a promuovere i servizi XaaS presso i clienti. Arrow supporterà anche il tema dell'AI e, in qualità di intermediario del settore IT e della componentistica, il distributore aiuterà quell'ecosistema a venire alla luce, supportando tutti gli attori che ne fanno parte nel loro go-to-market».*

ReeVo, attraverso le parole di **Carmelo Pesce, head of channel ReeVo cloud & cyber security, Italia & Spagna**, sottolinea come il suo 2024 avrà nella formazione un punto focale per essere in grado di rispondere a tutte le richieste che possono arrivare dal mercato. *«Re-*



eVo offre servizi integrati di Cloud, Cyber Security e Hybrid Cloud raggiungendo il mercato con un canale di distributori e Business Partner. Una delle principali sfide che vediamo per il 2024 è la gestione della complessità delle architetture IT, sempre più soggette alle richieste di scalabilità e integrazione di ambienti eterogenei, dovute alla proliferazione di applicazioni, dati e dispositivi connessi. La sicurezza rimane un'area critica di preoccupazione e per questo proteggiamo e custodiamo all'interno della nostra "cassaforte digitale" il reale patrimonio delle aziende europee – i dati – ben consapevoli che la domanda di risorse cloud è in continua crescita. In qualità di cloud e cybersecurity provider, puntiamo ad affrontare tutte queste sfide cercando di ascoltare le esigenze dei nostri clienti e di offrire sempre più servizi e supporto. Riteniamo sia importante consolidare le competenze dei nostri partner e per questo abbiamo potenziato il nostro programma di canale con corsi Sales, Technical Foundation ed Expert sui servizi che costituiscono il nostro Dna, perché riteniamo che più il partner si forma sulle tecnologie e più sarà in grado di erogare un servizio a valore per il cliente finale, sviluppando maggiore business. Nel 2024 continueremo a puntare sulla parte DevOps: eroghiamo già da tempo un servizio gestito della piattaforma Kubernetes, in modalità PaaS, che con-

sente agli sviluppatori di applicazioni containerizzate di concentrarsi solo sugli aspetti principali lasciando invece a ReeVo la gestione della complessa infrastruttura Kubernetes».

L'Intelligenza artificiale torna protagonista nel pensiero di **Emanuele Caronia, cofounder and Ceo di Exelab**, che la vede non più come un lusso, ma come un requisito strategico. «Oggi risulta fondamentale riconoscere la crescente democratizzazione della tecnologia e l'importanza di adottare in modo efficace soluzioni basate sull'AI. Questa tendenza, sostenuta da evidenze di un sostanziale incremento della produttività grazie all'adozione dell'AI, si rivela essenziale per competere in un mercato in costante mutamento. L'evoluzione tecnologica ha infranto il predominio tradizionalmente detenuto dai grandi attori nel settore ICT, che si fondava su complessi progetti di system integration. Ora, con tecnologie sempre più intuitive e accessibili, è finalmente possibile implementare soluzioni agili e tempestive che possono rappresentare una risposta effettiva alle esigenze del business. Questo sviluppo si fonda, tra le altre cose, su un'accelerazione dei processi di raccolta e analisi delle informazioni, pilastri fondamentali per



GLI APPROFONDIMENTI
DI BIZZIT

Gli MSP italiani evolvono
puntando sui servizi gestiti



continua a leggere

mantenere un vantaggio competitivo. In questo scenario, l'Intelligenza artificiale emerge non più come un lusso, ma come un requisito strategico indispensabile. La sua mancata integrazione rappresenta un chiaro rischio di perdita di competitività».

Alessandra Girardo, coo di Kirey Group, nel suo intervento porta l'attenzione su come il passaggio



al cloud sarà fondamentale per le aziende italiane per stare sul mercato. «Scomponibilità, flessibilità

e microservizi: seguendo queste tre parole cardine, possiamo prevedere che nel 2024 il canale ICT si rinnoverà in una logica sempre più on-demand, con cambiamenti applicativi, architetturali e di management aziendale. Prendendo ad esempio l'AI, protagonista tecnologica indiscussa dell'anno, prevediamo che le aziende che vorranno introdurla nei propri processi opereranno quasi certamente per un Llm di terze parti, da configurare come nuovo servizio.

Alla base di questi cambiamenti ci saranno diversi elementi. In primis, il passaggio più marcato verso il cloud-native, non solo a livello di applicazioni, ma anche di architetture IT, per raggiungere obiettivi di scalabilità, disponibilità, disaster recovery e business continuity per composizione di servizi cloud; e infine, anche il progressivo evolvere della mentalità "composable", paradigma abilitante di un mondo orientato alla modularità».



**GLI APPROFONDIMENTI
BIZZIT**



**Da system integrator a
managed service provider**

+ continua a leggere

Secondo **Ready Informatica**, nella persona di **Terenzio Preda, direttore commerciale**, la capacità di adattarsi all'evoluzione del mercato è fondamentale per essere vincenti in questa fase del mercato.



«Il successo delle Pmi si basa su: innovazione, adattamento e collaborazione. Riuscire a proporre ai clienti un'offerta di servizi basata su automazione e standardizzazione è cruciale per l'efficienza e la crescita dei profitti. L'Intelligenza Artificiale gioca un ruolo chiave portando una semplificazione delle operazioni e risparmio di tempo. Il mercato evolve costantemente come gli attacchi informatici: investire in soluzioni di sicurezza informatica avanzata per proteggere i dati aziendali deve essere una priorità assoluta. L'adattamento rapido è essenziale per rispondere al cambiamento e per questo Ready Informatica punta sulla formazione

continua dei propri rivenditori, attraverso eventi e training mirati, perché un team preparato comprende le esigenze dei clienti, propone soluzioni efficaci e offre valore aggiunto al servizio.

Le Pmi che integreranno efficacemente questi elementi saranno in grado di affrontare le sfide e avere successo!».

Per Romeo Scaccabarozzi, AD di Axiante, il 2024 sarà un anno particolare, soprattutto per le variabili esterne che stanno influenzando il mercato, ma il nucleo sarà sempre l'uomo.



«Il 2024 sarà un anno di test, considerando la volatilità macroeconomica, le tensioni geopolitiche e l'instabilità delle catene di fornitura. A fare la differenza sarà la capacità di adattarsi e quindi l'agilità, diffusa in tutta l'organizzazione. Le aziende hanno più che mai da guadagnare dai progressi tecnologici e ancora più da perdere dalla scelta di restare indietro. L'incertezza comporta dei rischi: comprenderli e gestirli offre l'opportunità di esplorare nuovi mercati e di acquisire quote di concorrenti meno agili. Per prosperare nell'incertezza occorre resilienza. Ecco perché ci siamo posti come obiettivo chiave di aiutare i nostri clienti a essere ancor più resilienti, dopo lo shock di tre anni fa. Al nostro interno, lavoreremo per consolidare la fiducia tra i gruppi di lavoro e costruire opportunità di crescita. Vogliamo spostare l'attenzione

dalla semplice certificazione alla creazione di capacità ed esperienze che consentano al talento di prosperare in qualsiasi ruolo. Oltre al benessere dei dipendenti e alla flessibilità, è importante il significato del lavoro: i collaboratori sono spinti non solo dalla missione di un'azienda, ma anche dalla comprensione del modo in cui i compiti specifici loro affidati diano un contributo diretto».

Andrea Ceccaroni, sales director Vem Sistemi, invece, mette in

risalto i punti principali necessari per distinguersi nel 2024. *«Credo che elementi chiave e differenzianti in questo mercato siano da ricondursi soprattutto a tre*



punti principali: competenze sempre più qualificate, piattaforme di automazione e vicinanza al cliente. Vem, nel panorama italiano dei system integrator, è una delle aziende meglio strutturate per cogliere questa sfida poiché ha la giusta dimensione per offrire un servizio personalizzato e la solidità finanziaria che le permette di fare investimenti in persone qualificate, un team di DevOps che realizza e gestisce le piattaforme di visibility e di automazione, senza dimenticare la vicinanza geografica ai nostri clienti con le nostre 8 sedi. I servizi Vem si basano da un lato su piattaforme di visibility, in grado di misurare lo stato di salute dei nostri sistemi, di automation che permettono di effettuare una serie di attività in maniera veloce, affidabile e scalabile, e

dall'altro su personale dei team Noc, Soc e Irt sempre più qualificato in grado di analizzare i dati forniti dalle piattaforme e intervenire in maniera puntuale ed efficace. Altro elemento distintivo è la stretta partnership con pochi vendor molto qualificati, che ci permette di avere un accesso privilegiato ai loro servizi e di poter scalare facilmente per dare a nostra volta il miglior servizio possibile alle aziende».

MegaByte Sistemi Informatici, attraverso **Roberto Vicenzi, direttore sales & marketing**, nel suo



intervento sposa la causa Open Source come strada per avere servizi per le Pmi con un approccio capace

di contenere i costi. «Come società attiva sul mercato dal 1990 nei servizi di consulenza informatica per le aziende di piccole e medie dimensioni, MegaByte proseguirà nel delineare soluzioni personalizzate e all'avanguardia che soddisfino anche le più importanti e complesse esigenze aziendali dei clienti. La trasformazione digitale comporta un cambiamento culturale tanto quanto tecnologico che impone alle organizzazioni di rivedere radicalmente il modo di operare e di saper garantire customer experience e vantaggi concreti. Le attività già avviate dall'azienda nel 2023 proseguiranno in modo ancora più importante nell'anno appena iniziato. In particolare, MegaByte ha in programmazione un calendario

ricco di iniziative per il primo semestre mirate a presentare i plus delle soluzioni dell'infrastruttura iperconvergente basate su software open source e hardware standard, un'opzione particolarmente attraente per le Pmi che vogliono ottenere i benefici dell'infrastruttura convergente con un approccio più economico e adattabile alle specifiche esigenze».

L'intervento di **Francesca Moriani, AD di Var Group**, è incentrato sul

valore che hanno le persone e come

siano loro la vera forza. «Stiamo vivendo un momento in cui le imprese sono impattate dalla diffusione



delle tecnologie in modo pervasivo, un'accelerazione dettata in gran parte dalla diffusione dell'Intelligenza artificiale. Di fronte a questa spinta, dobbiamo prima di tutto imparare a conoscere e ad adottare le tecnologie più evolute per capire come possono migliorare il nostro lavoro e aiutarci nel valorizzare le persone e le loro competenze. Per cogliere pienamente quest'evoluzione, è fondamentale adottare nuovi modelli organizzativi, che mettano le persone al centro, promuovendo i talenti grazie a un modello di leadership diffusa. Per noi è strategico far collaborare in modo più efficiente le quattro generazioni che popolano la nostra realtà. In Var Group siamo impegnati nell'ascolto attivo e vogliamo essere una fucina di sperimentazione. In un contesto di incertezza e cambiamenti, ci impegniamo a catalizzare questa trasfor-

mazione, creando un ambiente dove ognuno possa esprimere appieno il proprio valore».

Il fattore umano è importante anche per **Augusto d'Antinone, Ceo Exclusive Networks Italia**, perché la carenza di competenze è uno dei



grandi problemi che tutti dovranno affrontare nel 2024. «Una delle sfide maggiori che si porrà anche nel 2024 è la carenza

di risorse esperte, soprattutto in ambito cybersecurity. L'Italia sta da un lato accelerando nell'adozione di tecnologie innovative di IT Security che vedono sempre più un uso avanzato dell'AI, ma dall'altro deve affrontare la carenza di competenze. Il "mercato" dell'AI si presenta destrutturato e si discosta dalle dinamiche tradizionali del settore ICT. L'AI è molto spesso integrata nelle soluzioni dei vendor, richiedendo che i system integrator acquisiscano competenze specifiche per comprendere in quali applicazioni può essere implementata e con quali modalità in base ai business case del cliente. La materia è estremamente vasta ed è fondamentale avere idee molto chiare sugli ambiti di applicazione per evitare il rischio di dispersione di risorse ed energie. Un altro tema che anche quest'anno sarà importante riguarda i servizi gestiti. Per gli Msp un distributore come Exclusive Networks può svolgere non solo un ruolo consulenziale, ma agire come un vero e proprio fornitore di soluzioni "ready to go" che facilitano

notevolmente l'offerta dei system integrator verso i propri clienti. Il nostro obiettivo è aiutare rivenditori, system integrator e service provider a offrire ai loro clienti tecnologie all'avanguardia e servizi innovativi».

A chiudere la rassegna **Stefania Meregalli, marketing manager di C.I.E. Telematica** che, con i suoi 30 anni di esperienza sul mercato, ha sempre investito per incrementare il know-how dei suoi collaboratori e le partnership strategiche con altre aziende e fornitori.



«Questa scelta ci ha sicuramente premiato, riflettendosi sul rapporto che abbiamo costruito con i clienti, relazionale e consulenziale, che ci ha fatto diventare un punto di riferimento dalla selezione della tecnologia, la progettazione, l'integrazione di servizi e soluzioni fino alla fornitura.

Nel corso degli anni la nostra azienda ha cambiato pelle per proporre una nuova prospettiva sul mercato, questo ci ha portato a identificare chiaramente i vendors con cui investire e collaborare, per definire soluzioni mirate ai nostri clienti target. Un'ulteriore scelta strategica è stata quella di sviluppare un circolo virtuoso di collaborazione con altre aziende attive sul nostro mercato ma con competenze diverse dalle nostre, in modo da poter allargare il nostro portafoglio di soluzioni appoggiandoci a società di fiducia».

RIMANI AGGIORNATO
ISCRIVITI ALLA NEWSLETTER





I managed print services secondo Brother

di Fabrizio Pincelli

Con Pagine+ l'azienda offre un servizio che sgrava da ogni attività di manutenzione, centralizza il controllo delle macchine e abbate i costi, prevedendo che si paghi solo per le stampe prodotte.

Un giro d'affari globale di 42,09 miliardi di dollari nel 2023 che dovrebbe raggiungere i 63,35 miliardi nel 2026, facendo registrare un CAGR dell'8,52% annuo. Numeri di rilievo quelli forniti dalla società di ricerca **Mordor Intelligence** per il **mercato dei servizi di stampa gestiti** (managed print service, MPS). Numeri che mostrano quanto gradiscano le imprese ricorrere a questi servizi per migliorare la produttività e ridurre i costi.

Tra le aziende che per prime hanno creduto nell'efficacia dei servizi di stampa gestita c'è **Brother**, che grazie a **Pagine+** consente di sgravare completamente gli utenti dalla manutenzione della stampante. L'obiettivo è consentire di **ottimizzare i processi documentali**, liberando risorse per attività più rilevanti legate al core business. Il tutto, abbattendo i costi. Infatti, con Brother Pagine+, il **risparmio può arrivare fino al 40%**.

Questo perché Brother propone una formula a consumo che prevede si paghi solo per le stampe realizzate: se non si stampa non si paga nulla.

