radware

Guida

Guida per i CISO alla Security nell'era dell'IA

Indice dei contenuti

Introduzione

Negli ultimi anni, il ritmo del cambiamento nel settore della cybersecurity è passato da rapido a esponenziale. Nuove sfide, come gli attacchi automatizzati e potenziati dall'intelligenza artificiale, si affiancano a problematiche già note, come normative sempre più stringenti e la carenza di professionisti qualificati. In questo contesto, il compito del CISO — mantenere l'organizzazione sicura ed efficiente — è diventato ancora più complesso. Le domande cruciali si moltiplicano: Come possono le difese evolversi con la stessa rapidità delle minacce? Come rispettare un numero crescente di normative con un team ridotto? Come garantire la sicurezza in un panorama in continua trasformazione? Questa guida intende rispondere proprio a queste domande. Analizza i principali ostacoli che i CISO di oggi si trovano ad affrontare e identifica gli elementi chiave per costruire un ambiente più sicuro. Scoprirai come Radware® EPIC-AI™, grazie ad algoritmi avanzati e funzionalità generative basate sull'intelligenza artificiale, offra una protezione precisa, automatizzata e in tempo reale su tutte le piattaforme. Per i CISO e i loro team, questo si traduce in risposte più rapide, costi ridotti e una maggiore sicurezza per applicazioni e infrastrutture.

Parte I. Quattro sfide per mantenere la sicurezza delle applicazioni

Questo documento esamina uno spettro di responsabilità che spazia dalla valutazione del rischio e dalla garanzia di risposte rapide alla gestione delle attività di comunicazione e all'allocazione delle risorse. Ma quali sono le sfide che li tengono svegli durante la notte?

Sfida 1: Il panorama mutevole delle minacce

I dati della rete cloud di Radware mostrano cambiamenti significativi nell'attuale panorama delle minacce, incluso uno spostamento verso il livello applicativo. Le dimensioni, la frequenza e la complessità di questi attacchi continuano a crescere in tutti i vettori di attacco: il volume medio degli attacchi DDoS è aumentato del 127% su base annua nel 2024, gli attacchi bot sono aumentati del 61% su base annua nel primo semestre del 2024 e gli attacchi Web DDoS mitigati sono aumentati del 265% dal secondo semestre del 2023 al primo semestre del 2024.

Quattro fattori principali guidano oggi i cambiamenti nel campo della cybersecurity:

Motivazioni di gruppi hacker in evoluzione

Un'analisi dei gruppi di hacker-attivisti (hacktivisti) più attivi negli ultimi anni rivela l'incremento di tre diversi tipi di motivazione all'attacco:

Attacchi a sfondo politico - Gruppi come NoName, Killnet, Anonymous Russia e Passion Group sono diventati più attivi dopo l'invasione dell'Ucraina da parte della Russia. Da allora, abbiamo visto questa tendenza espandersi per includere altri eventi in cui vita e politica si intersecano, dall'Eurovision Song Contest ai Giochi Olimpici estivi. Tutti i raduni globali con un contesto politico sono attraenti per diversi gruppi di hacktivisti che vogliono prendere di mira le organizzazioni associate ai Paesi partecipanti. Ad esempio, una visita del presidente dell'Ucraina Volodymyr Zelenskyy in Canada lo scorso anno ha scatenato una serie di attacchi contro i siti Web canadesi. I siti del parlamento canadese, del primo ministro, delle banche, dei trasporti, degli aeroporti, ecc., sono stati tutti inattivi per giorni prima e durante la visita. Attacchi simili si sono verificati contro i siti Web del governo francese dopo che la decisione del Paese di fornire armi antimissile all'Ucraina ha attirato l'attenzione di NoName, uno dei principali gruppi hacktivisti filorussi.

Attacchi a sfondo religioso - Questo tipo di attacchi si verifica frequentemente quando gruppi di hacktivismo filo-islamico prendono di mira un Paese o un'organizzazione che ritengono abbia insultato o danneggiato la fede musulmana. Avrete forse notato che gruppi come Anonymous Sudan, Mysterious Team Bangladesh, Dragon Force Malaysia e altri sono diventati più attivi negli ultimi anni in diversi conflitti. Ma non è necessario essere una grande organizzazione o un marchio in prima linea nelle battaglie religiose per subire l'ira di questi attacchi. A novembre 2023, Cloudflare è stata attaccata perché stava proteggendo OpenAI, considerato dagli hacktivisti filo-palestinesi come associato al movimento filo-israeliano. Un altro episodio degno di nota è avvenuto durante la settimana della moda australiana, quando si sono verificati attacchi in tutto il Paese in risposta a un abito che riportava una frase araba tratta dal Corano.

