radware

Guide

CISO's Guide to Security in the Age of AI

Contents

Introduction

The pace of change in cybersecurity has gone from fast to exponential over the last few years. With new challenges like automated and AI-enabled attacks added to old headaches like strict regulations and staffing shortages, the CISO's mission to maintain a secure and efficient organization has become even more daunting—and the questions more difficult. You might ask: How can defenses evolve as fast as threats? How do you comply with more regulations and vulnerabilities with fewer security workers? How do I stay ahead so we can stay secure? This guide will tell you just that. It explores the biggest cybersecurity obstacles that today's CISOs face and suggests the missing elements needed to ensure a safer workplace. It also shows how Radware® EPIC-AI™ uses AI-powered algorithms and generative AI capabilities, working across platforms to ensure precise, hands-free and real-time protection. For CISOs and their teams, that means faster resolutions, lower costs and more secure applications and infrastructure.

Part I. Four Challenges in Maintaining Application Security

A CISO's whiteboard hints at a spectrum of responsibilities from assessing risk and ensuring quick responses to communication to-dos and resource allocation. But what are the challenges that keep them awake at night?

Challenge 1: The Shifting Threat Landscape

Data from Radware's Cloud Network shows significant changes throughout today's threat landscape, including a shift towards the application layer. The size, frequency and complexity of these attacks continue to grow across attack vectors with the average DDoS attack volume up 127% YoY in 2024, bot attacks up 61% YoY in H1 2024 and mitigated Web DDoS attacks up 265% from H2 2023 to H1 2024.

Four major factors drive changes within cybersecurity today:

Shifting Hacktivist Motivations

A review of the most active activist-hacker (hacktivist) groups over the last few years reveals the rise of three different types of attack motivation:

Politically motivated attacks – Groups like NoName, Killnet, Anonymous Russia and Passion Group all became more active after Russia invaded Ukraine. Since then, we've seen this trend expand to include other events where life and politics intersect—from the Eurovision Song Contest to the Summer Olympic Games. All global gatherings that have some political context to them are attractive to different hacktivist groups that want to target organizations associated with participating countries. For example, a visit by Ukraine President Volodymyr Zelenskyy to Canada last year sparked a series of attacks against Canadian websites. Sites for the Canadian parliament, prime minister, banks, transportation, airport, etc., were all down for days leading up to and during the visit. Similar attacks occurred against French government websites after the country's decision to supply anti-missile warfare to Ukraine caught the attention of NoName, a key pro-Russian hacktivist groups.

Religiously motivated attacks – These types of attacks frequently occur when pro-Islamic hacktivism groups target a country or organization that they feel has insulted or harmed the Muslim faith. You may have noticed groups like Anonymous Sudan, Mysterious Team Bangladesh Dragon Force Malaysia and others become more active in the last few years throughout several different conflicts. But you don't have to be a major organization or brand on the frontlines of religious battles to feel the wrath of these attacks. In November 2023, Cloudflare was attacked because they were protecting OpenAI, which was seen by pro-Palestinian hacktivists as being associated with the pro-Israeli movement. Another notable outbreak happened during Australia's Fashion Week, when attacks occurred across the country in response to a dress that featured an Arabic statement from the Koran.

Financially motivated hacktivists – Other hacktivist groups have become more formalized and financially driven. They provide attack tools for DDoS, account takeover (ATO) or crypto ceiling services. These types of groups publicize their capabilities on their social media channels, advertising to get their audience to buy and use DDoS-for-hire and botnet-for-hire tools to attack their own targets. Anonymous Sudan's "Infrashutdown" tool is readily available for purchase online.

Evolving Attacker Tools

Hacktivists' changing attack methods have also contributed to the shifting threat landscape. New attacks go beyond just increasing in size and speed. They're more automated and sophisticated than ever, often using multiple randomization techniques to avoid traditional defenses. They're also converging different attack vectors into single tools that make up all-in-one attack platforms. And you don't have to go searching the dark web for something like the well-known MHDDoS attack tool. It's publicly available on GitHub. This tool combines 56 different attack methods, including DDoS attack vectors (HTTP/S GET, POST floods), bot attack vectors (bypass CAPTCHA impersonates Google Search Engine crawler to appear like a legitimate bot), web application attack vectors (PHP, Apache, WordPress vulnerabilities), and built-in bypass capabilities against common defenses (Cloudflare, Google Shield).