Obiettivo personalizzazione

Il focus sul cliente e sulle sue esigenze è una priorità che Brother non perde mai di vista, sin dal momento in cui si decide di scegliere con quali periferiche lavorare. In tal senso, il cliente può ottenere una consulenza gratuita da parte degli esperti Brother così da effettuare un'analisi dettagliata sia del parco stampanti presente in azienda sia dei processi e delle esigenze di stampa, in maniera da progettare una soluzione tarata sugli effettivi bisogni. Tale soluzione potrà poi essere tenuta sotto controllo attraverso il software **BRAdmin Professional, che centralizza la configurazione e la gestione di stampanti** e multifun-

zione e consente di monitorarne lo stato. Tramite

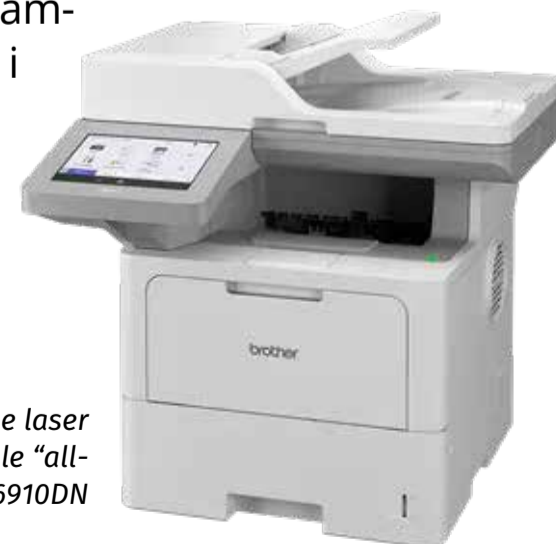
BRAdmin Professional è possibile avere analytics dettagliati per ottimizzare i consumi e snellire i processi.

Pagine+ permette, inoltre, di avere un totale automatismo nella gestione dei consumabili, che possono essere richiesti direttamente dalle macchine se si imposta una soglia di notifica. Brother provvederà a inviarli gratuitamente in azienda. Analogamente, per evitare fermi macchina, Pagine+ prevede un servizio di assistenza per i problemi legati

all'usura. In questo caso Brother interviene presso il cliente ripristinando il normale funzionamento della macchina, nel rispetto dei Service Level Agreement concordati.

Velocissime, sicure e facili da usare

Tra le macchine Brother che possono trarre vantaggio dei servizi di stampa gestita c'è anche la nuova serie di **laser monocromatiche** che prevede un modello **solo stampante HLL6410DN** e uno **multifunzione MF-CL6910DN**. Pensate per garantire stampe velocissime (50 pagine al minuto e la produzione della prima stampa richiede meno di 6,7 secondi), scansioni di livello professionale (passaggio singolo su due lati fino a 100 immagini al minuto) e facilità d'uso, offrono un triplice livello di sicurezza (per dispositivi, reti e documenti) in modo da ridurre la superficie di attacco. Dotate di connettività Gigabit Ethernet (ma in opzione c'è anche il WiFi a 5GHz) e di memoria fino a 2 GB, supportano inoltre l'iniziativa di Brother "zero-waste-to-landfill" (zero rifiuti rilasciati nell'ambiente), che attraverso i suoi impianti di rigenerazione in Europa riesce a ridurre l'impatto ambientale riciclando i toner e riutilizzando i componenti delle stampanti.



La stampante multifunzione laser monocromatica professionale "all-in-one" Brother MFC-L6910DN

 RICHIEDI LA
CONSULENZA GRATUITA



C.I.E. unifica la rete e la gestisce dal cloud

di Riccardo Florio

Attraverso le soluzioni e gli strumenti Cisco Meraki, il system integrator mette a disposizione un'infrastruttura di rete gestita dal cloud pensata per semplificare l'accesso, proteggere le risorse digitali e fisiche e creare spazi di lavoro più intelligenti.

Il modo di lavorare e i processi di business sono cambiati e **nessuno vuole tornare a quella che era la normalità aziendale di tre anni fa**. Oggi le aziende desiderano avanzare nel percorso verso la trasformazione digitale e sentono più che mai l'esigenza di predisporre workspace ibridi, scalabili e sicuri così come di sfruttare la flessibilità offerta dal cloud.

La flessibilità si ricerca anche nella varietà di dispositivi mobili utilizzati per il lavoro che, sempre più spesso, si trovano a condividere l'uso aziendale con quello personale, evidenziando la necessità di predisporre soluzioni efficaci di gestione e configurazione. In tutto ciò la sicurezza si conferma un tema irrinunciabile con un'integrazione sempre più serrata tra cybersecurity e sicurezza fisica.

Insomma, uno scenario che rende quanto mai pressante l'esigenza di disporre di reti sicure, flessibili, integrate, facil-

mente gestibili e aperte al cloud.
A tutte queste esigenze fornisce una risposta la piattaforma Cisco Meraki.

Gestione completa da un'unica dashboard in cloud

Cisco Meraki è la suite di soluzioni e strumenti che consente di predisporre un'infrastruttura di rete unificata e gestita dal cloud da cui usufruire di servizi digitali quali: sicurezza informatica, connettività fissa e wireless, amministrazione della mobilità aziendale, capacità di analisi avanzata e videosorveglianza.

Questa piattaforma elimina, pertanto, la complessità dell'integrazione tra network, sensori e la raccolta dei dati consentendo di sfruttare al meglio la capacità dell'infrastruttura e di ridurre l'impatto ambientale dell'organizzazione, migliorando la visibilità della rete e la sicurezza degli utilizzatori. Attraverso un modello di rete geografica definita da software (Software-Defined WAN) è possibile controllare il traffico di rete mediante un'interfaccia unica centralizzata e assicurare un elevato grado di sicurezza intrinseca.

Elemento distintivo di questa piattaforma è la **dashboard centralizzata basata su cloud**, attraverso la quale gli amministratori IT hanno la possibilità di gestire in modo semplice l'intera infrastruttura.

OTTIENI LA GUIDA
DI CISCO MERAKI



La proposta Cisco Meraki è unica nel suo genere per l'ampiezza delle soluzioni offerte che riescono a integrare, in modo coerente, componenti digitali e fisiche.

L'universo di Cisco Meraki

I componenti che definiscono la piattaforma Cisco Meraki sono i seguenti:

- **Switching.** Gli switch Meraki forniscono prestazioni elevate, affidabilità e facilità di gestione con il supporto di funzionalità avanzate come Power over Ethernet, voice VLAN e QoS per ottimizzare la trasmissione di voce e video.
- **Connettività wireless.** Le soluzioni WLAN Meraki sono progettate per fornire una copertura wireless affidabile e sicura e si avvalgono di tecnologie avanzate di roaming e ottimizzazione automatica del segnale, per garantire una connettività senza problemi.
- **Sicurezza dei dispositivi mobili.** Grazie alle funzionalità di Mobile Device Management è possibile semplificare la gestione di smartphone, tablet e altri dispositivi mobili, effettuare l'importazione automatica dei dispositivi sulla rete e modificarne la configurazione in pochi click.
- **Software-Defined WAN.** Le funzionalità di controllo del traffico di rete fornite dalla SD WAN offrono protezione dalle minacce, filtraggio del contenuto Web e creazione di VPN in modo automatico senza nessuna configurazione manuale.

- **Videocamere smart di sorveglianza.** Le telecamere di sicurezza Meraki, sfruttando la potenza dell'intelligenza artificiale, forniscono analisi video avanzate che consentono di comprendere come le persone sfruttano gli spazi sorvegliati nella piena garanzia della privacy. In combinazione con le applicazioni basate su API, i sensori forniscono anche informazioni su occupazione, livelli di rumore, temperatura e altro ancora per aiutare a mantenere un ambiente confortevole e sicuro.

Una soluzione che offre innumerevoli vantaggi alle PMI

Cisco Meraki si dimostra adatta alle esigenze delle piccole e medie imprese a cui offre i vantaggi di una soluzione, innanzitutto, **veloce da installare** grazie alla possibilità di preconfigurare i dispositivi prima ancora che vengano consegnati e collegati. Inoltre, si tratta di una soluzione **pensata per evolvere nel tempo** grazie a un'architettura basata sul cloud che consente di scaricare e installare automaticamente gli aggiornamenti del firmware, le nuove funzioni e gli aggiornamenti di cyber security. Un ulteriore elemento caratterizzante è il fatto di essere una soluzione **facilmente personalizzabile e gestibile**: attraverso un'unica Dashboard in cloud - accessibile da Pc, tablet e smartphone - le piccole aziende hanno la possibilità di monitorare le prestazioni delle proprie reti e apportare modifiche personalizzate alla loro configurazione in pochi secondi.

IL VALORE DI C.I.E.

Fondata nel 1994, C.I.E. vanta 30 anni di know-how nei mercati ICT e TLC, rappresentando un partner tecnologico di riferimento per le aziende che vogliono intraprendere la strada della trasformazione digitale, attraverso un portafoglio di soluzioni che spazia dalla collaboration al networking, dalla security all'Edge computing, dalla video sorveglianza alle smart city. La sua "value proposition" coniuga tecnologie innovative e servizi a valore aggiunto al fine di confezionare soluzioni ritagliate su misura delle specifiche realtà aziendali. Inoltre, C.I.E. vanta una partnership di lunga durata con Cisco e una conoscenza approfondita delle soluzioni Cisco Meraki. Per queste ragioni, il system integrator con sede a Monza, non solo rappresenta il **partner ottimale per implementare le soluzioni Cisco Meraki** ma anche quello in grado di integrare, con competenza e cognizione di causa, queste soluzioni con l'infrastruttura aziendale esistente nonché di farle dialogare con soluzioni di terze parti. In questo modo è possibile creare soluzioni su misura che si adattano perfettamente alle esigenze specifiche di ogni organizzazione e capaci di coniugare efficacemente i vantaggi della sicurezza IT e fisica, del lavoro in mobilità e della flessibilità offerta dal cloud.



Andrea Veca, managing director di Achab, offre a Partners uno sguardo approfondito sull'evoluzione degli MSP italiani con un focus sulle proprie soluzioni, pensate su misura per le esigenze specifiche del settore, con un forte accento sull'automazione e l'efficienza.



Andrea
Veca



Le infrastrutture ICT nelle PMI italiane: sfide e soluzioni

di Riccardo Florio

Nell'era digitale, le PMI italiane affrontano sfide cruciali nelle infrastrutture ICT: budget limitati, carenza di competenze tecniche e minacce alla sicurezza. In quest'ottica, il distributore milanese Achab risponde con soluzioni di Managed service provider flessibili ed efficienti, privilegiando l'automazione e il supporto costante, e si adatta all'evoluzione verso il modello SaaS. A raccontarci come sta evolvendo il mondo degli MSP in Italia è **Andrea Veca, managing director di Achab** il quale ci illustra l'approccio dell'azienda nella rivendita di soluzioni.

Quali sono le principali sfide che le PMI italiane incontrano nella costruzione di infrastrutture ICT?

In un mondo sempre più iperconnesso e in continua evoluzione, le piccole e medie imprese italiane hanno molte sfide legate alle infrastrutture ICT. Spesso si confrontano con limitazioni di budget e carenze di competenze tecniche necessarie per sviluppare infrastrutture ICT efficaci. Anche la sicurezza informatica e la conformità normativa sono sfide notevoli, richiedendo consapevolezza e adattamento ai nuovi regolamenti sulla privacy. Inoltre, è essenziale una cultura aziendale dinamica per massimizzare i benefici dell'IT gestito. Affrontare queste sfide richiede una pianificazione attenta, l'allocazione di risorse adeguate e, in molti casi, la collaborazione con partner esterni specializzati in ambito IT.

In che modo le vostre soluzioni per MSP migliorano la capacità dei fornitori di servizi IT di gestire le infrastrutture dei loro clienti?

Achab offre soluzioni MSP flessibili e a costi contenuti, orientate ai bisogni degli MSP in aree come sicurezza, backup e privacy. Con l'automazione integrata, i nostri prodotti massimizzano l'efficienza, permettendo di "fare di più con meno". Il

nostro team esperto fornisce supporto mirato e servizi personalizzati, per aiutare i partner a navigare le complessità del settore IT.

Qual è l'approccio di Achab nella rivendita di soluzioni, in un mercato sempre più orientato verso il modello SaaS?

Achab, distributore specializzato, offre infrastrutture ICT flessibili, efficaci e convenienti per PMI italiane, tramite servizi IT gestiti. Ci focalizziamo sui migliori prodotti internazionali, mirando a fornire soluzioni di valore. Il nostro servizio completo copre consulenza pre-vendita, consegna "chiavi in mano", formazione e manutenzione. Basiamo il nostro approccio su relazione, ascolto, condivisione e collaborazione, rendendo i prodotti soluzioni di qualità. Semplifichiamo le operazioni di clienti e partner, migliorando l'efficienza e la redditività. In un mercato orientato al Cloud e SaaS, Achab adotta strategie innovative, selezionando soluzioni SaaS di punta e collaborando direttamente con produttori rinomati, per assicurare prodotti di qualità e una comunicazione efficiente, eliminando gli intermediari. Poniamo enfasi sul supporto continuo, dalla consulenza pre-vendita alla formazione post-installazione, essenziale per il succes-

so nel SaaS. Miriamo a semplificare i processi, gestendo centralmente e automatizzando le soluzioni, ottimizzando le risorse per massimizzare l'efficienza operativa.

Come vengono formati e supportati i vostri MSP partner per assicurare servizi di gestione IT efficaci?

Dai corsi di formazione al supporto tecnico, dal coaching all'organizzazione di eventi, sia fisici che digitali, i nostri Partner possono trovare sempre un porto sicuro in base alle loro esigenze. In generale Achab favorisce lo scambio di esperienze e migliori pratiche anche tra i vari MSP partner. Questo approccio collaborativo consente ai partner di imparare dagli altri e di implementare soluzioni di successo. Guardando con attenzione a questi valori, Achab organizza ormai da diversi anni, tra gli altri eventi verticali, due importanti appuntamenti che sono diventati un punto di riferimento per il mercato dei servizi IT gestiti: l'MSP Day aperto a tutti e Aclub riservato ai Partner Achab.

Quali innovazioni tecnologiche state implementando per gli IT service provider e le PMI italiane?

Sempre attenti alle innovazioni, ci focalizziamo principalmente sulla cybersecurity, affrontando la



GLI APPROFONDIMENTI
DI BIZZIT

Achab risponde alle esigenze di business continuity e disaster recovery degli MSP

Con l'ingresso di Axcient x360Recover nel proprio portfolio, Achab arricchisce l'offerta di soluzioni studiate su misura per gli MSP e dedicate alla sicurezza dei dati e alla ripartenza delle aziende in caso di fermo



crescente complessità IT. Il nostro obiettivo è rafforzare la sicurezza aziendale multi-strato e semplificare la gestione IT. Achab supporta gli MSP con soluzioni mirate a superare queste sfide, garantendo sicurezza e facilitando la gestione dell'IT.

Considerando l'importanza crescente dell'AI, come la state incorporando nelle offerte per MSP e quali i vantaggi per le aziende italiane?

In ambito MSP l'intelligenza artificiale può avere impatto in 3 direzioni: eliminazione del "rumore di fondo" nella gestione dell'IT, individuazione dei veri pericoli e diminuzione dei falsi positivi in ambito sicurezza, aumento dell'efficienza nella gestione dei ticket di supporto. Pur continuando a guardare attentamente il mercato alla ricerca di nuove soluzioni, stiamo riscontrando che i vendor stanno già inserendo sistemi basati sull'AI nei loro prodotti esistenti che abbiamo a portfolio.



