

2026

Web Application Security Report

The AI Readiness Gap



Research by

Cybersecurity

INSIDERS

Executive Summary

AI has rewritten the rules of application security. It is now embedded in the applications organizations build, the automation layers that operate them, and the attacks that target them. Adoption is accelerating faster than most security architectures were designed to handle, creating exposure that adversaries are already exploiting.

The 2026 Web Application Security Report is based on a survey of more than 800 cybersecurity professionals. It examines how organizations protect web applications and APIs as AI reshapes application architecture, the threat landscape, and defensive responses.

The findings point to a widening readiness gap between modernization and operational control:

- **Confidence in security effectiveness drops sharply as AI enters the picture:**
This report shows that overall confidence in application security posture is only 29%, and it drops further to 15% for AI-integrated applications. This is the headline paradox: near-universal adoption, minimal readiness. Organizations are deploying AI faster than they trust their ability to secure it.
- **AI-assisted attacks are rising, and breaches follow:**
AI-generated and AI-accelerated attacks now rank as the number one emerging security risk. More than half of organizations experienced a web application or API breach in the past year, and the majority report an overall lack of confidence in their ability to defend against them.
- **Conventional detection and response remain slow:**
Our report shows that nearly one-third of organizations take a month or longer to realize they were compromised, and remediation times lag just as badly. Machine-speed attacks are colliding with human-speed detection and response, giving adversaries a durable advantage.
- **Consolidation is becoming strategic:**
AI-related security risk is now the top business driver for application security investment, and only 5% are fully satisfied with their current web application security tools. In response, 62% of organizations are consolidating tools—driven primarily by simplified management rather than cost reduction. Our findings suggest that fragmented stacks cannot operate at AI speed.

Across these findings, a consistent pattern emerges. Teams are deploying technology they do not fully trust, facing adversaries that move faster than they can detect, and relying on fragmented security tools built for a slower era. Closing the AI readiness gap requires architectural simplification, unified visibility, and AI deployed where it reduces detection and response timelines. In 2026, restoring control at AI speed is a baseline for resilience.

AI Adoption Outpaces Security Controls

AI adoption in security operations continues to accelerate, with 76% of organizations now using AI or machine learning in their defenses. Yet security confidence is moving in the opposite direction, from 42% to 29%. The more organizations deploy AI in their web applications, the less confident they are in their ability to secure them – dropping to 15% for AI-integrated applications and just 12% when defending against AI-generated attacks.

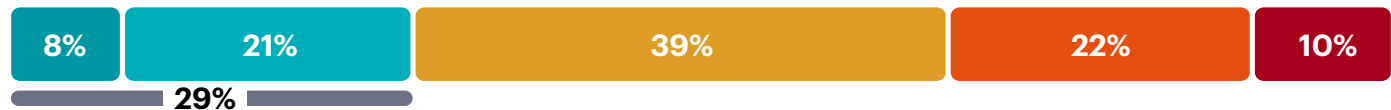
The near-overlap between the 29% who express high confidence and the 27% who report a clean year without an incident raises a harder question: does confidence reflect operational readiness, the absence of a recent breach, or perhaps lack of visibility?

That confidence gap reflects a structural gap between modern application behavior and the controls designed to protect it. Security tools built for predictable traffic and human-scale activity are now expected to operate at machine scale – inspecting model-generated payloads, monitoring autonomous service-to-service calls, and distinguishing legitimate automation from adversarial probes. Most were not designed for any of these.

Application developers push code and configuration changes daily while security policies aren't adaptive and update on review cycles. AI-integrated applications widen that gap further by changing behavior at runtime – a model that learns, a prompt chain that varies, an API call that adapts based on context. These are not static endpoints that can be inventoried once and monitored with fixed rules.

AI Lowers Security Confidence

▶ **APPLICATION SECURITY:** How confident are you in your organization's application security posture?



▶ **GEN-AI APPS:** How confident are you in the security of your LLM-powered or GenAI-integrated web applications and APIs?



▶ **AI ATTACKS:** How confident are you in your ability to defend against attacks generated by AI?



Extremely confident

Not at all confident

■ Extremely confident ■ Very confident ■ Moderately confident ■ Slightly confident ■ Not at all confident

When the security architecture cannot keep pace with the application architecture, visibility is the first thing teams lose. Organizations narrowing this gap are automating security policy updates so they deploy alongside application changes, not weeks behind them.

You Can't Defend What You Can't See

Even when policy updates keep pace, visibility remains fragile. AI-integrated services, shadow AI tools, and dynamically generated API endpoints are expanding the application footprint faster than security teams can map it. And what teams can't see, they can't protect.

Roughly one in eight (13%) of organizations report high confidence that they know all applications and APIs currently in use. Shadow AI widens the gap: 31% rank unsanctioned AI tools among their top concerns, yet GenAI services with embedded credentials and API integrations bypass standard provisioning workflows entirely.

The traditional inventory model assumes assets are provisioned through IT workflows and can be cataloged at deployment. This is almost impossible in dynamic environments where a service is built on a technology ecosystem of multiple systems and software providers. AI-integrated services amplify the challenge by self-provisioning API connections, embedding credentials at the application layer, and generating new endpoints that never pass through standard provisioning. The result is an attack surface larger and more dynamic than what current policies and tooling were designed to cover.

Most Teams Still Lack Full Asset Visibility

▶ How confident are you that you know all applications and APIs used in your organization today?

13% of organizations report high confidence that they know all applications and APIs currently in use



■ Extremely confident ■ Very confident ■ Moderately confident ■ Slightly confident ■ Not at all confident

What security teams cannot inventory, adversaries will discover for them. Organizations addressing this visibility gap are prioritizing automated API and application discovery as the foundation for every defensive layer that follows.

