The State of Cybersecurity in 2025: Key Segments, Insights, and Innovations

Perspectives from leading companies shaping the industry

TABLE OF CONTENTS

Featuring

Introduction

Cybersecurity is being reshaped by forces that extend beyond individual threats or tools. As organizations operate across cloud infrastructure, distributed endpoints, and complex supply chains, security has shifted from a collection of point solutions to a question of architecture, trust, and execution speed.

This report examines how core areas of cybersecurity are evolving in response to that shift. Across authentication, endpoint security, software supply chain protection, network visibility, and human risk, it explores how defenders are adapting to adversaries that move faster, blend technical and social techniques, and exploit gaps between systems rather than weaknesses in any single control.

Authentication

Authentication sits at the foundation of digital trust — yet its core mechanisms have changed little in decades. Passwords and one-time passwords (OTPs) still underpin most access systems, even as their vulnerabilities are well understood. Phishing, credential reuse, and session hijacking continue to bypass defenses designed for an earlier era. Attackers no longer need to break encryption; they only need to impersonate a user.

Authentication now defines the perimeter of modern security. As applications, data, and infrastructure move beyond centralized networks, identity has become the primary control point for trust. Every access request — human or machine — must be verified, validated, and continuously reassessed. The strength of that verification determines the strength of the entire security architecture.

The rise of passkeys and hardware-backed authentication marks a decisive shift. Authentication is evolving from verifying *what you know* to verifying *what you have* and *who you are*. This transition replaces shared secrets with cryptographic proof of possession — a structural change in how identity is established online.

Meanwhile, the threat environment is accelerating. Generative AI has made social engineering scalable, enabling adversaries to replicate voices, faces, and written styles with precision. As these attacks blur the boundary between human and machine, confirming genuine user presence has become critical.

In this new context, identity verification must be phishing-resistant by design — hardware-bound, cryptographically verifiable, and simple enough for universal adoption.

> *"Hackers aren't breaking in — they're logging in. In an AI-driven threat environment, authentication has to be hardware-bound and phishing-resistant."*
>
> **— Ronnie Manning, Chief Brand Advocate, Yubico**

Key Trends:

- **Passwordless authentication is becoming the enterprise standard**, driven by global adoption of passkeys and FIDO2 protocols.
- **Phishing-resistant MFA is now a regulatory and operational requirement**, replacing SMS and app-based one-time codes.
- **Hardware-backed credentials provide the strongest proof of possession**, immune to credential theft and AI-driven impersonation.
- **Digital identity wallets are emerging as the next frontier**, combining convenience, privacy, and cryptographic assurance.
- **Authentication is evolving from static verification to human-linked trust.**

yubico

Ronnie Manning
Yubico
Chief Brand Advocate

Ronnie Manning, Chief Brand Advocate at Yubico, summarizes the company's mission: "Yubico's mission has been to make the internet more secure for everyone — driven by making strong, phishing-resistant multi-factor authentication simple, accessible, and universal."

Founded in 2007, Yubico pioneered the modern hardware security key and co-created the open standards — FIDO2/passkeys, WebAuthn, and U2F — that underpin passwordless authentication today. The company's YubiKey has become the global benchmark for phishing-resistant MFA, used by enterprises such as Google, Microsoft, X, T-Mobile, and by millions of individuals across more than 160 countries.

Unlike traditional MFA methods that rely on passwords, codes, or mobile devices, YubiKeys provide cryptographically bound proof of possession, in a physical security key. "Hackers aren't breaking in — they're logging in," Manning notes. "Device-bound passkeys like those stored on the YubiKey are able to stop that entirely." Each key uses asymmetric cryptography to bind authentication to both the service and the user, eliminating phishable elements such as SMS-based OTPs, push apps, or shared secrets.

Yubico's technology advantage lies in its open-standard design and device-bound architecture. Its hardware security keys work with thousands of popular apps and services, and require no batteries or mobile connectivity — just a simple tap or touch to authenticate and verify the user's identity. Once a service is trusted, users can remain signed in, combining high assurance with a frictionless experience. The company offers YubiKey as a Service subscription and YubiEnterprise Delivery to 175 countries and 24 territories.

The market's shift toward passkeys — cryptographic credentials that replace passwords entirely — has made Yubico more essential than ever. Manning explains: "Passkeys are transforming authentication from 'prove you know something' to 'prove you possess something and intend to use it.'" Yubico's device-bound passkeys strengthen this model by ensuring credentials cannot be cloned, phished, or intercepted — anchoring trust in the physical world.