La cybertempesta perfetta: visioni della sicurezza nel 2024

Tendenze e previsioni della cybersecurity tra analisi e riflessioni per l'anno appena iniziato: competenze, guerre e tecnologie tra ransomware e vishing

di Leo Sorge

Il 2024 si preannuncia un anno di svolta nel modo in cui affrontiamo e gestiamo la sicurezza nel cyberspazio.

Provando una sintesi estrema, viviamo in un mondo sempre più difficile, nel quale ci sono pochi addetti, c'è diffusa ignoranza e purtroppo è quasi totale la cecità alle guerre e alle loro conseguenze.

Il rischio è che la sicurezza informatica diventi un mero tecnicismo, com'è infatti considerata dalla maggioranza delle persone e delle aziende di piccole dimensioni. Guardando bene, invece, si nota che la cybersecurity è probabilmente il singolo punto dal qua-

le partire per fare qualsiasi cosa. Senza porta di casa e polizia per le strade non si creano Stati né si gestiscono territori, siano essi fisici o digitali.

Nel considerare le prospettive per il 2024 nel campo della cybersecurity, osserviamo un panorama in rapida evoluzione, dove le nuove tecnologie e una sorta di terza guerra mondiale distribuita richiedono una sensibilità acuta verso informazioni non pubbliche e cambiamenti tecnologici e applicativi che operano su una scala mai vista prima. Questo contesto complesso e dinamico solleva interrogativi cruciali e impone sfide senza

precedenti, spingendo professionisti, aziende e governi a rivedere e adattare continuamente le loro strategie di sicurezza informatica. Diseguito, esploriamo le aree chiave che delineano il futuro della cybersecurity, ognuna delle quali riflette aspetti diversi di questo scenario in continua evoluzione. Volendo semplificare all'estremo, le macroaree di riferimento possono essere tre: **gestione del parco del talento, allargamento del perimetro e nuove applicazioni di tecnologie** già note. Oltre a svariate fonti giornalistiche, nell'analisi che segue abbiamo dato rilevanza al **Google Cloud Cybersecurity Forecast 2024** e all'analisi **Top 10 Cyber Security Trends And Predictions For 2024** svolta da Splashtop. I dati mostrati in alcune illustrazioni e riguardanti il 2023 provengono invece da **The CyberThreat Report: November 2023 di Trellix**.

SCARICA IL REPORT
GOOGLE CYBERSECURITY
FORECAST 2024



SCOPRI LA TOP 10 DEI
TRENDS 2024 NELLA
CYBERSECURITY



VAI AL REPORT
CYBERTHREAT
DI TRELLIX



Competenze, guerra, tecnologie

Diamo una prima occhiata a cosa ci aspetta nei mesi, o meglio anni,

a venire. Servono competenze, un'ampia visione delle conseguenze delle guerre in atto e la consueta attenzione per gli sviluppi tecnologici. Siamo sempre in uno scenario in veloce e imprevedibile movimento.

Gestione del parco del talento

Il problema principale è la bassa qualità dell'educazione in molte parti del mondo. Ancora di più in Italia, patria del diritto e del Rinascimento: i cybercriminali vanno diritti al sodo, senza proclami né diritti. Per combatterli con armi (speriamo) lecite e speriamo di pari potenza servono molti professionisti ricchi di competenze e con il mindset giusto. Ma non li abbiamo, né in ICT né in settori ancora più moderni come la transizione energetica o l'ESG, Environmental, Social e Governance. Quindi ad avvantaggiarsi sono le nazioni che hanno una popolazione molto più numerosa e molto più giovane della nostra, due punti che facilitano una statistica positiva nel numero dei formati e nel successivo aggiornamento.

In Occidente e nei Paesi occidentalizzati c'è oggi un **enorme gap di competenze e formazione** per numero e qualità delle persone. Come in tutti i processi, anche la formazione non è fatta bene, bensì è l'ultima conseguenza di una millenaria tradizione che mantiene in piedi sé stessa, non i suoi obiettivi. E riguarda sia gli operatori, sia i cosiddetti dirigenti: il talento sta diventando il problema centrale della nostra epoca. In particolare, nel

2024 andrà ad aumentare il gap di competenze in cybersecurity dei dirigenti aziendali. È una questione rilevante sia in Italia che in altre nazioni, indipendentemente dal fatto che le aziende siano specializzate o meno in questo campo. La crescente complessità delle minacce informatiche e l'importanza della sicurezza dei dati per tutte le organizzazioni rendono **essenziale che i dirigenti abbiano una solida comprensione dei rischi di cybersecurity e delle strategie per mitigarli.**

Nella formazione, però, poco si può fare se non si riparte da zero, pensando alla security by design e all'aggiornamento continuo di tutti (a partire dalle cosiddette teste pensanti).

Senza una cultura della sicurezza e la comprensione dei processi di conformità legale (si pensi al GDPR e alle altre leggi simili nel mondo), le decisioni prese dal dirigente sono inadeguate e portano al fallimento della specifica iniziativa.

Un po' ovunque esistono scuole di cybersecurity per dirigenti, così

come i programmi executive per formazione intensiva. Ma età e mentalità del dirigente medio fanno pensare a uno scarso profitto da nuova formazione: l'impressione è che la percentuale di dirigenti sostituiti per inadeguatezza tecnologica sia destinata a impennarsi.

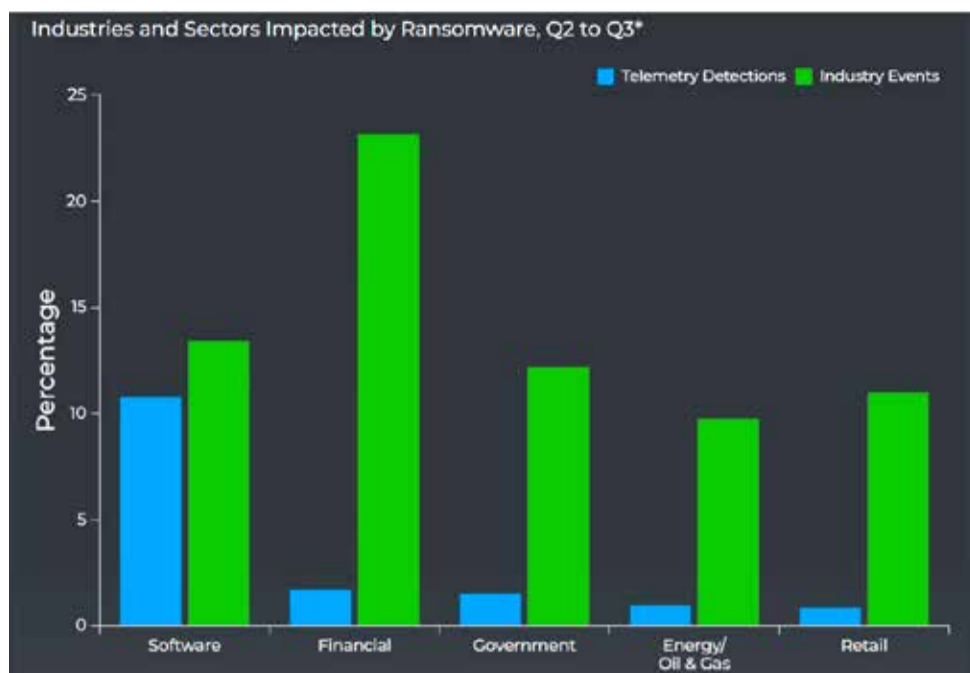
Allargamento del perimetro difensivo

Certamente il ransomware continuerà a essere la minaccia più forte ai sistemi informatici. Varie soluzioni di blocco, inattaccabilità dei dati e tecnologia dello storage rendono già da oggi estremamente difficile bloccare l'operatività dell'azienda attaccata.

Va forse fatto notare che l'eco delle varie notizie di cybercrimini è molto diversa dalla realtà misurata. Un qualsiasi diagramma che mostri entrambi i dati suddivisi in settore industriale mostra che in generale quel che si ascolta è *much ado for nothing*, molto rumor per nulla (o quasi). E questo rientrerebbe, se non direttamente tra le fake news (altro punto

IL TERRORE VIENE DAL PASSATO

L'avanzamento delle competenze permette anche di riscoprire e applicare tecniche antiche, quindi già note ma finora poco conosciute. Un esempio notevole raccontato (anche) nel Google Cloud Cybersecurity Forecast 2024 risale al 2013, quando un ricercatore ha descritto nell'ambito di un blog post l'uso di funzioni SystemFunctionXXX non documentate, alternative alle classiche funzioni crittografiche nell'API documentata di Windows. Questa metodologia non ha guadagnato popolarità fino al quarto trimestre del 2022, periodo in cui diversi esperti di sicurezza hanno iniziato a discuterne, pubblicando frammenti di codice nei loro blog e su GitHub. Di conseguenza si sono moltiplicati i campioni di malware che implementavano questa tecnica. Più recentemente è stato osservato l'uso di una tecnica anti-macchina virtuale (anti-VM), descritta in un libro di analisi malware del 2012, ma non ampiamente rilevata poiché l'uso dell'hypervisor non è comune in molti Paesi.



Nel grafico: Ransomware: differenza tra eco mediatica e numero di tentativi di attacco rilevati effettivamente (dati Trellix)

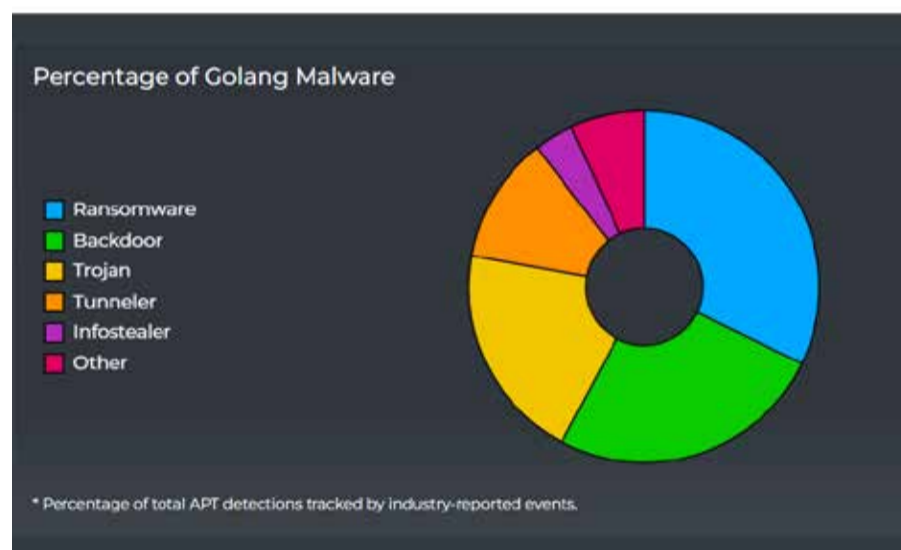
limitrofo alla sicurezza), perlomeno nel *fact checking*.

Google ritiene inoltre che si avrà un aumento nell'uso di vulnerabilità zero-day, targeting di ambienti ibridi e multcloud, servizi serverless e operazioni di estorsione sofisticate. Google rimarca come la supply chain sarà nell'occhio del ciclone, in quanto sia prevedibile l'aumento degli attacchi in particolare tramite gestori di pacchetti software come NPM, PyPI e crates.io.

Analogo discorso può essere fatto per i linguaggi di programmazione. Gli autori di malware stanno progressivamente orientandosi verso linguaggi moderni come Go (Golang), Rust e Swift. Questa tendenza è dovuta ai numerosi vantaggi offerti da questi linguaggi: un'ottima esperienza di sviluppo, funzionalità a basso livello, un'ampia libreria standard e l'integrazione semplice con pacchetti di terze parti. La creazione

di nuovi software destinati a eludere i sistemi di rilevamento diventa più economica. Di conseguenza, si assiste a un cambiamento nei toolkit impiegati dagli aggressori, con la necessità di sviluppare nuove firme di rilevamento. Purtroppo, i linguaggi moderni spesso includono un runtime esteso (come nel caso di Go) o impiegano tecniche di compilazione avanzate (come per Rust), complicando così le attività di reverse engineering. In altre parole, questi linguaggi offrono i benefici di packing e obfuscation tipici dei

software di protezione, senza necessità di utilizzare strumenti aggiuntivi.



Nel grafico i più recenti linguaggi di programmazione offrono nuove possibilità ai malfattori: il caso Golang (dati Trellix)

software di protezione, senza necessità di utilizzare strumenti aggiuntivi.

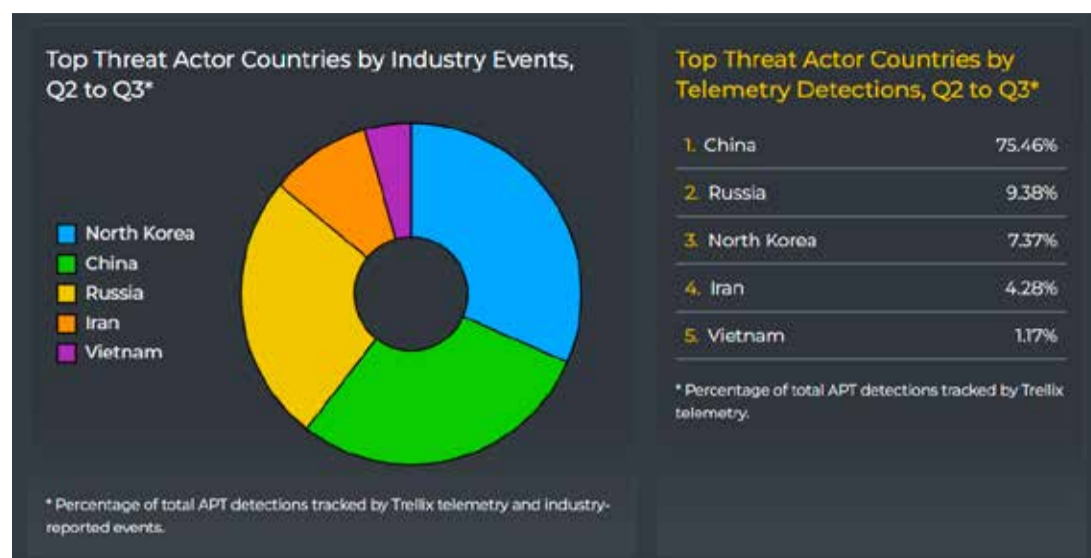
Spazio, nuova frontiera

Un aspetto rilevante per la sicurezza che verrà è nelle nuove infrastrut-

turazioni. Proliferazione satellitare, infrastrutturazione elettrica, connessioni dal sensore IoT all'edge computing fino alle auto a guida autonoma sono tutti fenomeni contemporanei che delineano perimetri di conflitto. Proprio lo spazio è sempre più sotto attacco. Tutti i sistemi satellitari hanno problemi di cybersecurity: accesso non autorizzato, interferenze e jamming, vulnerabilità delle stazioni a terra, attacchi ai dati, sicurezza dei software, satelliti commerciali, rischi per la sicurezza nazionale e globale, sfide nella legislazione e cooperazione internazionale e rischi associati ai satelliti obsoleti sono solo i principali punti di attacco. Sui satelliti in genere si usa la crittografia quantistica. Il suo vantaggio principale è la capacità di rilevare eventuali tentativi di intercettazione dei dati. **Questo avviene perché la misurazione di una particella quantistica (come un fotone) altera il suo stato, rendendo evidente qualsiasi tentativo di spionaggio e semplificando l'adozione di contromisure.** Gli attacchi, però, crescono, e con essi il relativo business della protezione.