AI Expands the Attack Surface and Accelerates the Threat

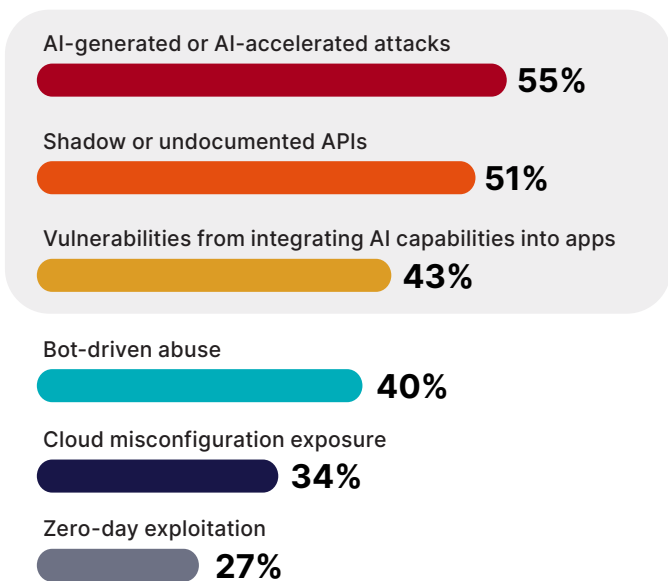
The AI-integrated applications and API endpoints that security teams struggle to inventory are also the fastest-growing targets for AI-driven attacks. AI-adjacent threats now occupy the top three positions in the risk rankings.

More than half of respondents rank AI-generated or AI-accelerated attacks as a leading risk (55%). Shadow or undocumented APIs follow closely at 51%, along with vulnerabilities introduced by integrating AI into applications (43%). These risks cluster together because AI simultaneously expands the application attack surface and accelerates exploitation. The data backs this up – a combined 74% report an increase in AI-assisted attacks over the past year, with 35% describing the increase as significant.

As organizations integrate AI into applications and workflows, they introduce new endpoints, service calls, and external model dependencies that create gaps traditional security architectures were never designed to cover. An AI agent deployed in a customer-facing workflow, for instance, may chain calls across internal APIs with service credentials, cache sensitive data in session memory, and accept natural-language inputs that bypass traditional input validation – all autonomously within a single session.

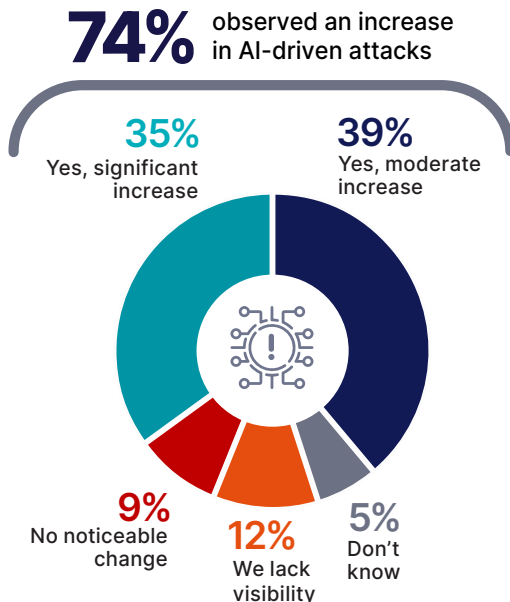
AI Now Defines the Risk Landscape

- ▶ Which emerging risks are increasing fastest in your environment



AI-Assisted Attacks Are Now Mainstream

- ▶ In the past 12 months, has your organization observed an increase in attacks that appear to be AI-generated or AI-assisted?



AI-assisted attacks exploit those gaps, testing credentials continuously, probing APIs methodically, and adapting patterns to evade signature rules and static thresholds. Organizations ahead of this curve are treating AI-integrated applications and their API endpoints as a distinct risk category, with dedicated discovery, classification, and monitoring separate from legacy application security workflows.

How Attacks Land

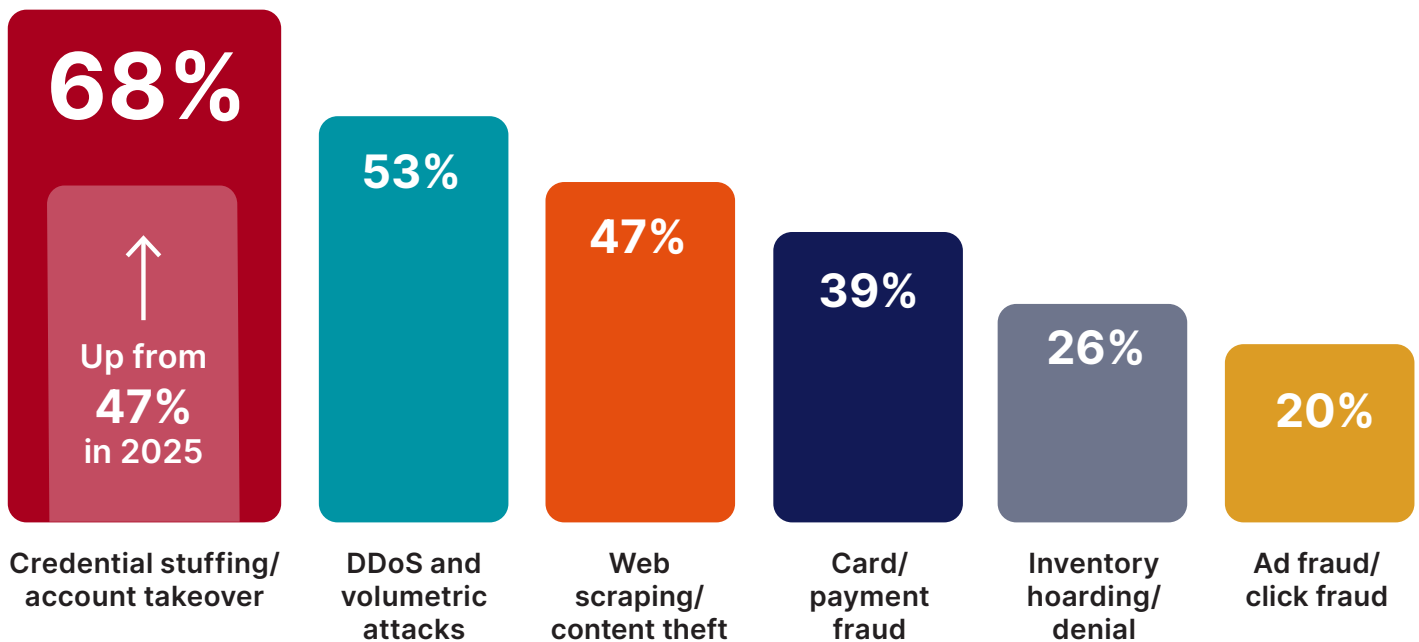
The risks are AI-driven, but the attacks target the entire application surface. The attack patterns topping the list are familiar but the speed, volume, and persistence behind them are new.