Hacktivisti motivati finanziariamente - Altri gruppi di hacktivisti sono diventati più formalizzati e finanziariamente motivati. Forniscono strumenti di attacco per DDoS, takeover dell'account (ATO) o servizi di crypto ceiling. Questi tipi di gruppi pubblicizzano le loro funzionalità sui loro canali di social media, facendo pubblicità per convincere il loro pubblico ad acquistare e utilizzare strumenti DDoS-for-hire e botnet-for-hire per attaccare i propri obiettivi. Lo strumento "Infrashutdown" di Anonymous Sudan è facilmente disponibile per l'acquisto online.

Strumenti degli aggressori in continua evoluzione

Anche il cambiamento dei metodi di attacco degli attivisti informatici ha contribuito alla trasformazione del panorama delle minacce. I nuovi attacchi non si limitano solo ad aumentare in dimensioni e velocità. Sono più automatizzati e sofisticati che mai, spesso utilizzando tecniche di randomizzazione multiple per eludere le difese tradizionali. Inoltre, stanno facendo convergere diversi vettori di attacco in singoli strumenti che costituiscono piattaforme di attacco all-in-one. E non devi cercare nel dark Web qualcosa come il famoso strumento di attacco MHDDoS. È disponibile pubblicamente su GitHub. Questo strumento combina 56 diversi metodi di attacco, tra cui vettori di attacco DDoS (HTTP/S GET, POST floods), vettori di attacco bot (bypassa il CAPTCHA impersonando il crawler del motore di ricerca Google per apparire come un bot legittimo), vettori di attacco alle applicazioni Web (vulnerabilità di PHP, Apache, WordPress) e funzionalità di bypass integrate contro le difese comuni (Cloudflare, Google Shield).

Questo tipo di strumento di attacco multivettore dimostra che gli aggressori moderni e i loro strumenti non fanno distinzione tra WAF, protezione DDoS, protezione bot e così via. Mentre le organizzazioni fanno una distinzione tra queste aree di protezione, di solito con team e budget separati per ciascuna, gli aggressori non lo fanno. Le organizzazioni devono spostare il loro approccio dalle protezioni a silos a una piattaforma integrata che protegga da un'ampia gamma di minacce e possa superare efficacemente questi strumenti di attacco all-in-one.

Crescita della comunità degli aggressori

Due fattori principali contribuiscono al recente incremento nella comunità degli hacker:

I giocatori sulle piattaforme online alimentano la crescita della comunità degli aggressori - Per prima cosa, osserviamo la trasformazione dei normali giocatori in aggressori. Quattro su cinque aggressori coinvolti in attacchi ATO e DDoS sono giocatori. Dalla pandemia di COVID, abbiamo visto crescere la comunità di gioco di 700 milioni di nuovi giocatori. Se anche solo una frazione di loro passasse agli attacchi, sarebbe un enorme salto di crescita per questo gruppo.

Gli hacker ampliano il loro raggio d'azione attraverso le reti online – Gli hacker sfruttano il potere dei social network per ampliare i loro attacchi. Usano i loro social network come cartelloni pubblicitari e utilizzano marketplace e centri di hacking in tutti questi network. In questo modo permettono agli hacker di ampliare il proprio pubblico e di coinvolgere più persone negli attacchi.

Rivoluzione degli attacchi guidata dall'intelligenza artificiale

Sembra che l'intelligenza artificiale tocchi ogni giorno più aspetti della vita e che la battaglia sulla cybersecurity non faccia eccezione. Nell'elencare i principali sviluppi che contribuiscono a trasformare l'attuale panorama delle minacce, non si può ignorare il crescente uso dell'IA nei cyberattacchi. Ecco uno sguardo a come funziona:

Automazione dell'IA – Gli hacker utilizzano l'IA per automatizzare i loro attacchi nello stesso modo in cui gli sviluppatori potrebbero usare ChatGPT o altri strumenti di intelligenza artificiale generativa (GenAI) per creare codice più velocemente e meglio. Gli hacker possono ora fare lo stesso con gli attacchi informatici, sviluppando strumenti GenAI dedicati come WolfGPT, XXXGPT e altri per creare codice per malware, botnet, cryptoware, strumenti DDoS, strumenti ATO e altro ancora.