AI-driven attacks have only heightened that need. Deepfakes, cloned voices, and synthetic identities have made it harder to verify who's really behind a login. "In a world where AI can fake almost anything," Manning says, "it's more important than ever to confirm you're human online. Hardware-backed authentication ties identity to a real person and requires user presence — it can't be spoofed by a machine."

Yubico's current innovations extend beyond authentication. The company is partnering with the SIROS Foundation and European research networks to develop *wwWallet*, the first passkey-enabled digital identity wallet for the web. In addition, Yubico recently announced new partnerships with HYPR and Nametag to integrate verified identity into the secure provisioning, recovery, and lifecycle management of YubiKeys. These projects reflect a broader shift toward digital identity systems where possession, intent, and privacy are cryptographically enforced.

Looking ahead, Manning expects binary trust to replace password-based identity altogether. "We're moving from trust by assumption to trust by possession," he says. "The strongest option should also be the easiest to use — and that's what Yubico is building." By anchoring trust in hardware and open standards, Yubico is enabling a future where identity is secure by design.

Yubico
Contact
Yubico
Ronnie Manning

SaaS Data Security

Modern organizations now operate primarily in the cloud. Every document, message, and workflow moves through an expanding network of SaaS platforms — from SharePoint, Google Drive and Slack to Jira, Notion, and beyond. This shift has made collaboration seamless, but it has also created a fragmented data landscape that's difficult to monitor and control.

The result is a silent, expanding web of exposure: over-shared files, forgotten integrations, and confidential information left accessible far beyond its intended audience.

As AI-powered tools connect these platforms, that exposure deepens. Unstructured data — text, messages, and documents — is now being ingested and interpreted by AI systems every day, turning previously dormant vulnerabilities into active risks.

For security teams, visibility has become the new perimeter. Knowing where data resides, how it moves, and who can access it now defines digital trust. Legacy approaches built for static, on-premise networks can't match the speed and fluidity of today's SaaS environments. Protecting data today means securing the workflows that enable collaboration itself.

Metomic was built for this reality. Its mission is to give organizations control over where sensitive data lives, who can see it, and how it's being used — transforming SaaS data security from a reactive defense into a proactive, intelligent safeguard.

> *"Most companies don't know where their sensitive data is, who has access to it, or what their AI tools are doing with it."*
>
> — **Ben van Enckevort,**
> CTO and Co-founder, **Metomic**

Key Trends:

- **Rapid SaaS adoption has outpaced traditional data governance frameworks.**
- **Unstructured, collaborative data now represents the majority of sensitive information in the cloud.**
- **Over-permissioned apps and forgotten integrations have become leading causes of exposure.**
- **AI-driven connectivity between tools is amplifying visibility and data classification challenges.**

Ben van Enckevort
Metomic
CTO & Co-founder

Ben van Enckevort, CTO and Co-founder of Metomic, captures the company's mission simply: "In today's workplace, data lives everywhere. Our mission is to protect the sensitive data that proliferates across the SaaS tools companies use every day."

Metomic's real advantage lies in automated, scalable remediation. "We can reduce permissions or fix misconfigurations automatically and at scale," explains van Enckevort. "And crucially, we involve end-users directly in the process. When our system detects risky behavior, it can prompt the employee in Slack or email with a one-click fix — making it fast and effortless for them to resolve safely."

That design choice embodies Metomic's cultural philosophy: security as a shared habit, not a bottleneck. By embedding remediation into the flow of work, Metomic helps organizations build lasting, security-aware cultures where every employee becomes a participant in protection.

The company's innovations in semantic classification deepen that capability. Rather than relying on rigid pattern-matching, Metomic's models can interpret meaning — automatically classifying entire SaaS asset inventories by sensitivity and context. "We can tag and label documents across platforms like Google Drive and SharePoint automatically," van Enckevort explains. "That context-aware intelligence helps teams manage security, streamline processes, and apply consistent data-sensitivity knowledge across all systems."

Van Enckevort foresees an arms race between AI-driven attackers and AI-powered defenders. "The risk surface area is exploding," he warns. "Any document, message, or dataset could influence an AI's behavior inside your organization." The next wave of cyber risk won't come from traditional hand-rolled malware, but from automated attackers (bots) that are looking 24/7 for any open opportunity. Context injection attacks will be a major concern for 2026 — attacks where ordinary files embed malicious instructions for privileged automated systems.