Cryptovalute e dove proteggerle

Un altro fronte di attacco verrà offerto dalla digitalizzazione delle



Nel grafico: Anche il Vietnam, con i suoi quasi 100 milioni di abitanti, si affaccia sul panorama geopolitico del cybercrimine (dati Trellix)

valute nazionali, magari in appoggio a nuove promesse politiche. Parecchi dei Paesi che hanno le elezioni nel 2024 hanno in piedi progetti che riguardano vecchie e nuove cybervalute: al nuovo presidente argentino si affiancheranno eletti negli Stati Uniti, in Russia, nell'Unione europea, Bielorussia, Taiwan, Canada, Colombia e molti altri Paesi.

La sicurezza è centrale nella gestione della blockchain che garantisce la notarizzazione dei trasferimenti di valuta, quindi aumentare il numero di queste valute equivale a dare ai criminali nuovi punti di attacco.

In quest'ambito, **gli attacchi potrebbero non fermarsi al guadagno diretto dato dal furto, ma anche destabilizzare una moneta digitale nazionale per influenzare l'economia di uno Stato.**

Non è facile garantire l'elevato livello di sicurezza informatica per prevenire tali minacce, anzi è chiaro che diventeranno una nuo-

va vulnerabilità nevralgica del sistema complessivo. Inoltre le posizioni sullo scacchiere di Nord Corea (posizione attiva) e Taiwan (posizione passiva), pur non ancora scoppiati in guerra aperta, sono punti nevralgici di conflitto anche cyber.

“Nuove” tecnologie

In qualità di tecnica più raccontata del 2023, l'intelligenza artificiale va considerata in qualsiasi articolo tecnico. L'AI e il quantum computing stanno ridefinendo le capacità di difesa e attacco nello spazio, sia cyber sia reale. Un'applicazione specifica dell'AI riguarda i deepfake video e audio, quest'ultimi detti anche vishing (voice phishing).

Quantum e post-quantum

Per ciò che riguarda il quantum computing, molti osservatori rimarcano che al di là di annunci miracolosi e di una modesta applicazione a criteri pratici, le effettive capacità di elaborazione di questi sistemi non sono poi molto mag-



GLI APPROFONDIMENTI
DI BIZZIT



**AI e Quantum Computing:
il futuro della security
secondo Cisco**

Nell'era dell'Intelligenza artificiale e del Quantum computing le aziende devono dare priorità alla resilienza, all'agilità, alla centralizzazione dei dati

[+ continua a leggere](#)

giori di quelle disponibili vent'anni fa, per cui investire sarebbe inutile. La critica non è infondata, ma non sono d'accordo con la conclusione. Esistono diverse tecnologie di elaborazione, trasmissione e cifratura quantistica, che elaborano teorie sulla scorta di principi diversi da quelli tradizionali. Se un'organizzazione riesce ad applicare questi risultati, otterrà un vantaggio competitivo enorme: investire continuamente serve a ridurre

L'ASSICURAZIONE DIVENTA MAINSTREAM

Non c'è vero disaster recovery senza una bella assicurazione, dicono alcuni. Ecco perché anche nella cybersecurity l'assicurazione diventa una componente standard della gestione del rischio aziendale, con l'adozione di soluzioni di sicurezza che possano ridurre i costi globali.

Secondo l'analisi Top 10 Cyber Security Trends And Predictions For 2024 di Splashtdot, infatti, nel 2024 le polizze assicurative per la cybersecurity diventeranno un elemento fondamentale nelle strategie di gestione dei rischi aziendali.

Di fronte a minacce informatiche sempre più sofisticate e frequenti, le aziende si affideranno maggiormente alle assicurazioni. Ma non c'è nessun pasto gratis: il prezzo di queste assicurazioni è notevolmente influenzato dal livello di protezione informatica dell'azienda.

La crittografia avanzata, l'autenticazione multifattore e dettaglio nei log di accesso sono elementi che rafforzano la sicurezza IT, diminuendo il rischio di danni da attacchi informatici e quindi diminuendo i premi assicurativi.

il tempo di adeguamento ad una eventuale supremazia altrui.

Inoltre confrontare gli algoritmi quantistici con quelli tradizionali migliora questi ultimi, com'è ad esempio per la cosiddetta crittografia post-quantum.

Forse è poco per giustificare gli investimenti necessari, ma forse no. In caso di successo, restare indietro porterebbe ad effetti drammatici. Prendiamola come un'assicurazione, visto che proprio questo settore sta crescendo anche in cybersecurity aziendale.

Intelligenza artificiale

Un altro punto rilevante, anche se per vari motivi sulla bocca di tutti, riguarda l'applicazione dell'intelligenza artificiale alla cybersecurity. Personalmente ritengo necessario fare molta attenzione agli aspetti normativi, che creeranno incertez-

za e discriminare tra i vari blocchi (US, Europa, Cina...).

Secondo Google, nel 2024 si vedrà un aumento dell'uso dell'AI e dei grandi modelli linguistici in attacchi di phishing e ingegneria sociale, rendendoli più sofisticati e difficili da rilevare.

Splashtop osserva però che AI e Machine Learning stanno giocando un ruolo cruciale nel migliorare i sistemi di rilevamento precoce e risposta alle minacce.

Certamente il 2024 sarà l'anno di preparazione all'applicazione dell'AI Act europeo e delle altre ipotesi normative (UK, USA etc). Visto l'elevato numero di esenzioni ipotizzate dal testo, però, è ragionevole pensare che la gran parte dei produttori preferirà redigere documenti di esenzione immediata piuttosto che adeguarsi nel futuro ad una disciplina che promette più

I COMPROMESSI IMPOSSIBILI DEL RANSOMWARE PER LE PMI

Per molti aggressori di Ransomware le piccole e medie imprese sono oggi l'obiettivo più interessante. Con i bilanci sotto pressione a causa dell'aumento dell'inflazione, molte di queste aziende sono state costrette a tagliare i costi dei loro programmi di sicurezza IT, lasciandole potenzialmente non sufficientemente attrezzate per far fronte a un attacco, ma con abbastanza denaro da rendere il tutto conveniente per i criminali.

Le organizzazioni criminali che veicolano i Ransomware riescono a muoversi più rapidamente con le imprese più piccole e ritengono, inoltre, che siano meno propense a coinvolgere le forze dell'ordine rispetto alle realtà enterprise, che hanno più familiarità con i meccanismi di segnalazione e sanno come ottenere il supporto delle autorità.

Le PMI vittime di questi attacchi si trovano quindi spesso a soppesare compromessi impossibili.

Da un lato, pagare i criminali li incoraggia a continuare le loro attività criminali. Dall'altro, pagare il riscatto può essere l'unico modo per impedire agli aggressori di far trapelare i dati ed evitare la divulgazione pubblica della violazione, che può avere conseguenze dolorose.

scontri che accordi. Inoltre l'accelerazione dell'Intelligenza artificiale è imprevedibile e certamente porterà sul tavolo nuove possibilità di attacco e di difesa del tutto imprevedibili a priori.

Guardando la situazione più dall'alto, in un certo senso la disponibilità di moltissimi dati di tipo diverso (dal sensore al video), analizzati da una grande varietà di software diversi per fini e tecnologia, ha reso necessario lo sviluppo di una capacità di analisi che prescindesse dal tipo di dato e dal tipo di software. I sistemi di sicurezza attuali compiono molte operazioni grazie all'equivalente di una chat in linguaggio naturale che permette ad un esperto di sicurezza di fare analisi senza che si debbano conoscere i dettagli implementativi. Molte di queste funzioni sono automatizzate.

Ovviamente questa tecnologia è disponibile anche ai cybercriminali, che realizzano per sé sistemi avanzati di crime-as-a-service. Chiaramente il 2024 dovrà mostrare una capacità del mondo libero di sviluppare sistemi di prevenzione e controffensiva molto più potenti di quelli dei criminali. Tutto sommato, il mondo libero ha una potenza tecnica ed economica molto maggiore di quella dei criminali.

Vishing: proteggiamoci dai Deepfake

Una tecnologia che sempre di più sconfina nella cybersecurity è il contrasto ai deepfake. Ad imma-

gini e testi perfetti ma falsi siamo abituati, ma agli audio e ai video ancora no. Si chiede quindi all'Intelligenza artificiale di approntare dei sistemi che scoprono un falso, evitando problemi che possono essere insormontabili.

Nel 2022 il vishing, ovvero il voice phishing, è aumentato di percentuali spaventose.

Già tra il 2022 e il 2021 l'aumento era stato del 550% secondo alcuni report, tanto da scavalcare il volume delle truffe via email e diventare la principale minaccia per le aziende.

Sono queste le tecnologie che dovrebbero caratterizzare la cybersecurity nel 2024, in attesa che se ne presentino altre.

Non temete, non mancheranno novità né sorprese.



GLI APPROFONDIMENTI
DI BIZZIT



SentinelOne vede un 2024 positivo per gli investimenti in cybersecurity

Per Paolo Cecchi di SentinelOne, l'AI sarà un nuovo strumento nelle mani degli hacker e apre nuovi scenari, fondamentale continuare a investire in sicurezza

[+ continua a leggere](#)

Contrastare il ransomware con la cyber resilienza

di Riccardo Florio

A 10 anni dalla sua comparsa, il ransomware rimane la minaccia IT più significativa per le Pmi, mentre i gruppi di criminali informatici continuano a fare evolvere le loro tattiche. Una risposta efficace risiede nell'adottare un approccio indirizzato alla cyber resilienza come quello suggerito da OpenText Cybersecurity



Pierpaolo Ali
Director Southern Europe, France, Belgium
& Luxemburg di OpenText Cybersecurity



Il ransomware rappresenta un “modello di business” di grande successo per i criminali informatici e rimane la minaccia informatica più significativa per le piccole e medie imprese.

I gruppi ransomware continuano a sperimentare e a far evolvere le loro tattiche in un panorama di minacce in continua evoluzione. Secondo i dati del **Cybersecurity Threat Report 2023 di OpenText Cybersecurity** (che si basa su 95 milioni di sensori reali) l'84% degli attacchi ransomware include minacce di data leakage e un numero crescente di gruppi di criminali informatici sembra rinunciare completamente alla cifratura, limitandosi a rubare i dati e a minacciare di pubblicarli.

Piuttosto che cifrare i file violati, diventa preferibile inviare alle vittime “screenshot” dei dati riservati come prova dell'avvenuta violazione, tentando di estorcere pagamenti. Questa strategia elimina la necessità di disporre di com-

petenze in materia di cifratura, di archiviazione e gestione delle chiavi di decifrazione e della capacità di distribuire il malware per la cifratura dei file attraverso l'intera infrastruttura dell'azienda target.

Una violazione dei dati può danneggiare significativamente la reputazione di un'azienda nei confronti dei propri clienti, a volte in modo così irreparabile che l'azienda potrebbe non sopravvivere. Inoltre, le autorità di controllo potrebbero multare le aziende che non hanno protetto i dati dei loro clienti; in alcuni casi, l'importo delle multe è più alto del riscatto e quindi l'effetto ottenuto è quello di incentivare le vittime a ricompensare gli aggressori pagando il riscatto.

"Il danno per le vittime è doppio - spiega Pierpaolo Alì, Director Southern Europe, France, Belgium & Luxembourg di OpenText Cybersecurity - poiché il costo della mancata conformità alle normative sulla privacy dei dati e il danno al brand possono essere ancora più devastanti delle interruzioni causate dal ransomware. Per questo motivo molte aziende sono portate a ritenere più conveniente la scelta di pagare il riscatto e nascondere l'intero incidente".

I metodi di ransomware si evolvono e la crittografia diventa più veloce

La maggior parte dei ransomware continua a diffondersi attraverso attacchi malware a più livelli. Nella maggior parte dei casi, il malware viene trasmesso attraverso campagne di phishing: nella prima fase,

l'utente viene indotto a cliccare su un allegato o un link dannoso, che infetta il computer con un client botnet che fornisce all'aggressore capacità di comando e controllo. Nella fase successiva, l'aggressore sfrutta il client botnet per installare un malware che gli consente di spostarsi e di effettuare ricognizioni all'interno dell'organizzazione prima di infettare l'ambiente con un ransomware. Anche lo sfruttamento delle vulnerabilità senza patch resta un veicolo molto importante. I cybercriminali utilizzano sempre più frequentemente tattiche di **trippla estorsione, in cui la cifratura dei dati viene combinata con la "data leakage" e gli attacchi DDoS** (Distributed Denial of Service) per aumentare la pressione sulla vittima.

Il Cybersecurity Threat Report 2023 di OpenText Cybersecurity evidenzia anche l'aumento delle tecniche di **Living off the Land (LotL)**, in cui gli attori delle minacce approfittano di applicazioni innocue per eseguire payload dannosi camuffati da processi legittimi. Un'altra tecnica che sta crescendo in popolarità è il side-loading DLL, in cui gli aggressori eseguono librerie DLL dannose dall'interno di applicazioni legittime e affidabili, spesso con privilegi di sistema elevati.



GUARDA IL VIDEO SULL'APPROCCIO DELLA CICALA E DELLA FORMICA PER GESTIRE I DATI SENSIBILI.


Un'ulteriore diversificazione riguarda l'uso di **nuovi linguaggi di programmazione, come Rust e Go**, che possono rendere più difficile il rilevamento dei file e facilitare la compilazione del malware in modo che venga eseguito su sistemi operativi o piattaforme diverse. Una conseguenza è che i ransomware non si concentrano più esclusivamente sul sistema operativo Windows ma **si estendono anche su Linux**. Il cybercriminale si sta anche concentrando per sviluppare **malware in grado di cifrare i file a velocità record**. In tal modo, il tempo che intercorre tra la penetrazione iniziale in un ambiente e la completa compromissione si riduce da settimane a giorni o addirittura ore e può risultare quasi impossibile per i difensori impedire la cifratura su larga scala.