Intelligenza artificiale negli strumenti - Sempre più spesso vediamo l'uso dell'intelligenza artificiale negli strumenti di attacco veri e propri per creare attacchi più sofisticati e superare le difese tradizionali come i CAPTCHA. A maggio 2024, un noto strumento DDoS chiamato stresser.cat ha pubblicato una registrazione dello schermo per dimostrare le funzionalità di risoluzione dei CAPTCHA dello strumento. La precisione di questa versione dello strumento si ferma al 77%, ma aumenterà senza dubbio con le iterazioni future.

AI per i zero day - Ricerche recenti hanno dimostrato come gli hacker possano ora creare attacchi autonomi a partire da vulnerabilità zero-day. Prendono le vulnerabilità e gli exploit comuni (CVE) che sono stati pubblicati e li trasformano automaticamente in attacchi. Quando i ricercatori dell'Università dell'Illinois Urbana-Champaign (UIUC) hanno testato ChatGPT 4 su un set di dati di 15 vulnerabilità del mondo reale, lo strumento ha ottenuto risultati significativamente superiori rispetto ad altri modelli e strumenti. Ha sfruttato l'87% di queste vulnerabilità con prestazioni che dovrebbero migliorare.

Che cosa serve per sopravvivere nell'era delle minacce informatiche automatizzate e potenziate dall'intelligenza artificiale? Combattere l'IA con l'IA. L'adozione delle protezioni basate sull'intelligenza artificiale può aiutare le organizzazioni a rimanere sicure di fronte agli strumenti di attacco potenziati dalle funzionalità dell'IA e della GenAI. Cercate una sicurezza intelligente che utilizzi l'intelligenza artificiale e gli algoritmi di apprendimento automatico per anticipare le ultime minacce e mantenere la vostra organizzazione al sicuro.

Sfida 2: Nuovi requisiti normativi

Anche i requisiti normativi sui processi e sugli strumenti di sicurezza hanno reso la vita più difficile per i CISO, i responsabili della sicurezza e i dirigenti a livello C.

PCI DSS 4.0 - Il Payment Card Industry Digital Security Standard (PCI DSS) 4.0 aggiorna i requisiti per tutte le entità che elaborano, facilitano o supportano transazioni finanziarie. A partire da marzo 2025, l'ultimo standard PCI DSS sggiunge nuovi requisiti per WAF, modelli di sicurezza positivi, protezione delle API e sicurezza lato client. Questi non facevano parte dei requisiti delle versioni precedenti.

NIS2 - La direttiva sulla sicurezza delle reti e dell'informazione (NIS) 2 estende gli standard di cybersecurity precedentemente stabiliti per i servizi essenziali nell'Unione Europea. L'aggiornamento include sanzioni per il mancato rispetto dei requisiti di gestione del rischio e di rendicontazione. L'ultima direttiva dell'Unione Europea richiede il mantenimento della disponibilità delle applicazioni, come ad esempio le soluzioni di protezione DDoS per essere completamente conformi e protette.

DORA - Il Digital Operational Resiliency Act (DORA) crea norme per le istituzioni finanziarie al fine di garantire la protezione, il rilevamento, il contenimento, il recupero e la riparazione delle tecnologie dell'informazione e della comunicazione.

GDPR - Il Regolamento generale sulla protezione dei dati (GDPR) impone standard alle organizzazioni ovunque si trovino che si rivolgono o raccolgono dati relativi a persone nell'Unione Europea. Il GDPR sanziona chiunque non rispetti i suoi standard di privacy e sicurezza.

HIPAA – L'Health Insurance Portability and Accountability Act (HIPAA) protegge le cartelle cliniche e altre informazioni sanitarie identificabili personalmente. Richiede salvaguardie, stabilisce limiti e conferisce alle persone diritti sui loro registri protetti.

Leggi sulla trasparenza – Negli Stati Uniti, le organizzazioni non possono più mantenere privati gli attacchi. La SEC richiede che le aziende comunichino qualsiasi incidente di cybersecurity rilevante per la loro attività entro quattro giorni lavorativi. Le aziende devono discutere pubblicamente delle violazioni con i clienti e, idealmente, vogliono evitare del tutto gli incidenti di cybersecurity.