"Every single asset matters," he concludes. "You need to know where it is, who can see it, and what it contains. That's the only way to keep it safe."

Metomic represents the next evolution of SaaS data security — combining semantic intelligence, automation, and people-centric remediation to turn protection into a continuous, proactive safeguard. In an era where AI blurs the lines between data and decision-making, Metomic stands for clarity — enabling organizations to innovate with confidence, knowing their information is protected at every layer.

Metomic
Contact
Metomic
Ben van Enckevort

Network Detection and Response (NDR)

As enterprise environments become increasingly distributed — spanning data centers, public clouds, and remote workforces — network visibility has become both more difficult and more critical. Attackers exploit gaps between security tools, moving laterally through hybrid systems and operating undetected within encrypted traffic. Endpoints can be deceived, logs can be incomplete, but network activity provides the one immutable record of what truly occurred.

The challenge lies in transforming that activity into usable evidence. Traditional intrusion detection systems generate alerts; they do not explain behavior. As adversaries leverage AI-driven automation and legitimate services to mask their movements, defenders require context — not just detection — to understand intent and scope.

This is where Network Detection and Response (NDR) has become indispensable. By converting network telemetry into contextual intelligence, NDR enables security teams to reconstruct attacks, verify incidents, and strengthen overall cyber resilience. In an era of pervasive encryption and AI-powered threats, the network has become not just another data source but the definitive layer of truth — essential to digital trust and operational continuity.

Corelight embodies this evolution, combining open-source heritage with AI-driven analytics to deliver clarity where other tools see only noise.

> *"As AI reshapes security, the organizations that win will be those that know — and can prove — exactly what happened on their network."* — **Vincent Stoffer,** Field CTO, **Corelight**

Key Trends:

- **Visibility as a foundation:** Network telemetry remains the most objective source of truth across hybrid and cloud environments.
- **Beyond endpoints:** Attackers increasingly evade traditional security solutions such as endpoint protection, making network-layer evidence essential for detecting lateral movement and exfiltration.
- **Encrypted insight:** Behavioral analytics now enable defenders to interpret encrypted traffic without decryption.
- **AI-accelerated defense:** Generative AI is transforming how analysts investigate and respond, turning raw network data into real-time understanding.

Vincent Stoffer
Corelight
Field CTO

Vincent Stoffer, Field CTO at Corelight, describes the company's mission as "making the world's networks safer by turning network and cloud activity into evidence defenders can act on."

Corelight emerged from the open-source network analysis project Zeek, long regarded as a cornerstone of advanced network forensics. That heritage defines Corelight's approach to network detection and response (NDR) — transforming raw network and cloud telemetry into structured, high-context evidence that gives security teams a definitive view of activity across their environments.

Traditional defenses rely on endpoint sensors or application logs. Corelight instead operates at the network layer — the one environment every attacker must traverse. "Attackers can evade endpoint security," Stoffer explains, "but they can't evade the network itself." By translating network traffic into actionable insight, Corelight provides defenders with visibility into lateral movement, exfiltration, and command-and-control activity that would otherwise remain undetected.

As enterprise architectures expand across on-premises, cloud, and hybrid systems, this form of visibility has become essential. Corelight's platform normalizes telemetry across these domains, correlating behavior through flow analysis and encrypted traffic analytics without decryption. "Encryption shouldn't mean blindness," Stoffer notes. "You can understand intent from patterns, even when the payload is hidden." This data-centric approach reflects a broader shift in NDR — from inspecting packets to interpreting behavior.

In addition, artificial intelligence now amplifies that capability. Corelight integrates GenAI-assisted triage and model context protocols that convert network evidence into plain-language summaries, accelerating decision-making and reducing analyst fatigue. "AI helps us close the gap between data and understanding," says Stoffer. "It gives defenders the ability to interpret complex environments instantly, without losing precision."

Corelight's latest innovations — including AI-driven Guided Triage, Flow Monitoring for AWS, and integration with the Model Context Protocol (MCP) — are designed to make network intelligence accessible to every SOC, regardless of size or maturity. These capabilities transform investigation from a manual, reactive process into an automated cycle of detection, interpretation, and response. "Our goal is to meet defenders where they work," says Stoffer. "Whether their data lives on-premises or in the cloud, they should have the same depth of visibility and the same confidence in what they're seeing." This philosophy reflects Corelight's data-first vision: empowering security teams with precise, transparent evidence that drives faster, smarter, and more defensible decisions across the entire incident lifecycle.