Credential stuffing and account takeover ranks as the top concerning bot-attack at 68%, a sharp increase from 47% last year. DDoS and volumetric attacks follow at 53%, and web scraping at 47%. Card and payment fraud (39%, up from 33% last year) and inventory hoarding (26%) represent the most direct financial exposure. Fraudulent transactions erode revenue immediately, while inventory denial blocks legitimate buyers from completing purchases. Credential stuffing also ranks as the most common attack type organizations experienced (58%).

Credential stuffing, DDoS, and web scraping are familiar attack types. What AI-driven bot infrastructure changes is the velocity, scale, and persistence behind them – rotating identities, fingerprints, and behavioral patterns faster than reputation lists, rate limiting, and CAPTCHA can adapt. Yet only 14% of organizations express high confidence in their ability to defend against sophisticated bots. These are known attacks at unprecedented scale, targeting defenses that can't keep up with a versatile, sophisticated adversary.

Credential Abuse Is the Primary Bot Threat

► Which types of bot attacks are you most concerned about?



Credential abuse remains effective because it operates inside normal authentication flows, blending into legitimate traffic. Organizations reducing their exposure here are layering behavioral analysis and session-level inspection on top of perimeter authentication; evaluating what each identity does after login, not just whether credentials are valid.

APIs: Highest Risk, Least Protected

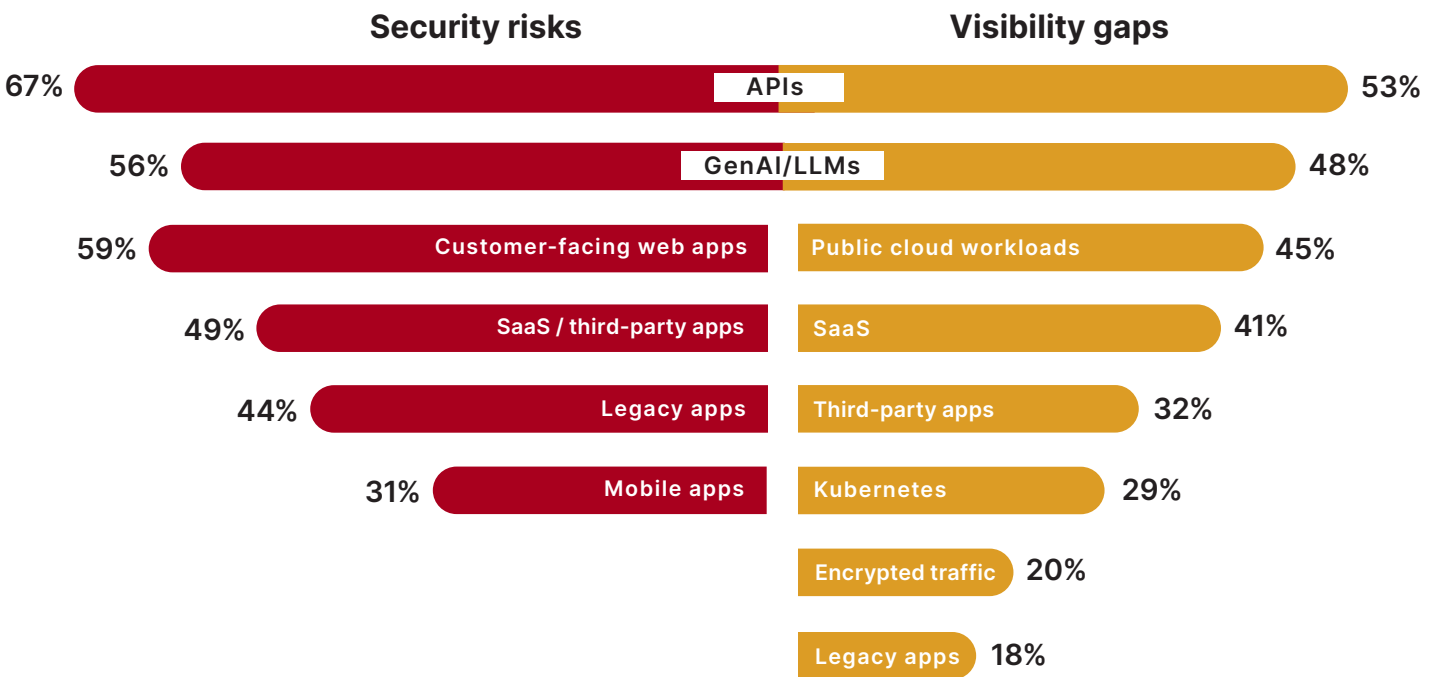
Layering behavioral analysis on top of authentication helps defend credential flows. But the biggest exposure isn't at the login page – it's at the API layer, where dynamic, complex applications are generating traffic at a volume and pace that outstrips traditional inspection, and in patterns that security controls were never tuned to detect.

APIs illustrate the report's central contradiction. They are identified as the highest-risk application category by 67% of respondents while simultaneously representing the largest visibility gap at 53%. In other words, the part of the application stack organizations worry about most is also the part they understand least. AI-integrated applications follow the same pattern, ranking near the top for both perceived risk (56%) and limited visibility (48%).

The API layer is where tooling fragmentation creates the most exposure. Cloud-native tools, standalone gateways, legacy WAFs, and embedded application-level controls each account for less than 25% of implementations, leaving inspection logic inconsistent across enforcement points.

APIs Combine Highest Risk with Lowest Visibility

► What are the highest security risks compared to greatest visibility gaps?



Organizations closing this gap are integrating API discovery, runtime protection, and policy enforcement into a single operational workflow, thereby ensuring the highest-risk category receives consistent coverage regardless of where it is deployed.