OpenText Cybersecurity contrasta il ransomware con la cyber resilienza

In uno scenario in cui il ransomware può infettare i sistemi in molti modi diversi e gli attaccanti continuano a diversificare le loro tecniche, anche le organizzazioni con programmi di gestione delle vulnerabilità eccezionalmente accurati non possono aspettarsi di evitare per sempre ogni compromissione. *“Questo non significa che sia inutile provarci - spiega Pierpaolo Alì - ma che bisogna spostare l'attenzione sulla resilienza informatica, non solo sulla prevenzione. La resilienza informatica implica l'adozione di misure per evitare gli attacchi, preparando, al contempo, la*

*propria organizzazione a rispondere agli attacchi ransomware che sfuggono alle maglie della rete. Gli aggressori di ransomware possono spesso violare singoli livelli ma di solito non tutti contemporaneamente. **Combinando tatticamente più livelli di protezione è possibile ridurre significativamente il rischio che un attacco di questo tipo abbia successo**”.* Una strategia di sicurezza multilivello richiede che i team di sicurezza predispongano **un solido piano di risposta agli incidenti**, in modo da poter agire rapidamente per bloccare la diffusione di un'infezione iniziale. Inoltre, serve **sviluppare e testare costantemente le capacità di backup**, in modo da essere sicuri di poter ripristinare i sistemi e i dati critici in tempo per proteggere la continuità delle operazioni. Infine è essenziale **rivalutare regolarmente il piano di resilienza IT** per assicurarsi che sia sempre adatto a fronteggiare le nuove minacce.

“Dal punto di vista delle soluzioni non bastano le applicazioni di data protection - conclude Alì - ed è per questo che OpenText Cybersecurity mette a disposizione un'ampia gamma di soluzioni software per la cyber resilienza, concepite per preparare le diverse tipologie di organizzazione a fronteggiare un attacco ransomware. L'offerta di OpenText Cybersecurity mette a disposizione gli strumenti appropriati per indagare e scoprire i punti deboli e le vulnerabilità e per assicurare che il team di sicurezza sia costantemente preparato e disponga delle competenze necessarie per utilizzare tali strumenti in caso di emergenza.”



La potenza dell'XDR per affrontare le nuove sfide di sicurezza

di Riccardo Florio

Attraverso la Unified Security Platform e la soluzione XDR ThreatSync, WatchGuard mette a disposizione gli strumenti per fronteggiare le sfide odierne di sicurezza, inclusi gli attacchi fileless e le minacce interne

Le soluzioni per la sicurezza di rete e quelle di rilevamento e risposta per gli endpoint (EDR, dall'inglese Endpoint Detection and Response) rappresentano due pilastri fondamentali nella strategia di sicurezza informatica di oggi ma ciascuna, singolarmente, presenta alcuni limiti intrinseci legati a una visibilità limitata a specifiche aree dell'infrastruttura IT.

Le tecnologie di sicurezza di rete, tra cui i firewall e i sistemi per il rilevamento di intrusioni, sono infatti fondate su una concezione tradizionale del perimetro e si focalizzano sulla protezione

dei punti di ingresso e uscita della rete, controllando il flusso di dati ai margini della stessa. Tuttavia, con l'affermazione delle tecnologie mobili e la diffusione del modello di lavoro ibrido, il confine della rete è diventato più dinamico e suscettibile a rischi, rendendo più complessa l'implementazione di misure di sicurezza efficaci. Questa evoluzione ha evidenziato i limiti di tali strumenti, che non riescono a fornire una visibilità completa degli endpoint.

Gli strumenti di EDR si rivelano essenziali per identificare e contrastare le minacce presenti sui dispositivi connessi alla rete ma, se utilizzati in modo isolato, non sono in grado di fornire una panoramica completa sulle minacce emergenti negli ambienti di rete sempre più diversificati che includono anche il cloud.

In assenza di un approccio unificato le aziende si trovano con una limitata la visibilità sull'intero ambiente, che impe-

disce di contestualizzare correttamente gli eventi di sicurezza e riduce l'efficacia nel rilevamento e nella risposta.

Il valore dell'XDR

Le soluzioni XDR (eXtended Detection and Response) estendono le capacità di rilevamento e risposta alle minacce su più domini di sicurezza che includono endpoint, reti, cloud e identità fornendo, nel contempo, una visione più semplice e unificata tramite una sola interfaccia. La capacità dell'XDR di raccogliere, aggregare e correlare automaticamente i dati provenienti da più prodotti di sicurezza consente di migliorare il rilevamento delle minacce e fornire funzioni di risposta agli incidenti. Utilizzando l'intelligenza artificiale e il machine learning, **l'XDR esegue un'analisi automatica per integrare i dati di sicurezza all'interno di un sistema di sicurezza** centralizzato per fornire una visione unificata degli incidenti che consenta azioni correttive più rapide. L'obiettivo principale di una soluzione XDR è, dunque, quello di aumentare il livello di accuratezza del rilevamento e di migliorare l'efficienza e la produttività delle attività di sicurezza.

È bene sottolineare che XDR non si limita a rilevare possibili attacchi sulla base delle signature, ma è in grado di monitorare i singoli sistemi IT per identificare eventuali anomalie rispetto al normale comportamento del sistema. Mediante l'uso dell'AI è possibile rilevare efficacemente attacchi fileless, attacchi

rootkit o minacce persistenti avanzate (APT) attraverso l'analisi combinata delle azioni effettuate su un sistema IT che, prese singolarmente potrebbero sembrare innocue e legittime ma nel loro insieme possono indicare che c'è un attacco in corso. Inoltre, l'XDR permette di ridurre le vulnerabilità legate agli errori umani e i falsi positivi nonché di favorire azioni di difesa semi-automatizzata da attacchi avanzati. Uno dei vantaggi principali di XDR è anche quello riuscire a rilevare i cyberattacchi prima che raggiungano gli endpoint attraverso la ricerca di indicatori di compromissione (IoC). L'XDR è chiamato anche a garantire la protezione dell'identità e ad affrontare i rischi associati, grazie a funzionalità progettate per rilevare e rispondere a questi specifici attacchi.

La piattaforma di sicurezza unificata di WatchGuard e ThreatSync

Per fornire a organizzazioni e Managed Service Provider un'unica piattaforma per semplificare e rafforzare ogni aspetto dell'utilizzo, della fornitura e della gestione della sicurezza, **WatchGuard ha sviluppato la Unified Security Platform**. La piattaforma di sicurezza unificata di WatchGuard rappresenta un'evoluzione nel campo della sicurezza informatica, che supera i confini di un insieme tecnologico, un programma per i partner e un sistema di gestione. Questa piattaforma incarna, infatti, l'idea che le soluzioni di sicurezza debba-

no essere perfettamente integrate con le metodologie basate sul modello as-a-service.

Un tassello importante incluso nell'architettura Unified Security Platform di WatchGuard è **ThreatSync, la soluzione XDR** completa e di semplice utilizzo che unifica i rilevamenti di più prodotti e accelera la risposta alle minacce attraverso un'unica interfaccia di controllo.

La soluzione sfrutta le funzionalità WatchGuard di sicurezza della rete ed EDR per fornire avvisi incrociati, che sono raccolti e trasformati in informazioni fruibili in tempo reale per una gestione della sicurezza end-to-end. ThreatSync permette anche di aiutare le aziende a identificare le aree di miglioramento e affrontare in modo proattivo le potenziali vulnerabilità.

ThreatSync si distingue per le seguenti caratteristiche:

- **Rilevamento delle minacce multiplatforma.** ThreatSync fornisce ampie funzionalità di rilevamento utilizzando gli indicatori di compromissione (IoC) provenienti da tutti i prodotti di sicurezza WatchGuard e mettendo tali indicatori in relazione tra loro. Tale correlazione e tale contesto multi-dominio consentono alla soluzione di rilevare e classificare le attività potenzialmente dannose relative a specifici ambienti, utenti e dispositivi per ridurre il tempo medio di risposta, migliorare l'accuratezza e, infine, permettere una più rapida risoluzione dei problemi di sicurezza.
- **Orchestrazione della sicurezza unificata e risposta alle minacce.** Fornendo agli amministratori della sicurezza e dell'IT una visione completa e integrata della superficie di attacco, ThreatSync consente di eseguire facilmente analisi complesse e predisporre una risposta efficace e rapida. ThreatSync consente di lavorare in modo più efficiente con una classificazione "smart" degli avvisi, policy di correzione automatizzate e opzioni per l'intervento manuale se necessario. Questo livello di orchestrazione della risposta alle minacce aumenta sia la portata sia la precisione con cui i team di sicurezza rispondono ai problemi.
- **Semplicità di implementazione e gestione.** Grazie a funzionalità di gestione e automazione intuitive e basate su cloud, WatchGuard ThreatSync facilita l'adozione dell'approccio XDR, specialmente in quei contesti dove il tempo e le competenze scarseggiano. Fornendo funzionalità XDR all'architettura Unified Security Platform di WatchGuard, ThreatSync integra l'intelligence tra i vari prodotti per ridurre i costi e gli oneri di gestione legati all'implementazione di più soluzioni specifiche per il rilevamento e la risposta alle minacce.

RIMANI AGGIORNATO
ISCRIVITI ALLA NEWSLETTER





Massimiliano Galvagna



L'80% delle risorse di detection viene dedicata a tecniche, tattiche e procedure degli attaccanti: a colloquio con **Massimiliano Galvagna**, country manager per l'Italia di Vectra AI

Vectra AI: sconfiggere i falsi positivi senza andare in cloud

di **Leo Sorge**

La Vectra AI Platform affronta la spirale del più: più superficie di attacco, più sofisticazione dei metodi di attacco, più strumenti, più regole, più burnout degli analisti di sicurezza. In un periodo nel quale la geopolitica è al centro del mondo, certamente la consapevolezza sui rischi di attacchi cibernetici è maggiore rispetto al passato.

Ne abbiamo parlato con **Massimiliano Galvagna**, country manager per l'Italia di Vectra AI.

“Stiamo lavorando molto nel settore militare e governativo. Siamo una delle poche tecnologie in grado di fare analisi al 100% on premises, quindi senza mandare alcunché in cloud” spiega Galvagna. Questo aspetto è estremamente importante sul lato militare, dove *“Vectra AI ha già delle collaborazioni importanti: lavoriamo anche con Leonardo”*.

Il falso positivo è un forte overhead

Una delle chiavi della risposta agli attacchi è la precisione: l'alto volume di falsi positivi è un overhead per il Soc. Vectra AI Platform abbassa drasticamente il numero di falsi positivi. *“Un elemento che ci differenzia è l'approccio - riprende il country manager -. Noi siamo presenti sul mercato da oltre dieci anni quindi la nostra tecnologia è molto matura. La maggior parte dei concorrenti si focalizza sul rilevare ciò che si discosta da una baseline, il consueto lavoro dell'utente: questo può portare a rilevare qualcosa di malevolo ma può anche rilevare molti falsi positivi”*.

Vectra dunque punta l'anomalia. *“Che io sappia, Vectra AI ha l'unica tecnologia sul mercato che usa algoritmi di intelligenza artificiale per rilevare tecniche, tattiche e procedure di attacco - spiega Galvagna -; quando noi scattiamo su un alert magari non*

DECRIPTARE I PAYLOAD NON È UN VANTAGGIO

Sempre di più la cybersecurity richiede l'efficacia della decrittazione nel rilevare attacchi cibernetici avanzati, come i nation state e i RansomOps manuali. Un'analisi di Alessio Mercuri, Security Engineer di Vectra, entra in dettaglio su alcune informazioni. La decrittazione dei payload dei pacchetti è spesso vista come un aiuto, ma in realtà non lo è. La decrittazione, passiva o attiva, è operativamente costosa e non offre vantaggi significativi nella tracciatura del canale C2 di un attaccante o nell'esfiltrazione dei dati. In particolare, gli attacchi nation state usano strumenti altamente personalizzati e configurati diversamente per ogni obiettivo, rendendo inefficace la decrittazione.

Anche gli attacchi RansomOps, essendo manuali e spesso modificati per evitare la rilevazione, non beneficiano significativamente della decrittazione. In entrambi i casi, la decrittazione non migliora sostanzialmente le capacità di rilevamento degli attacchi avanzati.

rileviamo una vera anomalia da rischio, ma solo il diverso comportamento di un utente”.

La costruzione di una baseline per il comportamento degli utenti, che per molti è l'attività principale o esclusiva, per Vectra rappresenta il 20% della detection; *“il restante 80% è dedicato alla ricerca di tecniche, tattiche e procedure degli attaccanti, un'attività che ci permette di individuare le reali compromissioni con grande precisione”*, riducendo i falsi positivi e quindi i costi di gestione.

L'Attack Signal Intelligence della Vectra AI Platform offre rilevamento e una risposta (XDR) agli attacchi ibridi, in velocità e su scala. *“L'enorme crescita del multi-cloud hanno reso più complessa la sfida della sicurezza per la maggior parte delle imprese moderne - interviene*

Paolo Lauretti, Regional partner manager per il Sud Europa - Vectra AI rimane focalizzata al 100% sul canale, dove stiamo registrando una crescita di oltre il 100% su base annua, con segnali incoraggianti per il 2024”.

Formazione ok in azienda e nella PA

Medie e grandi imprese in Italia fanno molta formazione e a un livello adeguato alle necessità. *“Sulle medio-grandi imprese, sicuramente c'è molta competenza e in percentuale direi che ci avviciniamo all'80% delle competenze necessarie: nei Soc ci sono analisti davvero molto formati, lo vediamo in tutti i settori dal telco al bancario, all'energy-oil-gas”.*

La formazione è buona, ma attira un numero ridotto di futuri esperti. Anche per questo, “i Soc sono sotto-staffati”. La formazione è adeguata per perseguire il day by day, ma “quando c'è un grosso incidente, tipicamente vengono ingaggiate delle aziende esterne”. Parlando invece del settore pubblico, in particolare della PAL, *“i fondi del PNRR sicuramente sono serviti ai Comuni, che li stanno investendo proprio sulle nuove tecnologie: stiamo lavorando con grossi player di mercato o di canale proprio verso tutti quei piccoli Comuni che non potrebbero attrezzarsi per comprare la nostra tecnologia”.*



**GLI APPROFONDIMENTI
DI BIZZIT**



In Maire, Vectra Ai fa diventare la sicurezza proattiva

La soluzione di Vectra Ai consente al Cyber Fusion Center di Maire di scoprire un attacco nel giro di pochi minuti e di intervenire di conseguenza per contrastarlo



continua a leggere

IT-OT: l'integrazione che guida l'industria 4.0

La convergenza tra tecnologie operative e IT è fondamentale per realizzare gli obiettivi dell'industria 4.0, e sviluppare nelle imprese manifatturiere resilienza, efficienza e innovazione, nonostante le sfide tecnologiche e organizzative.

di Mercedes Oledieu

“La trasformazione richiede convergenza”, ricorda la società di consulenza **Capgemini**, e questo è il caso di IT e OT. Tecnologia dell'informazione (IT) e tecnologia operativa (OT) rappresentano domini tradizionalmente distinti, ma oggi sempre più convergenti, per chiudere il cerchio della trasformazione digitale, e completare un lungo percorso di evoluzione e innovazione che promette di trarre dal paradigma Industria 4.0 i massimi benefici di business.

Da M2M a Industrial IoT, come cambia l'architettura di comunicazione

Con Industria 4.0, i computer, dispositivi, sensori, attuatori che controllano macchinari nei processi manifatturieri, da “standalone”, indipendenti, diventano connessi in rete, e in grado di comunicare tra loro.