Looking ahead, Stoffer sees NDR evolving into the connective layer that unites security operations. As organizations consolidate overlapping tools and move toward autonomous SOC workflows, the value of consistent, high-fidelity network evidence will only grow. "The network is the one place where truth persists," he concludes. "As AI reshapes security, the organizations that win will be the ones that know — and can prove — exactly what happened on their network." It's this commitment to precision, transparency, and evidence-driven defense that positions Corelight at the forefront of the next era in network security.

Corelight
Contact
Corelight
Vincent Stoffer

AI in Cybersecurity

Artificial intelligence is redefining the foundations of cybersecurity. What was once a reactive discipline — detecting and responding to breaches after they occur — is becoming an intelligent, autonomous system of defense. The speed and sophistication of modern cyberattacks have outpaced software-only protections, while the rapid expansion of digital infrastructure has made true end-to-end visibility harder to achieve.

From AI data centers to IoT networks, attackers now exploit the weakest link in a vast and interconnected chain. The same generative models used to drive innovation are being weaponized to automate attacks, craft polymorphic code, and probe vulnerabilities at unprecedented scale. Threat velocity is now measured in milliseconds, demanding defenses that operate at the same speed.

This is pushing cybersecurity closer to the hardware layer, where intelligence can act at the source of computation. The next generation of protection will be defined by hardware-anchored AI—systems that detect and respond directly at the silicon level. As the perimeter dissolves and attack surfaces multiply, integrating AI into hardware represents one of the most promising frontiers for securing critical infrastructure.

> *Software-only security can't keep up. The future of defense is hardware-anchored and AI-driven.*
>
> — **Gopi Sirineni,**
> Founder and CEO, **Axiado**

Key Trends:

- **Hardware-anchored defense:** Security is moving into silicon, enabling continuous, tamper-proof monitoring at the platform level.
- **AI as both weapon and shield:** Generative and autonomous AI are amplifying the sophistication of both attacks and defenses.
- **Zero trust at the platform layer:** Hardware-rooted verification extends zero trust beyond software, continuously authenticating users, firmware, and system processes.
- **Autonomous detection and response:** Embedded AI agents can learn, adapt, and isolate threats in real time — closing the gap between intrusion and mitigation.

Gopi Sirineni
Axiado
Founder & CEO

Gopi Sirineni, Founder and CEO of Axiado, summarizes the company's mission: "We sell AI-driven, hardware-anchored platform security. We're not replacing existing cybersecurity tools — we are augmenting them as the last line of defense."

Axiado was founded to address a structural flaw in how digital systems are secured. While most today's enterprise cybersecurity solutions defend at the software layer, and most of the at the port of entry in the application layers and at the HW port of entry, that is firewalls. Axiado embeds AI directly into the platform itself. Its Trusted Control/Compute Unit (TCU) sits beside a system's core processors, next to hard disk/storage, continuously analyzing behavior at the control and management layer where most software tools have no visibility. "It doesn't matter how the attacker got in," Sirineni explains "Once they touch the platform, data, or access, our AI detects it before it causes damage."

By embedding AI at the silicon level, Axiado delivers what Sirineni calls "autonomous platform security." The company's latest innovation — the Open Secure Agentic Framework — provides a framework and tools that allow Axiado and others to easily develop AI agents to run directly on Axiado's silicon to monitor, analyze, and act in real time. "It's the first of its kind in the market," he notes, "and our ecosystem partners can add their own agents to defend against specific attack types."

The potential impact extends far beyond enterprise systems. As data centers scale to power global AI demand, the stakes have never been higher. "AI data centers are growing fast, and protection of data is more important than ever," says Sirineni. "Software-only security can't keep up. Hardware-anchored, AI-driven security is the only way to outpace malicious actors."

By anchoring detection at the hardware layer, Axiado creates a true immutable root of trust—one that remains active even if higher software layers are compromised. This architecture provides visibility where conventional defenses fail, enabling threats to be detected and contained before they reach critical systems.

Sirineni believes this approach marks the start of a structural shift in cybersecurity. "Security has to be built in, not bolted on," he says. "The future of defense is silicon-native—where intelligence is embedded directly into the compute fabric." He predicts that AI-driven, hardware-based protection will soon become as standard as encryption, underpinning every layer of digital infrastructure from cloud servers to IoT devices.