This type of multi-vector attack tool shows that modern attackers and their tools don't distinguish between WAF, DDoS protection, bot protection and so on. While organizations make the distinction between these protection areas—usually with separate teams and budgets for each—attackers don't. Organizations need to shift their approach from silo protections to an integrated platform that protects from a wide array of threats and can effectively overcome these all-in-one attack tools.

Growth in Attacker Community

Two main factors assist the recent rise in the hacker community:

Gamers Fuel Growth in Attacker Community – First, we see the transformation of everyday gamers into attackers. Four out of five attackers involved in ATO and DDoS attacks are gamers. Since the COVID pandemic, we've seen the gaming community grow by 700 million new players. If even a fraction of them cross the line into attacks, it would be a tremendous jump in growth for this group.

Hackers Broaden Reach Through Online Networks – Hackers harness social power to scale their attacks. They use their social networks as billboards and use marketplaces and hacking malls across all of these networks. These social networks allow hackers to expand their audience and get more people to participate in attacks.

AI-Powered Attack Revolution

It seems like artificial intelligence touches more aspects of life every day—and the battle over cybersecurity is no exception. When listing major developments contributing to shifts in today's threat landscape, the growing use of AI in cyberattacks cannot be ignored. Here's a look at how it works:

AI automation – Hackers use AI to automate their attacks in the same way that developers might use ChatGPT or other generative artificial intelligence (GenAI) tools to create code faster and better. Hackers can now do the same thing with cyberattacks, developing dedicated GenAI tools such as WolfGPT, XXXGPT and others to create code for malware, botnets, cryptoware, DDoS tools, ATO tools and more .

In-tool AI – More and more we are seeing AI being used in actual attack tools to create more sophisticated attacks and overcome traditional defenses like CAPTCHAs. In May 2024, a well-known DDoS tool called stresser.cat published a screen recording to demonstrate the tool's CAPTCHA-solving capabilities. The accuracy of this version of the tool stops at 77%, but it will undoubtedly increase with future iterations.

AI for zero days – Recent research has shown how hackers can now create autonomous attacks from zero-day vulnerabilities. They take common vulnerabilities and exploits (CVEs) that were published and automatically turn them into attacks. When researchers at the University of Illinois Urbana-Champaign (UIUC) tested ChatGPT 4 against a dataset of 15 real-world vulnerabilities, the tool successfully significantly outperformed other models and tools. It exploited 87% of these vulnerabilities with performance expected to improve.

What's needed to survive in the age of automated and AI-enabled cyberthreats? Fighting AI with AI. Turning to AI-based protections can help organizations stay secure in the face of attack tools boosted by AI and GenAI capabilities. Look for intelligent security that leverages AI and machine learning algorithms to stay ahead of the latest threats and keep your organization secure.

Challenge 2: New Regulatory Requirements

New regulatory requirements on processes and security tools have also made life more difficult for CISOs, security managers and C-level executives.

PCI DSS 4.0 – The Payment Card Industry Digital Security Standard (PCI DSS) 4.0 updates requirements for all entities that process, facilitate or support financial transactions. Effective March 2025, the latest PCI DSS standard adds new requirements for WAF, positive security models, API protection and client-side security. These were not part of the requirements of the previous versions.

NIS2 – The Network and Information Security Directive (NIS) 2 expands cybersecurity standards previously set for essential services in the European Union. The update includes penalties for failure to meet risk management and reporting requirements. The latest European Union directive requires maintaining application availability, such as DDoS protection solutions to be able to fully compliant and protected.

DORA – The Digital Operational Resiliency Act (DORA) creates rules for financial institutions to ensure the protection, detection, containment, recovery and repair of information and communication technologies.

GDPR – The General Data Protection Regulation (GDPR) implements standards on organizations anywhere that target or collect data related to people in the European Union. The GDPR fines anyone who fails to comply with its privacy and security standards.

HIPAA – The Health Insurance Portability and Accountability Act (HIPAA) protects medical records and other individually identifiable healthcare information. It requires safeguards, sets limits and gives people rights over their protected records.

Transparency Laws – In the US, organizations can no longer keep attacks private. The SEC requires that they disclose any cybersecurity incident material to their business within four business days. Businesses need to talk about breaches with customers publicly, and they ideally want to avoid cybersecurity incidents altogether.