Credential Abuse and API Exploitation

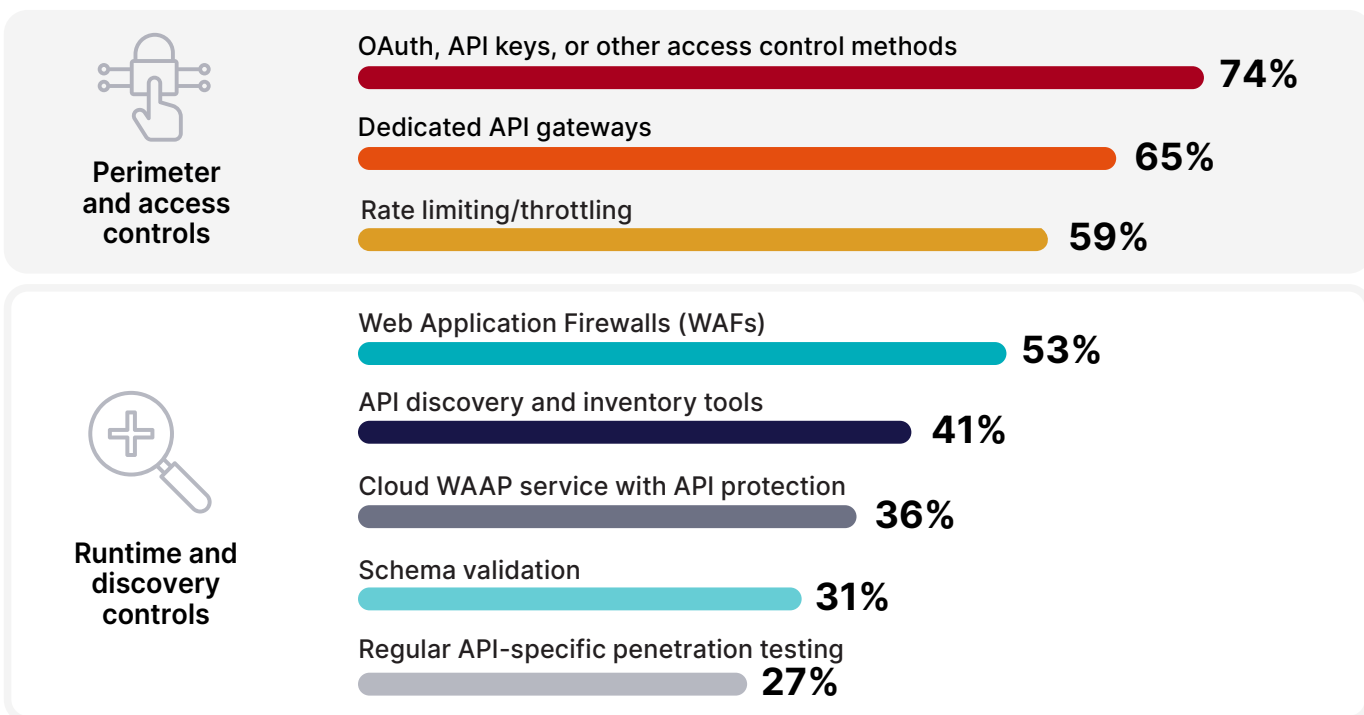
When API discovery, runtime protection, and policy enforcement operate in silos, attackers find the seams. The breach entry points confirm it: legitimate access paths now dominate over technical exploits as the primary way adversaries get in.

Credential stuffing and account takeover lead at 58%, followed by API abuse at 49% and web application exploits at 43%. These entry points succeed differently but share a common advantage: they operate inside legitimate access paths. Bot-driven credential stuffing works at scale, rotating identities and behavioral patterns to blend into normal authentication traffic; stopping it requires evaluating behavior and intent in real time to distinguish legitimate access from automated abuse before granting entry. API abuse is more targeted — an unmonitored endpoint provides the entry point, stolen credentials grant access through normal authentication flows, and the attacker inherits the compromised user's full authorization to query, extract, or modify data. Each step is individually routine; the chain is what makes it a breach.

Nearly half of organizations have experienced direct manipulation of API logic, parameters, or workflows. Yet defensive investment still favors the front door: OAuth and API keys are widely deployed (74%) and dedicated gateways reach 65%, while API discovery tools sit at 41% and schema validation at just 31%. The imbalance reflects a common assumption that authentication is the trust boundary. Once credentials are validated, session activity receives minimal scrutiny. But even the scrutiny that exists focuses on the wrong question – verifying who is calling an API reveals nothing about whether that call is appropriate, excessive, or logically abusive.

Most API Security Still Ends at Authentication

▶ How does your organization secure its APIs?



Organizations eliminating these gaps between authentication and API-level scrutiny are consolidating authentication, behavioral analysis, and API inspection under a shared policy engine with correlated telemetry.

When Breach Outpaces Detection

Even with stronger controls at the authentication and API layer, breach rates remain high. 53% of organizations experienced a web application or API-related breach in the past twelve months. The question is no longer whether compromise happens, but how quickly it is contained. Defenders are currently losing that race.

The detection and response timelines show where human-speed defense breaks down. Only 20% of organizations detect a breach within hours, and 54% take a week or longer – with nearly one-third taking a month or more. Remediation extends even further: 68% take longer than a day to contain an incident, and 39% require a month or more.

A partner API leaking records through a compromised integration token generates no alerts when monitoring depends on signature rules alone. Sometimes, the breach surfaces months later, discovered by a third party, not the security team. In the gap between compromise and discovery, adversaries have meaningful time for credential harvesting, lateral API mapping, privilege escalation, and data staging.