As AI automates detection and response, the role of human defenders will evolve. "AI won't replace cybersecurity professionals — it will elevate them," Sirineni explains. "Instead of chasing alerts, they'll design the trust frameworks that keep these systems secure."

Axiado's vision defines the next frontier of cybersecurity: intelligence embedded in the foundation of computation itself. With its Trusted Control/Compute Unit, Open Secure Agentic Framework, and commitment to collaborative defense, the company is transforming security from a software function into a core property of digital infrastructure.

Axiado
Contact
Axiado
Gopi Sirineni

Human Risk Management

As cybersecurity matures, one truth has become impossible to ignore: technology alone cannot solve human risk. The majority of breaches still trace back to human behavior — from credential reuse and phishing to accidental data exposure — yet traditional security awareness programs have struggled to turn awareness into measurable resilience.

The shift from one-off training to continuous human risk management marks one of the most significant evolutions in modern cybersecurity. Instead of treating people as the weakest link, organizations are beginning to recognize them as a dynamic layer of defense — one that can be guided, measured, and strengthened through data.

The rise of AI has accelerated this change. Attackers now weaponize automation, deepfakes, and social engineering at scale, while defenders harness the same technologies to personalize training, detect risky behavior, and deliver real-time interventions. Managing human cyber risk is no longer about teaching employees what *not* to do — it's about understanding how they behave, predicting where risk will emerge, and adapting faster than attackers can.

> *Human risk management is about understanding why risky behavior happens — and changing it over time*
>
> — **Jordan Daly**
> Chief Marketing Officer, **usecure**

Key Trends:

- **From awareness to outcomes:** The focus is shifting from completing courses to achieving measurable reductions in user risk.
- **Adaptive, data-driven learning:** Platforms now personalize training and interventions using behavioral insights and automation.
- **AI-powered social engineering:** Deepfakes, voice cloning, and hyper-personalized phishing are redefining the human threat landscape.
- **Security as culture:** Human risk management is becoming an ongoing, integrated part of organizational behavior — not an annual exercise.

Jordan Daly
usecure
Chief Marketing Officer

Jordan Daly, CMO at usecure, describes the company's mission: "Our goal is to make managing human cyber risk simple, scalable, and effective for MSPs and IT teams."

usecure was built to close a persistent gap in cybersecurity — managing human behavior efficiently and at scale. Most awareness solutions stop at training delivery; usecure focuses on measurable risk reduction. Its platform automates the full human risk management process: identifying vulnerable users, delivering tailored learning, running phishing simulations, and tracking risk improvement over time.

"With usecure, it's plug and play," Daly explains. "Sync your directory, and the platform automatically creates adaptive programs for every user."

usecure's automation-first design removes the operational burden from IT teams while ensuring every employee receives training relevant to their behavior and risk profile. The platform's analytics make human risk measurable, allowing security leaders to demonstrate real progress rather than course completions.

AI now plays a central role in that mission. Attackers are using it to create convincing deepfakes and hyper-personalized phishing. usecure applies the same intelligence defensively, adapting training and interventions in real time. "By analyzing behavior and context, we can deliver the right guidance at the moment it's needed," Daly notes.

The company is extending its capabilities to monitor user hygiene — such as credential reuse and unsafe account practices — providing visibility into risks that traditional awareness programs overlook.

While many enterprise solutions target large corporations, usecure has become the preferred platform for SMBs and managed service providers, combining simplicity with measurable outcomes through multi-tenant management and automated reporting.

Daly sees this evolution changing how the industry views people in cybersecurity: "Humans aren't the weakest link — they're the most adaptable layer of defense when supported correctly."

usecure's approach turns human behavior from a persistent vulnerability into a managed component of defense. By uniting automation, personalization, and measurable insight, it equips organizations to build resilient security cultures — ones that adapt continuously and stand up to the pace of modern threats.

usecure
Contact
usecure
Jordan Daly

Network Security

Network security has undergone a decade of transformation. The old perimeter has dissolved, encryption has become standard, and zero trust has redefined access control. Yet one critical layer remains dangerously exposed — the transport layer itself. Every transaction, message, and API call leaves behind a trail of metadata that reveals who is communicating, when, and with whom. Even when content is encrypted, packet timing, routing paths, and connection fingerprints can expose valuable intelligence about organizational structure and operational rhythm. Attackers no longer need to break encryption to map a network; they simply observe its behavior.