I CISO non possono più cercare soluzioni puntuali. Hanno bisogno di una piattaforma integrata per garantire la completa conformità a questi nuovi e più rigorosi standard.

Sfida 3: Espansione delle distribuzioni di cloud ibrido

L'aumento delle implementazioni di cloud ibrido crea anche difficoltà per i CISO. Un numero sempre maggiore di organizzazioni sta gestendo ambienti multi-cloud ibridi, sfruttando più distribuzioni di cloud pubblici e privati, mantenendo al contempo il data center on-premise.

Secondo il rapporto di Radware Application Security in a Multi-Cloud World 2023, il 55% delle organizzazioni oggi gestisce tre o più ambienti e il 73% delle organizzazioni continua a mantenere i propri data center hardware on-premise. Di conseguenza, devono mantenere il loro data center on-premise, gestire più fornitori di cloud e garantire una protezione coerente in tutti questi diversi ambienti.

Sfida 4: Carenza di personale e competenze in materia di cybersecurity

La quarta sfida che i CISO devono affrontare nell'ambiente odierno della cybersecurity riguarda quasi tutti gli aspetti del lavoro e la qualità del lavoro. È la reale e dolorosa carenza di esperti qualificati in cybersecurity. Secondo uno studio ISC Cybersecurity Workforce del 2024, il 67% delle organizzazioni deve far fronte a carenze di personale o di competenze in materia di sicurezza e ci sono quasi 4 milioni di posizioni aperte a livello globale per ruoli di cybersecurity. Di conseguenza, il 45% delle organizzazioni afferma di non riuscire a trovare personale qualificato. Questa carenza mette a dura prova i team di sicurezza e limita la loro capacità di monitorare le minacce e rispondere tempestivamente. Come possono i CISO risolvere questo problema? Devono cercare protezioni più automatizzate che richiedano una minore dipendenza dagli esseri umani. Allo stesso tempo, devono cercare servizi gestiti specializzati che possano fornire una base di soluzioni di sicurezza e gestione esperte.

Parte II. Che cosa è necessario per restare protetti?

Nell'attuale mondo di attacchi potenziati dall'intelligenza artificiale, proteggere la propria organizzazione significa essere all'avanguardia rispetto agli strumenti che generano attacchi più grandi, più veloci e più complessi. Abbiamo già discusso delle quattro sfide principali. Esploriamo ora le funzionalità chiave che i CISO dovrebbero cercare quando sono alla ricerca di una soluzione di sicurezza più moderna.

4 Funzionalità di cybersecurity per il mondo dell'IA:

Sicurezza intelligente – Non è facile raggiungere da soli la velocità e la potenza di calcolo dell'intelligenza artificiale. Combattete le minacce basate sull'intelligenza artificiale con una protezione basata sull'intelligenza artificiale grazie all'uso di una sicurezza intelligente alimentata da algoritmi basati sull'intelligenza artificiale.

Piattaforma integrata – Conformatevi agli standard e ai requisiti normativi più recenti e contrastate gli strumenti di attacco all-in-one che combinano diversi metodi di attacco, senza limitarsi solo alla protezione DDoS, al WAF o a un solo tipo di sicurezza. Una piattaforma integrata che correla un'ampia gamma di minacce offre la migliore protezione contro questi strumenti.

Protezione costante - Le minacce di oggi vanno dove andate voi. Proteggete tutti i vostri ambienti, on-premise, pubblici, privati o ibridi, e tutti i punti di accesso alle vostre applicazioni.

Difesa esperta - Superate le attuali carenze di personale nella cybersecurity e le campagne di attacco complesse e in rapida evoluzione con l'aiuto di un supporto esperto in sicurezza attivo 24/7.

Solo una soluzione che combini queste quattro aree può abbassare il tempo medio di risoluzione (MTTR), ridurre i costi e proteggere il vostro marchio. Questo è esattamente ciò che Radware fornisce.

Come rimanere al sicuro nell'era dell'intelligenza artificiale

Protezione delle applicazioni a 360° tramite la piattaforma di sicurezza cloud di Radware

Radware offre una protezione a 360 gradi per applicazioni e infrastrutture, grazie a una piattaforma integrata che combina sicurezza intelligente e difesa esperta applicata in modo coerente in tutti i vostri ambienti. Lo facciamo integrando EPIC-AI, la nostra intelligenza artificiale, in tutte le aree di protezione.