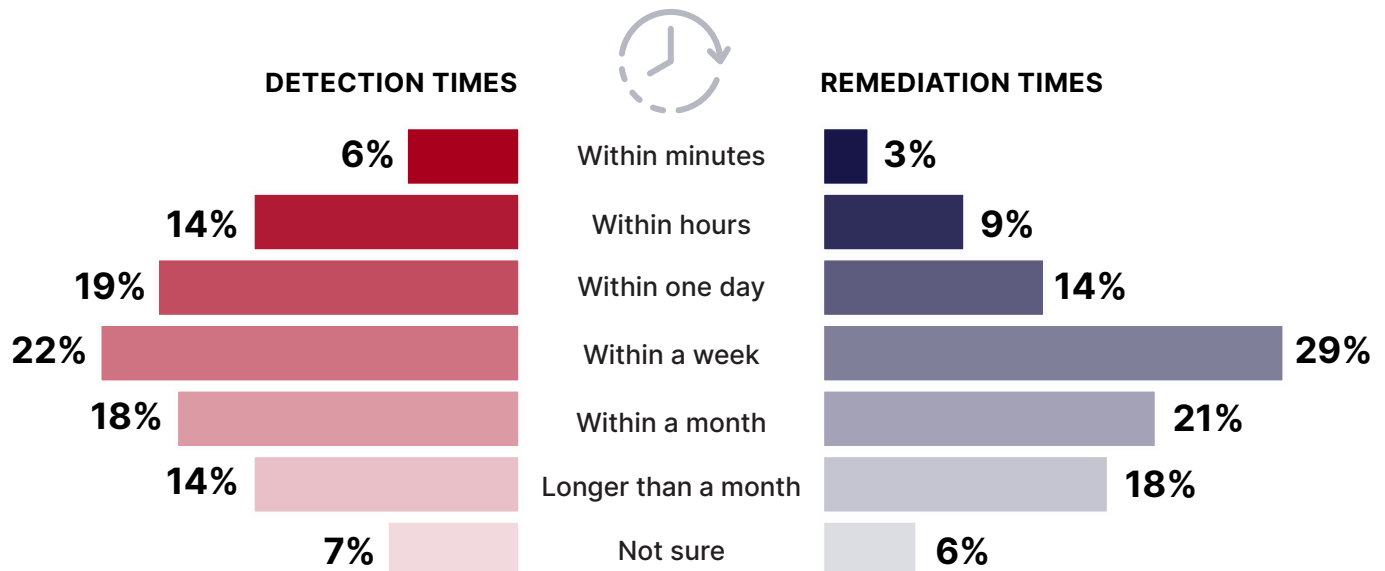
The timelines are slow for a structural reason: the signals required to understand an attack are distributed across disconnected systems. Network telemetry, application logs, API traffic, and security alerts are analyzed in separate workflows, leaving no single view of the full attack sequence. Even experienced analysts struggle to correlate these fragmented signals at the speed adversaries operate.

When enforcement layers do not share context, dwell time becomes the adversary's greatest advantage.

Detection Still Lags the Breach

▶ How quickly was the incident detected?

▶ How quickly was the incident remediated?



Organizations closing this gap are unifying detection and response telemetry across application and network layers – replacing ticket-driven handoffs with automated decision loops that can act in real time.

Post-Incident AI in a Real-Time Fight

AI in security operations serves four functions: detection, risk evaluation, decision support, and remediation. Current deployments concentrate on the decision support and remediation end. Incident analysis leads at 48%, vulnerability prioritization follows at 41%, and automated response reaches 32%. These functions address real operational pain — vulnerability prioritization ranks as the top concern at 51% — yet alert fatigue persists, triage remains slow, and remediation prioritization still depends on manual judgment. Meanwhile, 24% of organizations have not adopted AI or machine learning for application security at all.

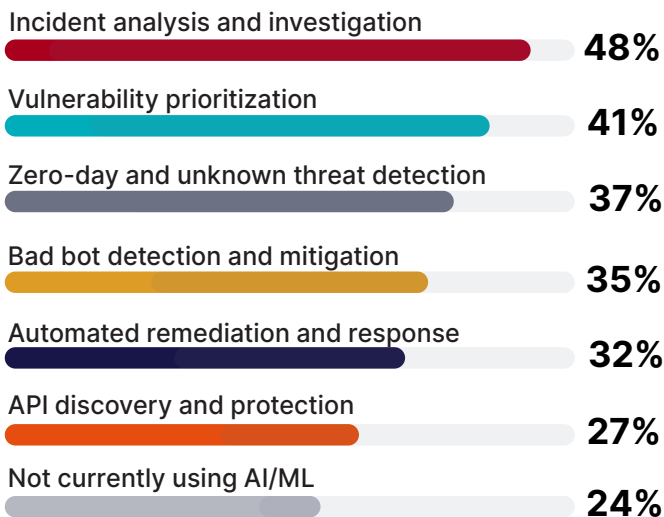
Detection and risk evaluation receive less investment despite carrying the most operational urgency. Zero-day and unknown threat detection reaches 37%, bad bot detection and mitigation 35%, and AI-driven API discovery sits at just 27%. Practitioners recognize the imbalance: faster triage (30%) and detection accuracy (26%) lead the list of where teams expect AI to deliver the greatest impact.

AI applied to detection and evaluation workflows remains uneven in maturity, and closing this gap requires both continued capability development and the foundations to support it: inline access to live traffic, shared context across enforcement layers, and unified policy.

Most Security AI Is Still Post-Incident

▶ In which areas are you applying AI or machine learning for application security?

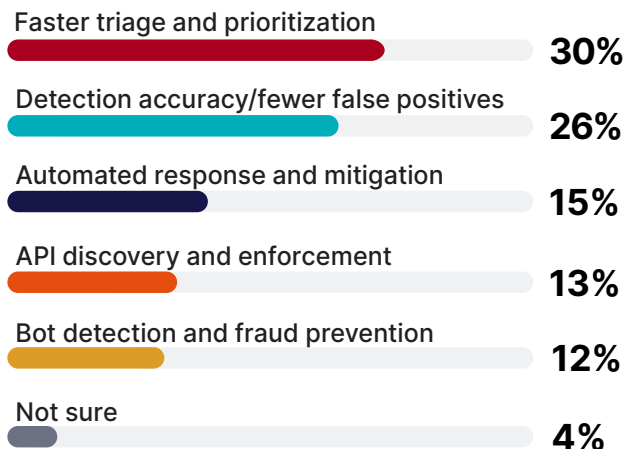
CURRENT USAGE



Teams Want AI Upstream

▶ Where do you expect AI/ML to have the biggest impact in application security over the next 12 months?

EXPECTED IMPACT



Organizations bridging this disconnect are shifting AI investment upstream — from post-incident analysis toward real-time detection, triage, and policy tuning — while retaining its value in investigation and vulnerability prioritization.