Un esempio è la comunicazione machine-to-machine (M2M), che consente lo scambio di dati tra macchine, e l'attuazione di operazioni, senza intervento umano. Tale tecnologia ha molta storia alle spalle, ma è comunque in conti-

SCARICA IL DOCUMENTO
DI CAPGEMINI



nua transizione: dai classici sistemi M2M, generalmente confinati in ambienti di fabbrica o impianti isolati, disconnessi da Internet, e collegati tra loro tramite connessioni dirette punto-punto (P2) su reti wired o wireless, si sta progressivamente migrando verso architetture di networking e applicazioni molto più distribuite ed estese, in cui gli elementi predominanti, e gli anelli di congiunzione con l'IT, sono la **Industrial Internet of Things** (IIoT), il cloud, i sensori, attuatori e dispositivi di campo "intelligenti", le connessioni multipunto, la tecnologia 5G, l'integrazione di 5G con il time-sensitive networking (5G-TSN). Industria 4.0 prevede infatti un percorso di implementazione che va oltre la comunicazione tra macchine nell'ambiente di fabbrica. Per compiersi pienamente, e concretizzare scenari applicativi come le smart factory e lo smart manufacturing, questa quarta rivoluzione industriale innescata da Industria 4.0 richiede necessariamente una sempre più profonda integrazione con i

sistemi IT che governano i processi di business. Per ridurre la latenza nei processi collaborativi di progettazione, fabbricazione, quotazione, spedizione dei prodotti, la società di ricerca e consulenza **Forrester** consiglia ai decisori dell'industria manifatturiera di colmare il divario tra i sistemi IT, nei propri uffici, e i sistemi OT, che popolano fabbriche, magazzini, laboratori.

SCARICA LA GUIDA
PRATICA PER COLMARE
IL DIVARIO IT/ OT DI
FORRESTER



Convergenza IT-OT, un percorso ineludibile per le imprese manifatturiere

Far convergere il mondo OT con il mondo IT significa **integrare le attrezzature di automazione e controllo dei dispositivi, macchinari, impianti, infrastrutture di produzione industriale, con i sistemi informativi e i data center aziendali.**

Questa integrazione tra ambiente fisico e digitale dà origine a **sistemi cyberfisici** (CPS) che, sul versante realizzativo, aprono la strada a tutta una serie di nuove sfide tecnologiche e di riorganizzazione dei processi, a vari livelli.

Valutando però i benefici, tali sistemi risultano cruciali per riuscire a compiere un nuovo salto di qualità sul piano della produttività e dell'efficienza di gestione delle imprese manifatturiere, e anche per sviluppare nuovi modelli di business.



L'APPROFONDIMENTO



WHITE PAPER

Integrazione del 5G con il Time-Sensitive Networking per le comunicazioni industriali



continua a leggere

Resilienza operativa e “product servitization”

In primo luogo, le emergenze sanitarie, le guerre, le tensioni geopolitiche hanno ampiamente dimostrato di generare turbolenze economiche e incertezza nei mercati globali, in grado di causare contraccolpi ed effetti devastanti sul funzionamento di supply chain ormai palesemente fragili da tale punto di vista.

La mancanza di adeguata capacità previsionale e visibilità sulle variazioni di disponibilità di materie prime e componenti nelle catene di fornitura, sui relativi prezzi, sui costi dei trasporti e delle operazioni logistiche, mette seriamente a rischio la sopravvivenza delle aziende di produzione, per le quali diventa più che mai **prioritario potenziare la resilienza operativa**, attraverso una più profonda digitalizzazione e interconnessione della tecnologia e dei processi OT con i sistemi IT. Riuscire a rendere la capacità produttiva più agile e flessibile in rapporto alle dinamiche della domanda diventa insomma un imperativo categorico per continuare a competere in scenari imprenditoriali sempre più complessi e difficili.

In secondo luogo, sul piano dei modelli di business, anche per il settore manufacturing sembra davvero finito il tempo in cui il prodotto è l'elemento preponderante dell'offerta che differenzia un'azienda da un'altra. La “servitizzazione” della manifattura si esprime oggi in modelli di commercializzazione e cre-

azione del valore che, assieme al prodotto, al macchinario industriale, offrono all'utente finale tutta una serie di sofisticati servizi digitali, indirizzati a **personalizzare e ottimizzare di continuo l'utilizzo e il funzionamento del macchinario** stesso, sfruttando il potenziale di Intelligenza artificiale (AI), apprendimento automatico (Machine learning - ML), Digital twin (DT). Ad esempio, acquisendo i dati generati dai dispositivi di campo e rilevati dai sensori IoT smart connessi alle attrezzature di fabbrica, le piattaforme Industrial IoT (IIoT) “edge-to-cloud” sono in grado di analizzare dati storici e real-time, ed elaborare **algoritmi di manutenzione predittiva** che aiutano a ottimizzare i piani d'intervento, riducendo i tempi di inattività delle linee di produzione e il numero di downtime imprevisti.

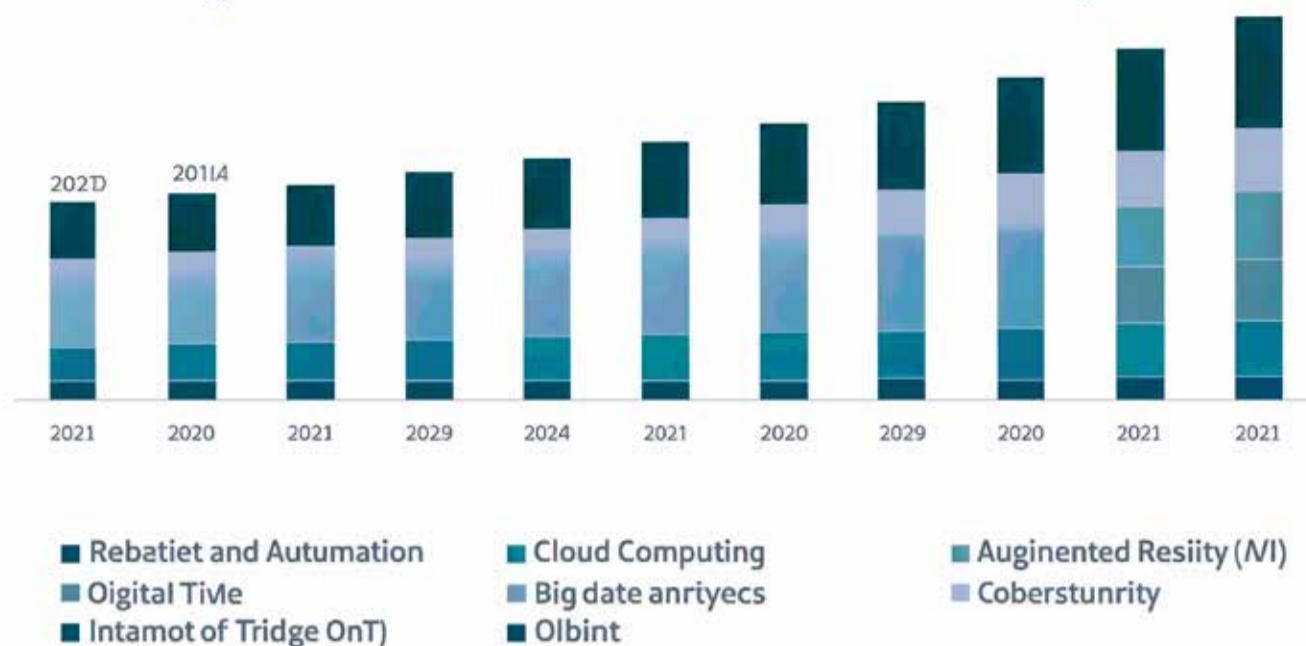
Industria 4.0 e tecnologia operativa, OT e IT sempre più integrate

Valutato 114,3 miliardi di dollari nel 2023, il mercato globale Industria 4.0, stando alle stime della società di ricerche Global Market Insights (GMI), è previsto raggiungere 555,1 miliardi di dollari nel 2032, crescendo con un CAGR (tasso annuo di crescita composto) pari al 20,2% nel periodo della previsione (2024 - 2032).

SCARICA IL REPORT
GLOBAL MARKET
INSIGHT



Mercato globale di Industria 4.0 (fonte: Global Market Insights)



In Italia, secondo i più recenti dati dell'Osservatorio Transizione Industria 4.0 del Politecnico di Milano, nel 2020 il comparto Industria 4.0 ha raggiunto un valore di 4,1 miliardi di euro, con una crescita dell'8%, trainata soprattutto dalle tecnologie IT, che rappresentano l'85% della spesa, contro il 15% delle tecnologie OT (operational technology). Gli investimenti delle imprese manifatturiere, indica lo studio, si sono concentrati soprattutto su

ca e consulenza **Virtue Market Research**, passerà, dai 96,34 miliardi di dollari del 2022, a 280,66 miliardi di dollari entro il 2030, con un CAGR del 14,3% (2023 - 2030). Tra i fattori che guidano la continua integrazione IT-OT, lo studio pone in primo piano la riduzione dei costi, attraverso la capacità di massimizzare l'uso delle risorse e dell'energia, controllando e monitorando con precisione questi complessi sistemi in maniera più diretta. Senza dimenticare che l'abilità di analizzare dati IT-OT su scala geografica, e ottenere insight in tempo reale, può aiutare, specie i dirigenti e manager di multinazionali in industrie come quella manifatturiera, mineraria, petrolifera, o dei trasporti, a migliorare l'efficienza delle operazioni OT-IT aziendali e dei processi decisionali.

SCARICA IL REPORT
DI VIRTUE MARKET
RESEARCH



progetti di connettività e acquisizione di dati. Ciò fa comprendere quanta strada nel nostro paese resti ancora da percorrere per una più sostanziale integrazione dei sistemi OT con le applicazioni IT.

Il trend globale di crescente convergenza IT-OT è tuttavia testimoniato dall'espansione del comparto OT che, secondo la società di ricer-

Tecnologia OT, le molte sfide d'integrazione e digitalizzazione

Va subito chiarito che, per determinare un impatto positivo sul business, le iniziative d'integrazione

OT-IT non possono limitarsi alla mera implementazione tecnologica, ma implicano la riorganizzazione di processi, procedure di lavoro, l'attuazione di strategie di formazione e change management orientate a trasformare la cultura e la mentalità del personale nello svolgimento delle varie mansioni. Ciò detto, la convergenza di questi due domini tecnologici si rivela generalmente complessa da attuare, principalmente a causa delle **differenze che contraddistinguono la tecnologia OT rispetto all'IT.**

Attrezzature e sistemi OT includono dispositivi di campo e dispositivi di controllo, tra cui sensori, attuatori, PLC (Programmable logic controller), PAC (Programmable automation controller), SCADA (Supervisory control and data acquisition), ICS (Industrial control system), DCS (Distributed control system), dispositivi HMI (Human-machine interface). Monitorando e controllando il funzionamento di linee di produzione, impianti e delicati processi industriali, per ragioni di sicurezza, i sistemi OT, storicamente, nascono "air-gapped", per restare **fisicamente isolati dai sistemi IT.**

I sistemi OT sono caratterizzati da tecnologia legacy, con un ciclo di vita lungo anche decenni, difficilmente concepibile per chi opera nell'amministrazione di sistemi e attrezzature IT.

Le applicazioni OT sono costituite da **sistemi embedded** e apparati hardware-software sviluppati ad hoc per eseguire funzioni specifiche. Si tratta di attrezzature e dispo-



GLI APPROFONDIMENTI
DI BIZZIT

Innovazione e opportunità nell'Industria 4.0: gli insight dell'Osservatorio Lectra

Lectra presenta l'Osservatorio dell'innovazione e della trasformazione nei settori fashion, arredamento e automotive: "La crescita dell'Industria 4.0 aumenta l'efficienza produttiva"

[+ continua a leggere](#)

sitivi "rugged", dotati di particolare robustezza, adatti a operare con elevata disponibilità e affidabilità nel tempo in ambienti industriali difficili, dove le condizioni estreme di temperatura, umidità, vibrazioni, polvere, sporcizia, interferenza elettromagnetica (EMI) danneggerebbero i computer e server ordinari, tipicamente installati in uffici e data center climatizzati.

A livello di networking, i sistemi OT eseguono le funzioni di automazione e controllo comunicando attraverso una **varietà di protocolli industriali** (Modbus, CIP, CC-Link, Profinet, EtherCAT), spesso per gestire processi "mission-critical" e "safety-critical".

Questi ultimi, a differenza dei processi e delle applicazioni IT, si concentrano soprattutto su affidabilità e sicurezza fisica delle infrastrutture, richiedono **requisiti di funzionamento real-time** (hard real-time o soft real-time) e un **comportamento deterministico** del sistema.

Dalla necessità di coordinamento, ai crescenti rischi di cybersecurity

L'eterogeneità tecnologica esistente tra OT e IT, i differenti requisiti che tali applicazioni devono soddisfare, l'utilizzo di diversi strumenti di amministrazione, l'esistenza di silos informativi nei vari reparti, non facilitano la collaborazione tra team dei due domini e, tantomeno, il raggiungimento di **una visione e una data governance olistica sulle operation aziendali**. L'integrazione infrastrutturale può richiedere l'introduzione di nuovi tool per l'acquisizione e l'analisi unificata dei dati OT e IT, l'aggiornamento dell'hardware OT datato con nuovi dispositivi e componenti, per consentire la comunicazione con l'IT e il cloud attraverso connessioni wired o wireless.

Oltre a tutto ciò, per rendere affidabile la convergenza IT-OT, e creare nuovo valore di business, indica uno studio di settore di **Info-Tech Research Group**, la sfida cruciale da affrontare resta la cybersecuri-

ty. L'integrazione della tecnologia OT nella sfera IT aumenta notevolmente le potenziali vulnerabilità, e la superficie esposta a minacce e attacchi cibernetici di varia natura. Un fattore aggravante è poi il fatto che un'azione di hacking su un sistema cyberfisico può determinare conseguenze ben più gravi rispetto a quelle che può subire un'infrastruttura IT: si pensi, ad esempio, agli impatti causati dai crescenti e recenti attacchi perpetrati a danno di varie categorie di infrastrutture critiche, come quelle di [Colonial Pipeline](#).

La natura legacy dei sistemi OT rende problematica la comunicazione con i moderni protocolli e tool di gestione della sicurezza IT, riducendo anche la visibilità sugli endpoint OT connessi.

In aggiunta, spesso l'hardware OT è basato su firmware e software non originariamente progettato per la connessione Internet e la protezione da attacchi cibernetici. I processi, le regole, le politiche di security dell'OT sono differenti da quelli dell'IT: ad esempio, le pratiche di applicazione delle patch di correzione delle vulnerabilità, comuni nel mondo IT, sono spesso inapplicabili sui sistemi e le attrezzature OT.

L'applicazione di patch o modifiche della configurazione può infatti causare malfunzionamenti, o richiedere downtime non tollerabili nella tecnologia operativa, che regola l'automazione e il controllo del delicato funzionamento di processi e applicazioni industriali.