5 fatti sulla nostra protezione unica, potenziata dall'IA

- Protegge tutte le tue applicazioni mobili e Web e le API in tutti i tuoi diversi ambienti: cloud pubblici, data center di cloud privati, microservizi ecc.
- Blocca una vasta gamma di minacce, tra cui attacchi Web, abuso di API, bot dannosi, attacchi basati sull'intelligenza artificiale, attacchi DDoS e così via.
- Combatte queste minacce esterne con una piattaforma integrata dotata di motori di protezione in tempo reale, tra cui WAF, protezione API, gestione bot, protezione DDoS e Web DDoS, protezione lato client e protezione dal takeover dell'account (ATO).
- Offre piena visibilità e controllo della protezione della rete e delle applicazioni grazie alla nostra piattaforma di sicurezza cloud, gestita da un unico portale.
- Dotata degli algoritmi di apprendimento automatico basati sull'IA di EPIC-AI per affrontare la sofisticatezza e la complessità degli attacchi attuali.

Parte III. Presentazione della piattaforma di sicurezza cloud di Radware alimentata da EPIC-AI

Che cosa è esattamente EPIC-AI e come rafforza la protezione delle applicazioni cloud a 360 gradi di Radware?

Radware EPIC-AI

Radware offre intelligenza artificiale potenziata e funzionalità GenAI sulla propria piattaforma di sicurezza cloud per proteggere le app, ridurre il tempo medio di risoluzione (MTTR) e risparmiare sui costi. EPIC-AI funziona su tutte le piattaforme per garantire una protezione precisa, automatizzata e in tempo reale.

Grazie a EPIC-AI, Radware fornisce una piattaforma di sicurezza integrata nel cloud a più livelli che offre:

Integrazione tra più punti di applicazione

Le soluzioni Radware possono integrarsi attraverso i vari punti di applicazione, inclusi i nostri prodotti (Alteon e DefensePro X) e i servizi cloud e i servizi di terze parti (da NGINX, Envoy o cloud pubblico—AWS, Google Cloud e altro). Ci integriamo con questi punti di applicazione per applicare le politiche di sicurezza, le signatures e le regole in modo uniforme, indipendentemente da dove risiede l'applicazione. Questo approccio di integrazione unico, senza eguali sul mercato, offre ai clienti la protezione coerente che cercano negli ambienti on-premise, privati e di cloud pubblico.

Motori di protezione cloud in tempo reale

I motori di protezione cloud in tempo reale di Radware forniscono protezione WAF, gestione dei bot, protezione DDoS, protezione Web DDoS, protezione API, protezione da takeover dell'account (ATO) e protezione lato client. Ognuno di questi moduli offre agli utenti una soluzione d'eccellenza che sfrutta l'intelligenza artificiale e gli algoritmi di apprendimento automatico per rilevare automaticamente e con precisione e bloccare in modo mirato le attività dannose, compresi gli attacchi Web DDoS Tsunami, i bot simili a umani guidati dall'intelligenza artificiale e gli attacchi alla logica aziendale delle API.

Fabric multipiattaforma

Questo livello collega i nostri motori di protezione in tempo reale in un'unica soluzione integrata e completa. Utilizza algoritmi di blocco delle fonti guidati dall'intelligenza artificiale, informazioni sulle minacce e feed basati sui dati per bloccare preventivamente le fonti dannose prima che causino danni. La correlazione cross-model basata sull'IA e la messa a punto dei criteri e le raccomandazioni supportate dall'IA attraversano i motori di protezione, consentendo loro di rilevare accuratamente gli attacchi e ridurre al minimo i falsi positivi e i falsi negativi. I clienti di Radware possono vedere attraverso i motori di protezione e bloccare le fonti dannose prima ancora che queste tentino di accedere ad altre applicazioni.

Core di Gestione SOC

Le funzionalità Core di gestione SOC di Radware consentono servizi gestiti 24 ore su 24, 7 giorni su 7, potenziati dall'intelligenza artificiale, e una gestione e operazioni di sicurezza automatizzate. Il SOC Xpert di Radware basato su IA fornisce una risoluzione automatica e istantanea degli incidenti e accelera l'analisi delle cause principali riducendo il MTTR fino al 95%. Questo servizio fornisce funzionalità potenziate dall'IA per il team di risposta alle emergenze (ERT) di Radware per offrire servizi gestiti migliori e più automatizzati. Inoltre, aiuta le organizzazioni con il proprio SOC a risolvere gli incidenti in modo più rapido e accurato. Fornisce una risoluzione automatica e istantanea delle minacce, accelera l'analisi delle cause principali e offre rimedi e raccomandazioni, persino intraprendendo azioni per risolvere automaticamente l'incidente al posto vostro. Questo riduce l'MTTR da ore a minuti, con una riduzione complessiva fino al 95% dell'MTTR per incidente!