Tool Fragmentation

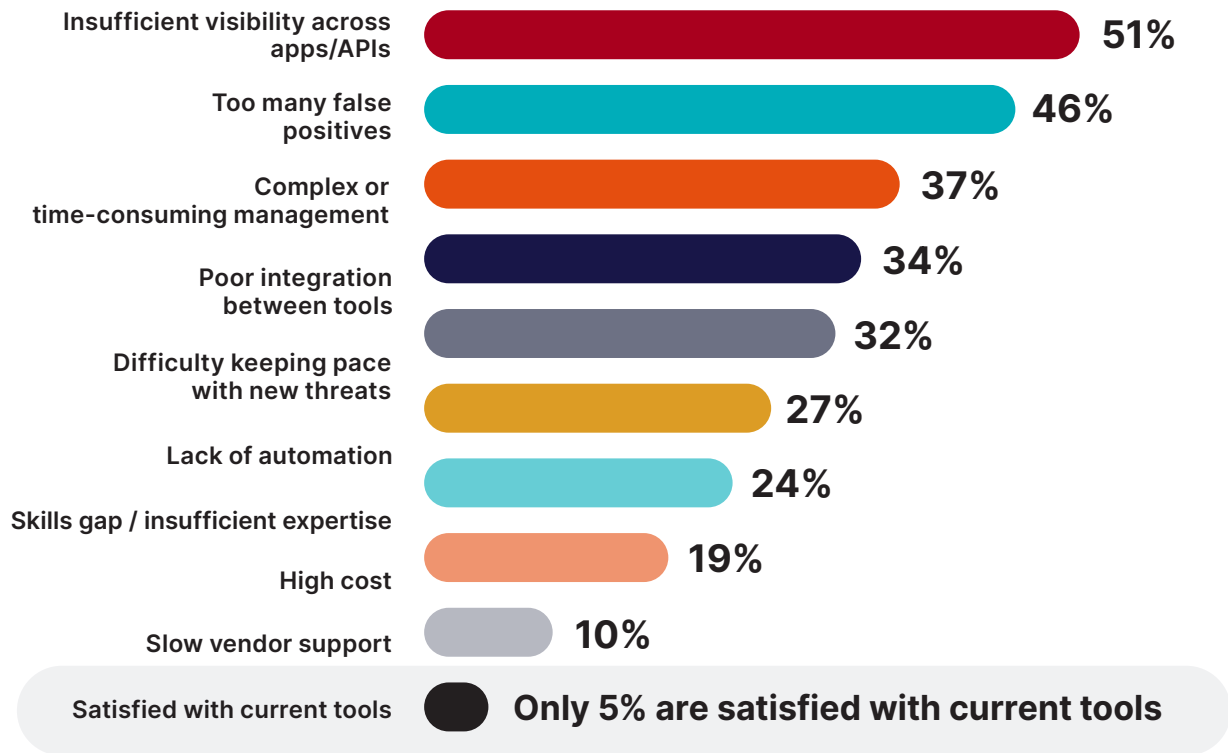
Deploying AI in the right workflows requires a security platform that can act on what AI finds. Just 5% of respondents say they are satisfied with their current application security tools.

The top cited challenge with current tools is insufficient visibility across applications and APIs at 51%. False positives follow at 46%, directly undermining detection accuracy and analyst efficiency. Complex management at 37%, poor integration between tools at 34%, and difficulty keeping pace with new threats at 32% complete the list. When asked what would most improve their security posture, practitioners reinforce the same priorities: better visibility (53%), fewer tools with better integration (45%), and fewer false positives (42%).

When inspection engines operate independently, the operational burden multiplies: policies must be duplicated, telemetry reconciled manually, and detection signals remain siloed. These demands fall on teams already stretched by persistent cybersecurity talent shortages, leaving less time for proactive threat hunting and architecture improvement.

Tool Sprawl Is Breaking Security Workflows

► What are the biggest challenges with your current application security tools?



Insufficient visibility, false positive volume, and poor integration share a common amplifier: tools operating in silos reinforce each gap rather than closing it. Organizations recognizing this cycle are looking beyond incremental tool upgrades toward unified platforms that can address visibility, accuracy, and integration as a single architectural problem.

The Solution: Platform Consolidation

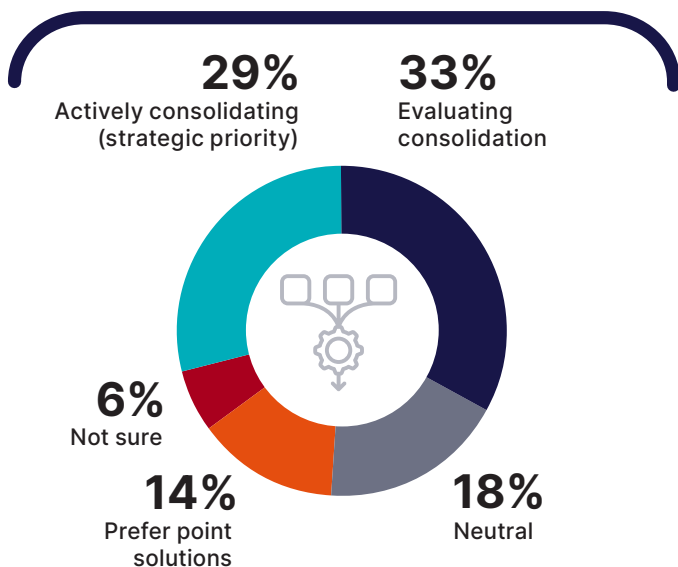
Fragmentation creates cracks that show up as visibility blind spots, inconsistent policy enforcement, or siloed detection signals. Consolidation is how organizations are closing them, and 62% are already consolidating or planning to. Of those, 29% are actively consolidating as a strategic priority and 33% are evaluating options. Only 14% prefer to continue with a specialized point solution approach. The motivations tell the story: simplified management and operations lead at 31%, followed by reduced integration complexity at 19%, faster threat detection and response at 16%, and consistent policy enforcement (14%). Reduced total cost of ownership trails at 13%.

In practice, consolidation delivers three outcomes: simpler operations, consistent enforcement, and lower total cost. Fewer consoles to monitor, fewer policies to reconcile, and one correlated view of what is hitting the application stack – instead of four or five partial ones. For security teams already stretched by talent shortages and alert volume, consolidation reduces the operational load, freeing capacity for proactive threat management instead of manual correlation across disconnected tools. Operational simplification drives cost reduction in turn — fewer licenses, less integration overhead, and a smaller management footprint.