L'APPROFONDIMENTO



STUDIO

La complessa sfida della sicurezza nella convergenza dei sistemi IT-OT



continua a leggere



Market review

Protezione degli endpoint:
EDR, XDR, MDR

Soluzioni per la protezione degli endpoint: EDR, XDR, MDR

La violazione degli endpoint rappresenta il veicolo principale per lanciare attacchi e sottrarre dati. Le soluzioni per la protezione degli endpoint sono di diversi tipi e permettono di individuare minacce avanzate e predisporre azioni di risposta efficaci, sfruttando anche le tecnologie innovative di intelligenza artificiale.

di Riccardo Florio

L'evoluzione delle modalità di lavoro e degli strumenti informatici ha fatto in modo che, attualmente, il 70% di tutte le violazioni abbiano origine nell'endpoint. Per scongiurare la sottrazione di dati o il blocco dell'operatività diventa quindi essenziale per i team IT riuscire ad aumentare la capacità di analisi e di avviare azioni di rimedio da remoto. Le soluzioni per la protezione degli endpoint sono in rapida evoluzione ed è importante capire come si articolano le differenze funzionali, soprattutto quando le termino-

logie utilizzate variano da fornitore a fornitore.

Endpoint detection and response (EDR)

L'Endpoint detection and response (EDR) rappresenta un significativo passo in avanti rispetto alle tradizionali soluzioni antivirus concentrandosi, appunto, sulle attività di rilevamento e risposta. Spesso, infatti, i cyber criminali puntano a compromettere un desktop, un laptop, uno smartphone, un server o un altro endpoint per creare un punto d'appoggio all'interno della

rete dell'organizzazione presa di mira da cui partire per spostarsi ad altri endpoint e sottrarre più informazioni possibili.

Il metodo per la sicurezza degli endpoint è stato per molto tempo esclusivamente di tipo reattivo, individuando le potenziali minacce alla sicurezza attraverso la corrispondenza con le firme (signature) e i modelli di attacco noti.

Per proteggersi da queste attività dannose, l'EDR pone una priorità sul monitoraggio continuo e sulla scoperta delle minacce, prevedendo funzionalità di risposta automatica su ogni endpoint. **L'EDR adotta, invece, un approccio predittivo** focalizzandosi sull'identificazione di minacce persistenti avanzate e di malware sconosciuti, progettati per eludere le difese di sicurezza tradizionali. Per rilevare le minacce avanzate, la maggior parte delle soluzioni EDR sfrutta la potenza combinata dell'intelligenza sulle minacce, del machine learning e dell'analisi avanzata dei file.



GLI APPROFONDIMENTI
DI BIZZIT



Endpoint osservato speciale:
nel new normal, la sicurezza
parte dall'EDR



continua a leggere

Le soluzioni EDR registrano e memorizzano query, comportamenti ed eventi di sicurezza, consentendo ai team di cybersecurity di rilevare e analizzare le attività sospette. In caso di violazione o rilevamento, l'EDR conterrà il malware isolandolo e ne comprenderà il comportamento facendo agire il file compromesso all'interno di un ambiente protetto (per esempio, una sandbox). L'EDR contribuirà inoltre a condurre un'analisi approfondita delle cause e a velocizzare la risposta agli incidenti.

Tuttavia, solitamente, per rilevare l'attività nociva sul dispositivo un sistema EDR richiede l'installazione di un agente specifico. Inoltre, **non è in grado di fornire indicazioni su come gli aggressori potrebbero combinare endpoint infetti con altre attività dannose nel cloud**, identità utente compromesse o azioni in altre parti della rete, per lanciare un attacco organizzato in più fasi.

Inoltre, una configurazione errata di un ambiente EDR **può generare un gran numero di avvisi trasformando così l'attività di sicurezza informatica in una semplice gestione degli allarmi**, senza fornire la capacità di interagire in modo efficace con tali segnalazioni.

Extended detection and response (XDR): un passo in avanti

Il panorama delle minacce informatiche diventa sempre più sofisticato e gli attacchi oggi sfrutta-

no molteplici vettori in ambienti aziendali complessi.

Il software EDR monitora e registra l'attività sugli host, ma manca di un contesto più ampio che vada oltre gli endpoint.

L'extended detection and response (XDR) riunisce la telemetria di sicurezza delle piattaforme di sicurezza degli endpoint, dei firewall, dei gateway web, dei carichi di lavoro del cloud, dei sistemi di identità e altro ancora fornendo un livello più ampio di visibilità che si dimostra più adatto alla crescente complessità dei moderni ambienti IT.

Di conseguenza, espande il valore dell'EDR fornendo una visibilità più ampia e integrata, capacità di analisi delle anomalie di comportamento e funzionalità di risposta automatizzata che si estendono alle reti, ai carichi di lavoro "in-the-cloud" e oltre.

Le piattaforme XDR mirano ad abbattere i tradizionali silos di soluzioni di sicurezza, in modo che i team di sicurezza possano collegare più efficacemente i diversi eventi e contestualizzarli per scoprire le minacce più sofisticate e orchestrare azioni di risposta automatizzate.

Questi sistemi necessitano però di personale altamente qualificato (oggi merce rara), che deve avere le competenze per valutare correttamente i diversi aspetti di

una minaccia: dal suo contenuto al contesto, alle informazioni di identità, alla rete fino alla posta elettronica.

Centralizzare i dati sulla sicurezza migliora la capacità di rilevamento

Una capacità fondamentale delle soluzioni XDR consiste nel raccogliere e normalizzare i dati sulla sicurezza provenienti dall'intero stack tecnologico dell'infrastruttura aziendale. Centralizzando eventi, avvisi, metriche, analisi del comportamento degli utenti e altro ancora all'interno di un'unica piattaforma, **l'XDR fornisce le basi per applicare un'analisi migliore.**

La correlazione dei set di dati normalizzati consente anche di **identificare minacce o attività interne sospette** che verrebbero probabilmente ignorate analizzando gli eventi in modo isolato.

Per esempio, una compromissione dell'endpoint o un tentativo di intrusione nella rete, che di per sé non desterebbero sospetti, potrebbero essere messi in relazione con una modalità di accesso anomala a un database segnalata da un broker di sicurezza in cloud; il collegamento tra i due eventi potrebbe indicare una campagna di attacco in corso piuttosto che due anomalie isolate. Le soluzioni XDR sono progettate per **gestire queste indagini in modo automatico, invece di so-**



GLI APPROFONDIMENTI
DI BIZZIT

Internet Security Report:
attacchi a doppia estorsione
aumentati del 72%

 continua a leggere

vraccaricare i team operativi di sicurezza facendogli correlare manualmente gli eventi.

Unificando la risposta al rilevamento tramite un'unica piattaforma i team di sicurezza acquisiscono, così, maggiori capacità di individuare le minacce, isolare sistemi e utenti, limitare l'accesso alla rete, mettere offline gli endpoint infetti o rispondere in altro modo attraverso l'intero ambiente aziendale.

Accelerazione delle indagini e aumento della produttività

L'efficienza del flusso di lavoro introdotta da XDR è pensata specificamente per **aiutare i team di sicurezza che dispongono di risorse limitate** a essere più produttivi. L'integrazione tra i diversi livelli di sicurezza IT fornisce la storia completa delle minacce anziché prospettive parziali e l'analisi automatizzata delle cause profonde riduce, come già sottolineato, l'onere della gestione manuale degli avvisi.

Queste funzionalità consentono al personale di stabilire meglio le priorità delle indagini in base al rischio effettivo. Gli analisti possono dedicare meno tempo a ricomporre le "timeline" delle attività dei sistemi e degli utenti attraverso i diversi prodotti di sicurezza, mentre il machine learning supervisionato raggruppa gli avvisi correlati. In alcuni casi di utilizzo di XDR il **numero di avvisi che richiedono una revisione umana può essere ridotto fino al 90%**.

La sostituzione delle attuali solu-

zioni di rilevamento e risposta con soluzioni XDR integrate richiede però una certa attenzione. **Gli approcci di tipo "rip-and-replace" rischiano di provocare inconvenienti.** Un rollout graduale che si concentri prima sui punti critici più importanti, come la riduzione dei falsi positivi dei SIEM e dei firewall attuali o l'automazione delle routine di contenimento, può mostrare il valore dell'XDR.

L'erogazione di XDR in cloud riduce inoltre le barriere alla migrazione, poiché le modifiche all'infrastruttura sono minime.

Man mano che i team di rilevamento, "incident response", "threat hunting" e "IT forensics" si abituano a una visibilità più ampia e all'aumento dell'efficienza del flusso di lavoro, si crea lo slancio per espandere la portata dell'XDR. Anche se i risultati non si materializzeranno da un giorno all'altro, il guadagno a lungo termine che si ottiene andando oltre il rilevamento e la risposta limitati a un singolo vettore è sostanziale.



GLI APPROFONDIMENTI
DI BIZZIT

Cloud security al bivio: i dati sensibili aumentano, la protezione insegue

Lo studio 2023 Thales Cloud Security ha analizzato le sfide della sicurezza in cloud diventando lo standard di fatto per le infrastrutture e i servizi digitali moderni. Con Simone Mola, Regional Sales Manager di Thales, abbiamo analizzato i dati rilevati da questo studio.

 [continua a leggere](#)

Rilevamento e risposta gestiti (MDR)

Il panorama delle minacce si è notevolmente ampliato, con un maggior numero di controlli di sicurezza che generano migliaia di avvisi e quantità enormi di dati. Oltre all'analisi di questi dati, i team di sicurezza devono incorporare le informazioni sugli asset e sui rischi provenienti da tutta l'azienda per definire le priorità di risposta in base al potenziale impatto aziendale.

Molti team di sicurezza elaborano e correlano i dati manualmente, rendendo difficile la gestione del volume e della complessità.

Per questa ragione, molte organizzazioni si rivolgono a **fornitori di servizi di rilevamento e risposta gestiti (MDR) per trasferire le attività operative in modo che le risorse interne possano concentrarsi su iniziative più strategiche**. In questo modo i responsabili della sicurezza possono ottimizzare i loro programmi.

Casi d'uso comuni per i servizi MDR

L'MDR comprende un'ampia gamma di funzionalità di rilevamento e risposta personalizzabili che le organizzazioni possono applicare in base alle proprie esigenze e risorse. Anche se i fornitori possono differire, i servizi principali si concentrano spesso sul monitoraggio, l'identificazione e l'investigazione degli avvisi di sicurezza. Alcune organizzazioni scelgono di esternalizzare completamente le

operazioni di sicurezza, affidando al partner MDR l'intero stack tecnologico, i processi e le competenze. Altre utilizzano l'MDR come estensione delle operazioni di sicurezza interne, aggiungendo ulteriore visibilità o esperti.

L'MDR può avere un impatto positivo in relazione agli **aspetti di tipo operativo** perché consente di ridurre i costi legati all'infrastruttura, al personale e alla gestione. Inoltre, **risponde al problema della gestione di un eccesso di allarmi e dei falsi positivi e aumenta l'efficacia** poiché blocca gli attacchi più rapidamente e riduce i rischi, migliora il rilevamento e consente la ricerca proattiva delle minacce, rafforzando i controlli per prevenire attacchi futuri.

Scegliere il fornitore idoneo

Per affrontare il volume e la sofisticazione delle minacce moderne i principali fornitori di MDR stanno sfruttando tecnologie come l'intelligenza artificiale e gli analytics per far evolvere le loro offerte.

Nella scelta di un servizio MDR gestito alcune delle funzionalità che andrebbero ricercate sono:

- capacità di monitoraggio continuo con visibilità sulle attività sospette;
- raccomandazioni di rilevamento e risposta basate sull'intelligenza artificiale;
- disponibilità di rapporti di compliance;
- supporto diretto da parte di consulenti per la sicurezza;
- valutazioni delle vulnerabilità

e indicazioni per la mitigazione dei rischi.

Nella scelta di un fornitore di MDR le organizzazioni dovrebbero anche valutare la telemetria, l'intelligence sulle minacce, la capacità di individuare le minacce e di operare in ambienti cloud e ibridi.

MSSP contro MDR

In passato i servizi di sicurezza gestiti erano riconducibili al controllo delle modifiche, agli avvisi di sicurezza e alle escalation; con l'MDR la loro portata si è ampliata per includere anche le componenti di rilevamento e risposta.

La componente di "detection" gestita consiste nella gestione della ricerca delle minacce e utilizza gli strumenti di analytics e di threat intelligence per individuare i comportamenti nocivi per conto del cliente prima che siano disponibili le signature per identificarli.

La parte di "response" gestita consente al service provider di intraprendere un'azione adeguata, attraverso fasi pre-approvate, per rispondere a un'intrusione e difendere il proprio cliente da un attacco. Queste fasi possono essere personalizzate in base al tipo di attacco, all'asset, all'utente e così via e l'MDR si avvale di dispositivi di rilevamento di rete, come Deep Discovery, e di strumenti di sicurezza per gli endpoint.

I servizi MDR consentono alle organizzazioni di aggiungere alla propria struttura di sicurezza funzionalità di rilevamento e risposta disponibili 24/7.

Tra i fattori che stanno attualmente determinando la crescita dei prodotti MDR vi sono i cyberattacchi, le lacune nei servizi esistenti e la mancanza di competenze qualificate e a costi accessibili. In breve, le organizzazioni sono **interessate agli MDR per migliorare la loro capacità di rilevare e rispondere alle minacce e ciò rende gli MDR un tassello di una strategia di sicurezza più ampia.**

Tradizionalmente, la differenza tra i fornitori di servizi di sicurezza gestiti (MSSP) e di servizi MDR è che il primo offre monitoraggio e gestione della sicurezza in outsourcing, che include firewall e IPS. Gli MSSP si concentrano sulla tecnologia e sulla sua gestione, mentre gli MDR forniscono un servizio specifico che soddisfa le esigenze delle organizzazioni che non dispongono di risorse e competenze interne in materia di sicurezza. Va osservato che negli ultimi anni gli MSSP hanno spesso fallito nell'adattare i servizi alle reali esigenze dei clienti, **enfaticamente eccessivamente gli aspetti del monitoraggio a scapito di una risposta personalizzata.** La sfida per le aziende clienti non riguarda tanto la possibilità di ricevere avvisi di sicurezza quanto, piuttosto, di rispondere alle minacce che generano tali avvisi. La "risposta" è proprio l'elemento che caratterizza i vantaggi dei servizi MDR e i clienti cercano servizi di rilevamento delle minacce e di risposta sempre più completi.

Scegliere la soluzione più adatta per la vostra organizzazione

EDR

Consigliato se la vostra organizzazione:

- desidera fare un passo in avanti nella propria postura e capacità di sicurezza oltre l'uso dei cosiddetti antivirus di nuova generazione;
- dispone di un team dedicato alla sicurezza che ha tempo e competenze per intraprendere azioni a seguito degli avvisi e delle raccomandazioni prodotte dalla soluzione EDR;
- sta predisponendo una strategia di cybersecurity completa e vuole stabilire le basi per un'architettura di sicurezza scalabile.

XDR

Consigliato se la vostra organizzazione:

- desidera migliorare la capacità di rilevamento delle minacce avanzate;
- vuole accelerare le attività di analisi e investigazione sulle minacce multi dominio sfruttando una console di gestione unificata;
- sta soffrendo a causa del sovraccarico di avvisi di sicurezza generati da un'architettura informatica organizzata in silos sconnessi tra loro;
- sta cercando di ridurre i tempi di risposta.