Traditional encryption protects confidentiality, but not invisibility. The transport layer still emits observable signals that can be captured, correlated, and exploited through traffic analysis. At scale, this metadata becomes a powerful reconnaissance tool — allowing adversaries to identify high-value targets, predict activity cycles, or model dependencies between systems. The result is that even "secure" communication can reveal enough to compromise an organization's security posture before a single packet is decrypted.

The rise of AI automated traffic analysis and the looming impact of quantum computing are now amplifying that threat. Large-scale behavioral models can already classify encrypted traffic and infer sensitive operations. At the same time, state actors are recording encrypted traffic today with the expectation of decrypting it tomorrow, once quantum computing renders current cryptographic algorithms obsolete.

In this environment, the confidentiality of data in transit can no longer rely on encryption alone. Securing how communication moves — its metadata, routes, and behavioral signatures — has become as critical as securing the data itself. The next frontier of network defense will not just encrypt information; it will conceal its movement, mask its origin, and obscure its destination.

> *"Adversaries don't need to break encryption to map a network — they can track patterns, endpoints, and behaviors. That's the reconnaissance that starts every cyber kill chain."*
>
> — **Eric Sackowitz,**
> CTO & Co-Founder
> SecureCo, A Quantum Network Company

Key Trends:

- **Beyond encryption:** Protecting context as well as content — concealing metadata, routing, and network signatures.
- **AI-driven reconnaissance:** Attackers using automation and behavioral analysis to classify encrypted traffic and extract intelligence from transport-layer behavior.
- **Quantum risk preparedness:** Shifting from encryption strength to transport-layer concealment as the next layer of defense.
- **Invisible networks:** Embedding concealment and resilience directly into the transport layer so that movement itself cannot be profiled.
- **Networks and systems are expanding:** More people working from home, more servers and systems to serve the expanding users, and more sources of information expanding the network at an exponential rate thereby increasing the risk.

Eric Sackowitz
CTO & Co-Founder
SecureCo, A Quantum Network Company

David Laizerovich
President and CEO
SecureCo, A Quantum Network Company

David Laizerovich and **Eric Sackowitz** of SecureCo outline the company's mission in these terms: securing data in transit beyond encryption and transforming network communication into more stealth-based communication.

Most cybersecurity solutions protect content through encryption, but leave context exposed. "Adversaries don't need to break encryption to map a network," Sackowitz explains. "They can track patterns, endpoints, and behaviors — the reconnaissance that starts every cyber kill chain."

SecureCo's patented communications platform removes that visibility. By eliminating network signatures, metadata, and routing patterns, it conceals not only the data but the existence of communication itself. Laizerovich describes it as "making data in transit unobservable, unattributable, and undisruptable — even across contested or high-risk networks."

The platform integrates three core capabilities: **Ephemeral attribution & identity dissociation**, **Multi-layer transport obfuscation**, **and Adaptive Non-Deterministic Routing that blends real traffic into natural-looking variability.** Together, they create a moving and self-concealing communications layer where identifiers and routes shift continuously, leaving no stable signal to exploit. Even intercepted traffic yields no actionable intelligence — there is nothing consistent to analyze.

SecureCo embeds this concealment into the network itself rather than layering it on top. The result is secure connectivity without open ports VPNs, proxies, or manual attribution controls — a resilient, invisible transport fabric that simplifies deployment and reduces the attack surface.

Artificial intelligence will add an adaptive dimension. SecureCo's evolving pattern-of-life model will be learning to analyze network behavior and dynamically adjust routing and attribution in real time. "We're building networks that evolve under pressure," Laizerovich explains. "They move, adapt, and conceal like living systems."

The rise of quantum computing makes this model essential. Once quantum decryption becomes practical, static encryption will no longer be sufficient. SecureCo's approach renders data in transit uninspectable — disrupting reconnaissance before it begins and neutralizing quantum interception.

Looking ahead, Laizerovich and Sackowitz see network defense evolving toward embedded and adaptive concealment by design. "Security must exist within the network itself," says Sackowitz. "Protection can't depend exclusively on external tools or add-ons — it has to be part of how the network operates." As communications become increasingly distributed, they predict that obfuscation, attribution control, and AI-driven adaptation will become standard components of infrastructure. "Visibility will be the new vulnerability," Laizerovich adds. "The networks that survive will be the ones no one can see — and that's exactly what we're building toward."