CISOs can no longer look for pinpoint solutions. They need an integrated platform to ensure full compliance with these newer and stricter standards.

Challenge 3: Expansion of Hybrid Cloud Deployments

The rise of hybrid cloud deployments also creates difficulties for CISOs. More organizations are running hybrid multi-cloud environments, leveraging multiple public and private cloud deployments along with keeping the on-prem data center.

According to Radware's Application Security in a Multi-Cloud World 2023 report, 55% of organizations now run three or more environments—and 73% of organizations still maintain their on-prem hardware data centers. As a result, they need to maintain their on-prem data center, deal with multiple cloud vendors and ensure consistent protection across all these different environments.

Challenge 4: Shortages of Cybersecurity Staffing and Skills

The fourth challenge that CISOs face in today's cybersecurity environment affects almost all aspects of the job and the quality of the work. It's the real and painful shortage of experienced, qualified cybersecurity experts. According to a 2024 ISC Cybersecurity Workforce Study, 67% of organizations face shortages of security staff or skills, and there are close to 4 million open positions globally for cybersecurity roles. As a result, 45% of organizations say they can't find qualified staff. This shortage puts a major strain on security teams and limits their ability to monitor threats and respond to them in a timely fashion. How can CISOs resolve this issue? They need to look for more automated protections that require less dependency on humans. At the same time, they need to seek out expert managed services that can provide a base of expert security and manage solutions.

Part II. What's Needed to Stay Protected?

In today's world of AI-enhanced attacks, keeping your organization protected means staying ahead of the tools that drive bigger, faster and more complex attacks. We've already discussed the four key challenges. Now let's explore the key capabilities CISOs should seek out when searching for a more modern security solution.

4 Cybersecurity Capabilities for the AI World:

Intelligent Security – Matching the speed and computing power of artificial intelligence isn't easy to do on your own. Fight AI-based threats with AI-based protection through the use of intelligent security powered by AI-based algorithms.

Integrated Platform – Comply with the latest standards and regulatory requirements and combat all-in-one attack tools that combine several attack methods without targeting just DDoS protection, WAF or any one type of security. An integrated platform that correlates across a wide area of threats gives you the best protection against these tools.

Consistent Protection – Today's threats go where you go. Protect across all your environments—on-prem, public, private or hybrid—and all entry points into your applications.

Expert Defense – Overcome today's major cybersecurity staffing shortages and complex, rapidly evolving attack campaigns with help from 24/7 expert security assistance.

Only a solution that combines these four areas can drive lower mean time to resolution (MTTR), save costs and protect your brand. This is exactly what Radware provides.

How to Stay Secure in the Age of AI

360° Application Protection by Radware's Cloud Security Platform

Radware provides 360-degree protection for your applications and infrastructure with an integrated platform combining intelligent security and expert defense that is applied consistently across all your environments. We do this by infusing EPIC-AI, our AI-powered intelligence, across all areas of protection.

5 Facts About Our One-Stop, AI-powered Protection

- Defends all your mobile and web applications and APIs across all your different environments: public clouds, private cloud data centers, microservices, etc.
- Stops a wide array of threats, including web attacks, API abuse, bad bots, AI-based attacks, DDoS attacks and so on.
- Combats these outside threats with an integrated platform featuring real-time protection engines including WAF, API protection, bot manager, DDoS and Web DDoS protection, client-side protection and account takeover (ATO) protection.
- Provides full visibility and control of your network and application protection with the help of our cloud security platform, which is managed from a single portal.
- Infused by EPIC-AI's AI-powered, machine learning algorithms to handle the sophistication and complexity of today's attacks.

Part III. Introducing Radware's Cloud Security Platform Powered by EPIC-AI

So what exactly is EPIC-AI and how does it empower Radware's 360-degree Cloud Application Protection?

Radware EPIC-AI

Radware delivers AI-powered intelligence and GenAI capabilities across our cloud security platform to secure apps, reduce mean time to resolutions (MTTR) and save costs. EPIC-AI works across platforms to ensure precise, hands-free and real-time protection.