MDR

Consigliato se la vostra organizzazione:

- non dispone di un programma affidabile di detection and response e degli strumenti correlati per affrontare e risolvere rapidamente le minacce avanzate;
- desidera aumentare la postura di sicurezza senza assumere altro personale;
- ha difficoltà a dotarsi di professionisti della sicurezza IT qualificati e specializzati;
- aspira a conseguire un livello di protezione che le consenta di rimanere aggiornata sulle ultime minacce.

OpenText CyberSecurity

 www.opentext.com

opentext™ Cybersecurity


PUNTI DI FORZA


- **Elevata precisione nel rilevamento.** OpenText minimizza i falsi allarmi del 97%, garantendo un rilevamento accurato del 99% delle minacce (valutazioni di MITRE Engenuity)


- **Expertise in sicurezza.** Il team di OpenText, operativo 24/7/365, offre esperienza avanzata in caccia alle minacce, investigazioni forensi e risposta agli incidenti.

- **Visibilità estesa.** Le soluzioni OpenText estendono la visibilità oltre gli endpoint, correlando dati da reti, cloud e altre fonti, per una protezione comprensiva contro le minacce

- **OpenText EnCase Endpoint Security**
- **OpenText Webroot Endpoint Protection**
- **OpenText Managed Extended Detection and Response**

 OpenText EnCase Endpoint Security è la soluzione EDR di OpenText progettata per offrire una difesa robusta degli endpoint attraverso capacità avanzate di rilevamento, indagine e risposta; si rivolge a organizzazioni più grandi con esigenze avanzate di analisi forense e risposta agli incidenti, offrendo strumenti dettagliati per indagini complesse. Questo prodotto permette alle organizzazioni di identificare rapidamente le minacce avanzate, valutare con precisione l'impatto degli incidenti e implementare azioni di risposta mirate per mitigare i rischi. Prevede un'interfaccia utente sofisticata che può gestire autenticazioni basate su certificati e fornire documentazione di supporto per affrontare vari problemi di sicurezza.

 OpenText Webroot Endpoint Protection è la soluzione EDR adatta a uffici domestici e piccole imprese che necessitano di sicurezza multi-endpoint. Webroot si distingue per la sua capacità di offrire una protezione leggera, basata su cloud e facile da gestire attraverso un'interfaccia utente semplificata.

 Per le aziende che cercano un approccio gestito alla sicurezza è disponibile il servizio OpenText Managed Extended Detection and Response che combina l'expertise degli analisti di sicurezza di OpenText con tecnologie avanzate per monitorare, rilevare e rispondere alle minacce in modo proattivo. Questo servizio estende le capacità di rilevamento e risposta oltre gli endpoint, integrando dati di sicurezza da una varietà di fonti come reti, cloud, e-mail e server, utilizzando tecnologie avanzate di machine learning e analisi comportamentale per identificare comportamenti sospetti e anomalie in tempo reale, consentendo ai team di sicurezza di agire rapidamente contro attacchi complessi. Il servizio MDR di OpenText si distingue per la sua capacità di adattarsi alle specifiche esigenze di sicurezza di un'organizzazione, offrendo una protezione personalizzata che copre non solo gli endpoint, ma anche reti e applicazioni cloud.

WatchGuard



800-911938



italy@watchguard.com



www.watchguard.com



PUNTI DI FORZA

- **Disponibilità 24/7.** Garantisce una sorveglianza ininterrotta, operando 24 ore su 24, 7 giorni su 7.
- **Team qualificato.** Il servizio si avvale dell'expertise di un team SOC composto da specialisti altamente qualificati nel campo della sicurezza IT.
- **Intelligenza Artificiale.** Utilizzando algoritmi di AI, WatchGuard MDR è in grado di effettuare un rilevamento proattivo delle minacce.
- **Riduzione del carico operativo.** La soluzione elimina la necessità per i partner di investire in un proprio SOC, in tecnologie dispendiose e nella ricerca di personale specializzato.

WatchGuard MDR

La soluzione MDR di Watchguard permette ai partner MSP di esternalizzare al SOC di WatchGuard il carico di monitorare e gestire la sicurezza degli endpoint dei clienti, nonché la ricerca proattiva e il contenimento degli attacchi informatici.

La peculiarità di WatchGuard MDR risiede nella sua capacità di liberare i partner dal peso di allestire un proprio SOC o di investire in tecnologie dispendiose e ricerca di personale specializzato. Interamente gestito da un team esperto di professionisti della sicurezza informatica e operante dal cloud, WatchGuard MDR sostiene i partner con indicazioni precise per la remediation e linee guida per la valutazione dei rischi, contribuendo a contrarre la superficie di attacco dei loro clienti.

La soluzione oltre a rafforzare la sicurezza 24/7, offre ai partner uno strumento efficace per rispondere alla crescente domanda di servizi di rilevamento e risposta a minacce sofisticate.

WatchGuard MDR offre un monitoraggio continuo individuando comportamenti anomali grazie all'IA avanzata e al team SOC sempre operativo.

Grazie al rilevamento proattivo, è in grado di identificare minacce complesse che potrebbero eludere altri sistemi di sicurezza.

Ogni allarme viene analizzato per confermare l'incidente e generare una risposta automatizzata efficace assicurando un intervento immediato per una pronta ripresa. WatchGuard MDR emerge, inoltre, come una soluzione vantaggiosa per quelle aziende che aspirano a un servizio di sicurezza di alto livello ma sono consapevoli e prudenti nelle spese.

Infine, la soluzione offre protezione 24 ore su 24 fornendo report di valutazione periodici che aiutano i partner a migliorare il livello di sicurezza dei loro clienti. Questa trasparenza non solo dimostra la capacità di risposta di WatchGuard MDR ma educa anche i clienti sulla natura delle minacce e sulle misure preventive adottate, permettendo loro di comprendere meglio il valore del servizio.

CrowdStrike

 www.crowdstrike.com




PUNTI DI FORZA


- Uso avanzato dell'AI e del machine learning
- Approccio Cloud-Native
- Integrazione con soluzioni di terze parti
- Offerta di servizi gestiti di XDR


- **Falcon Insight XDR**
- **Falcon Go**
- **Falcon Complete XDR**

CrowdStrike Falcon è il prodotto per la protezione degli endpoint, fornito come parte della piattaforma cloud-native per la sicurezza degli endpoint e come agente di sicurezza unificato con moduli aggiuntivi quali il monitoraggio dell'integrità dei file, la sicurezza del cloud, la protezione delle identità e altri.

 CrowdStrike Falcon Insight XDR è una piattaforma potenziata dall'intelligenza artificiale che estende la visibilità a livello enterprise, rileva le minacce avanzate e fornisce una risposta automatica sugli endpoint. Questa piattaforma combina le informazioni sulle minacce con un'avanzata tecnologia di rilevamento e risposta con la capacità di mettere in correlazione la telemetria nativa cross-dominio di CrowdStrike con quella di terze parti mediante specifici connettori per le soluzioni di aziende che aderiscono alla CrowdXDR Alliance.

Le componenti XDR native includono EDR, identità, cloud, threat intelligence mobile, gestione delle vulnerabilità, protezione dei dati; le integrazioni con l'ecosistema aperto di terze parti includono soluzioni di Email, Network detection and response, Identity and access management, Single sign-on (SSO), Security service edge, Secure web gateway, Cloud access security broker.

 CrowdStrike ha anche lanciato un nuovo bundle di prodotti, chiamato Falcon Go, pensato per le esigenze delle piccole e medie imprese.

 CrowdStrike Falcon Complete XDR è l'offerta Managed XDR che mette a disposizione funzionalità avanzate di rilevamento e risposta alle minacce guidata da esperti e attiva 24 ore su 24, 7 giorni su 7 che sollevano le aziende dagli oneri di implementazione e gestione. Fornisce funzioni di ricerca delle minacce, monitoraggio, analisi e risposta sulla superficie di attacco dei clienti. CrowdStrike è stata inserita tra i leader del Magic Quadrant di Gartner 2023 per le piattaforme di protezione degli endpoint.

BITDEFENDER

GRAVITYZONE EXTENDED DETECTION AND RESPONSE (XDR)

GravityZone XDR rileva in maniera nativa gli attacchi nell'intera azienda, incluso dispositivi fisici e IoT, piattaforme ibride e multi-cloud, oltre a workload nativi del cloud. XDR combina il rilevamento automatico delle minacce e l'analisi delle cause principali, assemblando i segnali provenienti da più sistemi e presentandoli in un formato che chiunque può interpretare. I team di sicurezza non devono eseguire analisi manuali, potendo così concentrarsi su una risposta rapida agli incidenti che interessano identità, rete, e-mail, cloud ed endpoint.

CISCO

CISCO XDR

Cisco offre un approccio aperto e flessibile all'XDR, che consente ai clienti di attingere alla gamma di soluzioni Cisco Secure e di sfruttare gli investimenti esistenti. Tale metodo migliora il rilevamento delle minacce, permette di ottenere visibilità e intelligence con un approccio multivettoriale e multi-vendor fornendo ai team security funzionalità efficaci per l'assegnazione delle priorità. Le soluzioni Cisco XDR aumentano la produttività e compensano la carenza di esperti attraverso funzionalità di automazione per contrastare minacce avanzate.

CHECK POINT SOFTWARE

HORIZON XDR/XRP

Horizon XDR/XPR assicura una prevenzione completa sull'intero sistema di sicurezza aziendale: endpoint, rete, dispositivi mobili, e-mail e cloud. La soluzione integra i dati di Defender for Endpoint con altri prodotti Check Point e con altre fonti dati di terze parti, analizzandoli per scoprire attacchi nascosti. Offre prevenzione dalle minacce, correlazione tra eventi tramite Intelligenza artificiale e threat intelligence, e analisi approfondite per rilevare attacchi nella kill chain, esaminando comportamenti, contesti e danni.

ESET

ESET INSPECT

ESET Inspect è una soluzione XDR che fornisce una visione completa del sistema e delle minacce, permettendo analisi dettagliate e una pronta reazione agli incidenti. Integrata con i prodotti ESET Endpoint Protection, offre capacità notevoli nella sicurezza IT: rileva minacce persistenti avanzate, interrompe attacchi fileless, blocca minacce zero-day e protegge da ransomware. Inoltre, contribuisce a garantire il rispetto dei criteri aziendali, diventando un elemento chiave per mantenere un ambiente di lavoro sicuro e conforme alle normative.

FORTINET

FORTIXDR

FortiXDR di Fortinet fa parte della piattaforma SecOps e correla i dati provenienti da endpoint, rete, cloud e altri data lake per rilevare gli attacchi nascosti che avvengono a livello aziendale. Una volta rilevati, FortiXDR conduce automaticamente azioni di risposta agli incidenti oppure può aiutare gli analisti a rimediare rapidamente. I risultati prodotti da FortiXDR sono basati su analytics, AI e automazione end-to-end. Il rilevamento delle minacce e l'analisi delle correlazioni dei FortiGuard Labs monitorano i feed di sicurezza identificando le attività sospette.

PALO ALTO NETWORKS

CORTEX XDR

Cortex XDR blocca attacchi malware, exploit e fileless avanzati grazie allo stack di sicurezza degli endpoint. Utilizza il machine learning per creare un profilo del comportamento e rilevare anomalie indicative di un attacco. L'analisi permette di identificare i tentativi degli attaccanti di confondersi con utenti legittimi. L'agent leggero blocca le minacce utilizzando la protezione basata su comportamento, intelligenza artificiale e analisi cloud-based. Riduce i tempi di risposta alle minacce, semplifica le operazioni e aumenta la produttività SOC.

KASPERSKY

KASPERSKY ENDPOINT DETECTION AND RESPONSE (EDR) EXPERT

Kaspersky EDR Expert offre una visibilità completa su tutti gli endpoint della rete aziendale e una protezione superiore, automatizzando le attività EDR di routine e consentendo agli analisti di rilevare, assegnare le priorità, analizzare e neutralizzare velocemente minacce complesse e attacchi di tipo APT. Utilizza un singolo agente che può essere gestito sia da una singola piattaforma di gestione cloud based sia da una console offline in ambienti di tipo "air-gap", con threat intelligence e rilevamento personalizzabile.

SENTINELONE

SENTINELONE SINGULARITY ENDPOINT SECURITY

La soluzione EDR non è più sufficiente ma serve adottare una piattaforma XDR, come quella offerta da SentinelOne capace di rilevare l'emergenza, una soluzione integrata con altre piattaforme che può arricchire il contesto dell'evento con informazioni utili (eXtended Detection) e che assicura capacità di contrasto, al fine di mitigare il rischio (eXtended Response). Inoltre, SentinelOne offre una soluzione basata sull'AI e ha presentato Purple AI, un sistema dotato di AI generativa rivolta agli specialisti di cybersecurity, i cosiddetti «threat hunters».

TREND MICRO

TREND VISION ONE

Trend Vision One - Endpoint Security offre protezione omnicomprensiva e strumenti di rilevamento e risposta centralizzati per vari asset. L'architettura a singolo agente fornisce antimalware, anti ransomware, controllo delle applicazioni e dispositivi. Lo stesso agente permette anche la raccolta dati in tempo reale per il funzionamento dei moduli avanzati di rilevamento e risposta (XDR). Inoltre, la soluzione garantisce controllo completo su client, server, e-mail, cloud, network, mobile e reti OT, integrando moduli ASRM e ZTSA in Vision One.

VODAFONE BUSINESS

ENDPOINT GUARDIAN

Vodafone Business offre soluzioni avanzate di EDR/XDR per la protezione di endpoint e infrastrutture dei clienti, dalle piccole alle grandi aziende. Le tecnologie proposte offrono protezione dagli attacchi, identificando comportamenti sospetti e potenziali minacce; offrono una risposta rapida ed efficace, rimuovendo la minaccia e isolando il dispositivo. Il cliente è supportato nella mitigazione dell'attacco grazie a un servizio ampiamente personalizzabile, disponibile in differenti livelli di servizio, dagli orari d'ufficio fino a una copertura 24x7.

VECTRA AI

VECTRA AI PLATFORM

Vectra AI Platform fornisce una risposta veloce e efficiente contro gli attacchi IT, con visibilità in tempo reale e dettagli essenziali per l'intervento immediato. Sfrutta l'Attack Signal Intelligence per l'automazione del rilevamento, triage e priorità delle minacce, coprendo oltre il 90% delle tecniche MITRE ATT&CK grazie alle contromisure brevettate MITRE D3FEND. Con un rilevamento basato su AI, firme e intelligence, Vectra traccia gli attacchi, inclusi i movimenti laterali, in data center, cloud e identità digitali.menti laterali su data center, cloud e identità.



GLI APPROFONDIMENTI
DI BIZZIT



XDR migliora la risposta agli attacchi

Com'è lecito attendersi, esistono vari approcci all'XDR. Gli approcci single-stack pagano il lock-in su un unico fornitore, spesso offrendo una ridotta copertura del perimetro. I sistemi ibridi o aperti, invece, sono indipendenti dal fornitore, completano le tecnologie esistenti e possono essere integrati con altri pezzi del puzzle (es.: SIEM e SOAR, più adatti a grandi aziende), raggiungendo i risultati migliori senza dover ricorrere a gestioni dati complesse come i data lake.

[+ continua a leggere](#)