Radware offre anche funzionalità di conformità, analisi avanzate e integrazioni con terze parti per rendere l'esperienza fluida e inclusiva. Tutto questo è gestito da un portale unificato e integrato.

Caso di studio: L'intelligenza artificiale assiste Radware nella protezione chirurgica del Web da tsunami DDoS

La posta in gioco

La capacità di Radware di bloccare gli attacchi evasivi utilizzando una protezione Web DDoS alimentata dall'intelligenza artificiale è stata impiegata di recente per una banca dell'area EMEA. La banca, che ha subito un'ondata di attacchi DDoS sul Web, ha dovuto affrontare potenziali perdite finanziarie e di reputazione associate ai tempi di inattività se gli attacchi fossero andati a buon fine.

La sfida

Fermare questi attacchi sarebbe stato un compito difficile per una tipica soluzione di sicurezza DDoS. Il numero di richieste al secondo (RPS) ha raggiunto i 14,6 milioni, l'equivalente di 14 milioni di persone che tentano di accedere al proprio conto bancario su questo sito ogni secondo per tutta la durata dell'attacco. La durata dell'attacco è stata di diversi giorni e ha visto più ondate di attacco. Alcune ondate sono durate fino a 20 ore, solo per un singolo attacco!

La soluzione

Radware è stata in grado di fermare automaticamente questi attacchi in pochi secondi. Utilizzando la creazione automatica di firme in tempo reale, ha bloccato tutte le minacce prima che potessero avere un impatto sulla banca o sui suoi utenti finali. Una delle firme in tempo reale includeva oltre 27 parametri per controllare con precisione cosa bloccare e cosa non bloccare in modo da fermare il traffico dannoso e consentire il passaggio di quello legittimo. Tutto questo è stato fatto automaticamente, senza che la banca intraprendesse alcuna azione e senza alcun impatto sui clienti della banca.

La protezione di questa banca EMEA da parte di Radware offre ai CISO una chiara tabella di marcia su come possono combattere l'IA con l'IA: utilizzando algoritmi basati sull'IA per creare firme in tempo reale in pochi secondi.

Sintesi

Radware EPIC-AI nel mondo reale: Protezione dove conta di più

Nell'attuale panorama in rapida evoluzione delle minacce informatiche, i CISO devono affrontare sfide considerevoli per garantire a un ambiente di lavoro più sicuro. Si trovano ad affrontare un panorama di minacce in evoluzione, caratterizzato da hacktivisti motivati, strumenti di attacco in continuo sviluppo e attacchi automatizzati abilitati dall'intelligenza artificiale. Hanno anche problemi noti, tra cui un insieme di rigide normative per la conformità alla cybersicurezza e l'espansione delle implementazioni di cloud ibrido. Ad aggravare lo stress, tutto ciò avviene in un periodo di carenza di personale e competenze nel campo della cybersecurity.

Radware utilizza l'intelligenza artificiale per aiutare le organizzazioni a superare le loro sfide. Neutralizza le minacce abilitate dall'IA con soluzioni di sicurezza potenti grazie a EPIC-AI, utilizzando algoritmi avanzati e funzionalità di intelligenza artificiale generativa per operare su tutte le piattaforme e garantire una protezione precisa in tempo reale. In questo modo, i clienti hanno a disposizione una piattaforma integrata per garantire la coerenza della protezione su tutte le applicazioni e gli ambienti. Garantisce inoltre motori di protezione intelligenti e basati sull'AI per un rilevamento e una mitigazione accurati e in tempo reale e crea una risposta automatizzata e basata sull'AI per un tempo medio di ripristino (MTTR) più rapido. Migliorate la vostra sicurezza nell'era dell'intelligenza artificiale, riducendo allo stesso tempo le spese generali e le necessità di personale. Combattete l'IA con l'IA con l'aiuto di Radware.

RWI 402 | 22.01.2025