Consolidation Is Now the Default Direction

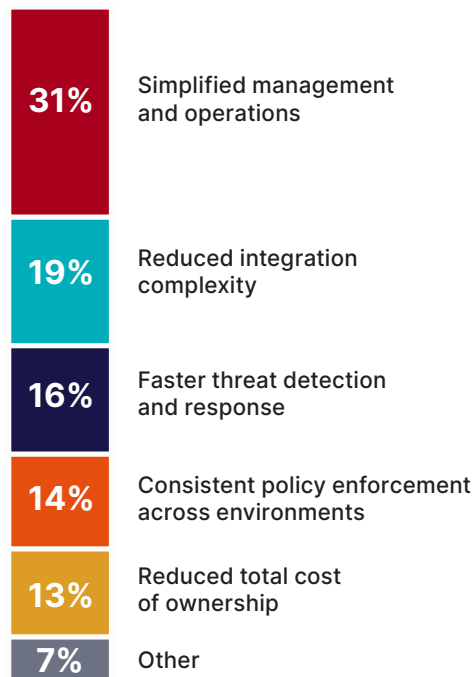
▶ Is your organization actively consolidating application security tools?

62% are either actively consolidating application security tools or evaluating consolidation options



Teams Consolidate for Control, Not Cost

▶ What is the primary operational driver behind consolidation efforts?



Unified platforms are easier to operate, ensure consistent enforcement, and save costs.

Organizations furthest along this path are consolidating policy definition and response logic on shared data — enabling consistent enforcement across cloud, on-premises, and edge deployments while reducing both management overhead and total cost of ownership.

Where Investments Are Headed

With consolidation underway, investment patterns confirm the architectural shift. The top five planned investment areas are all platform-aligned.

Investment priorities cluster into two tracks. Capability-focused investments expand what organizations protect: API security (52%), WAF/WAAP (47%), AI-driven security solutions (46%), cloud-native security (44%), and threat intelligence (42%). Operations-focused investments improve how that protection is delivered: security automation (53%), platform consolidation (48%), and staff training (36%). The two tracks are interdependent — API security without automation is manual, automation without consolidation is fragmented, and consolidation without AI-driven detection leaves the speed gap wide open.

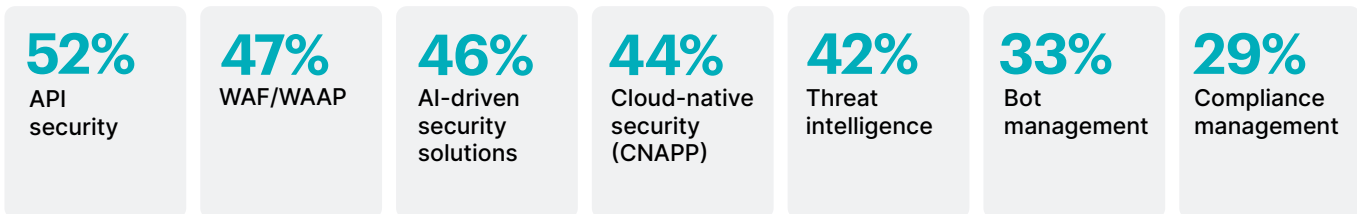
Selection criteria point in the same direction. Ease of integration leads at 48%, followed by accuracy and low false positives at 43%, and the ability to consolidate multiple functions (such as WAF, API, bot, DDoS protection) at 38%. Pricing and licensing rank lower at 21%. Security teams selecting application security platforms are prioritizing operational simplicity over feature count or cost.

AI-related risk now serves as the primary business driver for investment at 29%, ahead of cloud migration at 22%. At the same time, 56% report increasing budgets.

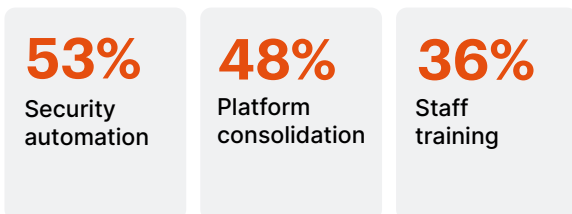
Investment Is Following the Platform Model

► In which areas does your organization plan to invest to enhance application security?

CAPABILITY INVESTMENTS



OPERATIONS INVESTMENTS



Organizations leading this shift are selecting platforms based on integration depth and enforcement breadth, and measuring success by operational outcomes rather than tool coverage.

What's Next for Application Security

The Readiness Gap Is Self-Reinforcing

Each finding in this report looks like a separate problem but together, they form a feedback loop. Security teams with poor visibility can't tune detection to the application surface they actually have. Untargeted detection floods analysts with false positives (46%), burying the signals that matter. Buried signals mean longer dwell time — 80% of organizations fail to detect a breach within the first hours. And breaches that go undetected teach teams nothing about where their blind spots were, so the cycle resets. Meanwhile, adversaries are accelerating the other side of the equation: 74% of organizations report an increase in AI-driven attacks over the past year. The gap widens from both directions at once. When the time to correlate across four or five consoles exceeds the time an adversary needs to finish a breach, the architecture has failed by design. Behind every week-long detection gap is a security team that saw the alerts but couldn't connect them fast enough, a CISO explaining to the board why the breach wasn't caught sooner, and an organization counting the cost in exfiltrated records, regulatory exposure, and eroded customer trust.

What Consolidation Delivers, and Where It Falls Short

Platform consolidation interrupts the cycle at its most actionable point: the fragmented tooling that prevents teams from seeing, correlating, and acting on threats in one place. Just 5% of organizations are satisfied with their current tools. 62% are already consolidating or planning to. The payoff is concrete — simplified management, consistent enforcement across APIs, bots, and AI endpoints regardless of deployment, and cost reduction that follows from operational simplification rather than budget cuts. But the data also exposes a sequencing issue. Organizations are investing heavily in new capabilities such as API security at 52% and AI-driven solutions at 46%, but at the same time they are investing in consolidation at 48%. Many are stacking new tools on architectures that haven't been unified yet. Capability without consolidation adds coverage without coherence, and the fragmented feedback loop persists.

From Investment to Outcome

One more pattern deserves attention. 29% of organizations express high confidence in their security posture, and 27% report a clean year without a breach. Those numbers almost certainly describe the same organizations. The overlap suggests that confidence measures the absence of a detected incident rather than the presence of strong security. Organizations with mature detection and visibility actually surface more incidents, not fewer. This means the readiness gap is likely wider than these numbers suggest, because the organizations most exposed are also the least equipped to know it.