With help from EPIC-AI, Radware provides a multi-layered integrated cloud security platform that offers:

Integration across multiple enforcement points

Radware solutions can integrate across enforcement points, including our own products (Alteon and DefensePro X) and cloud services, and third-party services (from NGINX, Envoy or public cloud—AWS, Google Cloud and more). We integrate with these enforcement points to apply security policies, signatures and rules in a uniform manner, regardless of where the application resides. This unique integration approach, which is unmatched in the market, gives customers the consistent protection they are seeking across on-prem, private and public cloud environments.

Real-time cloud protection engines

Radware's real-time cloud protection engines provide WAF, bot management, DDoS protection, Web DDoS protection, API protection, account takeover (ATO) protection and client-side protection. Each of these modules gives users a best-of-breed solution that is leverage AI and machine-learning algorithms to automatically and accurately detect and surgically block malicious activity—including Web DDoS Tsunami attacks, AI-driven human-like bots and API business logic attacks.

Cross-platform Fabric

This layer connects our real-time protection engines into one integrated, holistic platform solution. It uses AI-driven source-blocking algorithms, threat intel and data-driven feeds to preemptively block malicious sources before they cause harm. Cross-model AI-based correlation and AI-powered policy tuning and recommendations go across the protection engines, allowing them to accurately detect attacks and minimize false positives and false negatives. Radware customers can see across protection engines and block malicious sources before those sources even attempt to access other applications.

SOC Management Core

Radware's SOC Management Core capabilities enable 24/7, AI-empowered managed services and automated security management and operations. Radware's AI SOC Xpert provides automated and instant resolution of incidents and accelerates root cause analysis with up to 95% reduction in MTTR. This service provides AI-powered capabilities for Radware's Emergency Response Team (ERT) to offer better and more automated managed services. It also helps organizations with their own SOC resolve incidents faster and more accurately. It provides automated and instant resolution of threats, accelerates root cause analysis and offers remediation and recommendations—even taking actions to automatically solve the incident for you. This reduces MTTR from hours to minutes with up to 95% overall reduction in MTTR per incident!

Radware also provides compliance capabilities, advanced analytics and integrations with third parties to make the experience seamless and inclusive. All of this is managed from a single-pane-of-glass integrated portal.

Case Study: AI Assists Radware in Surgical Web DDoS Tsunami Protection

The Stakes

Radware's ability to stop evasive attacks using AI-powered Web DDoS protection was put to use recently for an EMEA bank. The bank, which suffered a wave of Web DDoS attacks, faced potential financial and reputational losses associated with downtime if the attacks succeeded.

The Challenge

Stopping these attacks would have been a difficult task for a typical DDoS security solution. The scale of requests per second (RPS) reached 14.6 million, the equivalent of 14 million people attempting to access their bank account on this site every second for the duration of the attack. The duration of the attack lasted several days and featured multiple attack waves. Some waves went on for as long as 20 hours—just for a single attack!

The Solution

Radware was able to automatically stop these attacks in seconds. Using real-time automatic signature creation, it blocked all threats before they could have any impact on the bank or its end users. One of the real-time signatures included over 27 parameters to accurately control what to block and not block, so malicious traffic would be stopped while legitimate traffic gets through. All of this was done automatically with no action taken by the bank—and no impact on the bank's customers.

Radware's protection of this EMEA bank gives CISOs a clear roadmap for how they can fight AI with AI: by using AI-based algorithms to create real-time signatures within seconds.

Summary

Real-world Radware EPIC-AI: Protection Where It Matters Most

In today's rapidly evolving cyberthreat landscape, CISOs must overcome considerable challenges on the road to a more secure workplace. They face a shifting threat landscape featuring motivated hacktivists, evolving attack tools and automated AI-enabled attacks. They also have familiar headaches including a set of strict cybersecurity compliance regulations and the expansion of hybrid cloud deployments. Adding to the stress, all of this comes during a time of cybersecurity personnel and skills shortages.

Radware uses artificial intelligence to lift organizations above their challenges. It neutralizes AI-enabled threats with security solutions powered by EPIC-AI, using AI-powered algorithms and generative AI capabilities to work across platforms and ensure precise real-time protection. This gives customers an integrated platform to ensure consistency of protection across all applications and environments. It also ensures intelligent, AI-powered protection engines for real-time, accurate detection and mitigation—and creates hands-free, automated and AI-powered response for faster mean time to remediation (MTTR). Improve your security in the age of AI while reducing overhead and staffing needs. Fight AI with AI with help from Radware.