The organizations that close this gap won't be those that spend the most or deploy the most tools. What separates them is prioritizing and sequencing: discovery first, to establish continuous visibility and break the feedback loop; followed by enforcement consolidation, to unify policy, telemetry, and response under a shared operational model; then AI-driven detection and response — deployed where it demonstrably reduces decision time, measured rigorously, and scaled where it performs.

The following principles translate that sequence into operational action.

Closing the AI Readiness Gap

Closing the AI readiness gap requires more than investment — it requires proper sequencing. A week to detect, a month to contain. In the gap between, adversaries harvest credentials across systems, map internal API dependencies, stage data for exfiltration, and establish persistence. Each principle below targets a specific link in that chain, from the visibility gaps that let attackers in, to the architectural fragmentation that slows the response.

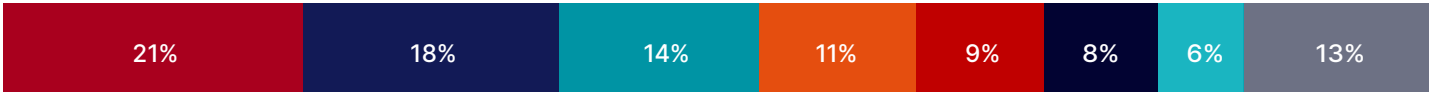
PRINCIPLE	WHAT EFFECTIVE PROGRAMS DO	WHY NOW
1 Close the Visibility Gap	Run continuous, automated discovery across all deployment environments. AI-integrated applications require separate classification — their risk profile, API dependencies, and data flows differ from legacy applications.	The attack surface is growing faster than security teams can map it manually. What remains uninventoried remains unprotected.
2 Defend Beyond the Login Page	Deploy behavioral analysis to evaluate intent before granting access — distinguishing legitimate users from automated credential abuse in real time. Layer session-level inspection after authentication to detect API logic abuse, parameter tampering, and excessive data retrieval. The login page is one checkpoint in a continuous evaluation, not the trust boundary.	Bot-driven credential stuffing blends into normal authentication traffic at a scale that rate limiting and CAPTCHAs cannot match. Targeted API abuse operates inside authenticated sessions with the compromised user's full authorization. Each requires a different defensive response, and most organizations only invest in the front door.
3 Compress the Exposure Window	Replace sequential, ticket-driven handoffs with automated decision loops that correlate signals across application and network layers. Handoffs measured in hours cannot contain adversaries that operate in minutes.	Adversaries that operate continuously exploit every hour of dwell time. The exposure window between detection and containment determines blast radius.
4 Move AI Upstream	Expand AI investment beyond post-incident forensics and vulnerability workflows toward detection and triage, where 30% of practitioners expect the greatest impact. Pilot AI capabilities in these upstream workflows, measure their effect on decision time and detection accuracy, and scale what performs.	Most security AI today concentrates in post-incident analysis (48%) and vulnerability prioritization (41%). Moving AI upstream toward detection and triage can reduce the window between compromise and containment, but maturity varies — organizations seeing results are deploying selectively and in a focused way, not broadly.
5 Unify the Platform	Bring WAF, API protection, bot management, and DDoS mitigation under shared policy and telemetry. Automate security policy updates so they deploy alongside application changes, not on separate review cycles. Managing four consoles with four policy sets produces gaps, not consistency.	Fragmented tooling amplifies every operational gap. Independent inspection engines add management overhead, increase alert noise, and drive up cost, making the visibility and accuracy challenges teams already face harder and more expensive to resolve.

Organizations that execute across all five principles — closing visibility gaps, hardening authentication and session scrutiny, compressing detection timelines, deploying AI where it demonstrably performs, and unifying the platform beneath it all — will narrow the readiness gap. Those that address them in isolation will find that each unresolved gap continues to amplify the others.

Methodology and Demographics

This report is based on a survey of 871 cybersecurity and IT professionals conducted in early 2026. The research examines how organizations are securing web applications and APIs, focusing on AI-driven threats, detection and response capabilities, tool consolidation, and investment priorities. Using a stratified sampling approach, the survey achieved a 95% confidence level with a margin of error of $\pm 3.3\%$.

CAREER LEVEL



■ Manager/Supervisor ■ Specialist ■ Director ■ Vice President ■ Consultant ■ CTO, CIO, CISO, CMO, CFO, COO
 ■ Project Manager ■ Other

DEPARTMENT



■ IT Security ■ IT Operations ■ Business Executive ■ Software Engineering/Development ■ DevOps/Platform Engineering
 ■ Compliance / Risk ■ Other

COMPANY SIZE



■ Fewer than 100 ■ 100 – 499 ■ 500 – 999 ■ 1,000 – 4,999 ■ 5,000 – 9,999 ■ Over 10,000

INDUSTRY



■ Financial Services ■ Technology, Software & Internet ■ Healthcare, Pharmaceuticals & Biotech ■ Government
 ■ Manufacturing ■ Professional Services ■ Energy & Utilities ■ Retail & E-commerce ■ Telecommunication ■ Other

©2026 Cybersecurity Insiders. All rights reserved.

Limited editorial citation (up to 100 words and one unaltered chart) is permitted with clear attribution to “**Cybersecurity Insiders, 2026 Web Application Security Report**” and a visible link to [cybersecurity-insiders.com](https://www.cybersecurity-insiders.com).

The report sponsor may reference the findings and use individual charts or data points in presentations and marketing materials with proper attribution. The full report, underlying dataset, and research methodology remain the intellectual property of Cybersecurity Insiders and may not be reproduced, redistributed, or incorporated into derivative research without written permission.

This report was produced by Cybersecurity Insiders with the support of **Fortinet**. Permissions: info@cybersecurity-insiders.com



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future.

Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, application, multi-cloud, or edge environments. Fortinet ranks #1 as a security company, with more than 900,000 clients who trust their solutions and services to protect their businesses.

www.fortinet.com

Cybersecurity

I N S I D E R S

BENCHMARK YOUR SECURITY MATURITY

Independent cybersecurity research revealing the gaps
that shape cybersecurity strategy

Cybersecurity Insiders produces independent research based on surveys of cybersecurity leaders and practitioners worldwide. Our reports reveal where security strategies break down in practice — helping organizations benchmark their maturity, identify capability gaps, and prioritize the actions needed to close them.

For more information, visit

cybersecurity-insiders.com