"Every breach starts with visibility," he concludes. "If an attacker can't see you, they can't target you. Our aim is to make global communications invisible to observation — protecting not just the data, but the connections that carry it."

SecureCo is defining what comes next in network defense: a world where invisibility itself becomes the ultimate safeguard.

SecureCo
Contact
SecureCo
Eric Sackowitz
David Laizerovich

Software Supply Chain Security

As organizations increasingly assemble their software from a mix of open-source components, third-party libraries, and AI-generated code, the integrity of the software supply chain has become a defining challenge in enterprise security. Traditional code-scanning and vulnerability-management tools were built for a world where source code was accessible and predictable. That world has largely disappeared.

Today's attackers exploit modern software ecosystems by embedding malicious or vulnerable components deep within compiled binaries — far beyond the reach of conventional tools. Visibility and trust once taken for granted, has become the critical weakness. Even the creators of software often lack full awareness of what exists within their own products.

This has demanded enterprise security teams shift from reactive patching to proactive assurance. Organizations are investing in technologies that can verify, not just trust, the provenance and behavior of every component in their codebase. According to Gartner, by 2028, 85% of software-engineering teams in large enterprises will have deployed software supply-chain-security tools, up from 60% in 2025.

The next frontier of assurance lies at the binary level. To truly secure the software supply chain, defenders must move beyond surface inspection toward mathematical certainty — understanding code not by how it appears, but by what it does.

> *The problem is limited visibility into software supply chains — and that problem is only amplified with the rise of open-source and AI-generated code*
>
> — **James Hess,**
> Founder and CEO, **Unknown Cyber**

Key Trends:

- **Limited visibility into software composition is the root cause of modern supply-chain risk.**
- **The rise of open-source, third-party, and AI-generated components has amplified hidden vulnerabilities.**
- **Binary-level verification is emerging as the most reliable basis for software trust.**
- **Customer-conducted deterministic analysis is replacing vendor questionnaires and probabilistic, model-driven approaches.**

James Hess
Unknown Cyber
Founder & CEO

Born from the U.S. government's DARPA Cyber Genome Project, Unknown Cyber has developed a new method for verifying software integrity at the binary level. Its patented technology inspects the mathematical behavior of code — how it functions in register and memory — rather than relying on surface-level or model-driven analysis. "We find what other technologies can't see," explains **James Hess**, Founder and CEO. "We detect malicious or vulnerable components that traditional methods simply miss."

This low-level inspection gives Unknown Cyber a deterministic view of how software truly behaves. Unlike probabilistic systems that depend on model training or pattern recognition, its approach directly computes a function's effects on register and memory. "Once we've seen a function, we know it forever, no matter how obfuscated," says Hess. This precision enables organizations to uncover hidden risks within open-source, third-party, or AI-generated software without needing access to source code or proprietary IP. This enables Unknown Cyber to solve the software supply chain visibility problem exposed by Salt Typhoon's Snappybee/Deed RAT telecom compromises, Silk Typhoon's PlugX campaigns, NPM package hijacks, the 3CX supply chain attack, and the new wave of LOL and AI-generated attacks since SolarWinds/SUNBURST.

The company's Software Scan platform operationalizes this capability for enterprises and government agencies, enabling them to "trust but verify" their software ecosystems. It continuously validates the provenance and behavior of every binary component, proving that code is free from tampering, malware, or hidden vulnerabilities — an essential control in modern zero-trust architectures.

Hess describes the platform as a universal verification layer for software, capable of tracing the lineage and behavior of binaries across complex ecosystems. "Every organization wants to believe their software is clean," he says. "We give them the proof needed for trust." He notes that Software Scan is increasingly used in regulated and mission-critical environments, where assurance at the binary level is not optional but fundamental. "You can't defend what you don't understand," Hess adds. "Our technology makes a customer's level of understanding measurable."

Looking ahead, Hess foresees a cybersecurity landscape defined by verification rather than assumption. He believes the growing use of open-source and AI-generated code will make binary-level attestation a universal standard for software assurance. "We're entering an era where you must know what's inside your software," he says. "Trust based on documentation isn't enough. Verification at the binary level is the only path to confidence."

He predicts that over the next decade, low-level binary analysis will underpin both DevSecOps pipelines and third-party software procurement. "It's going to be the commodity solution everyone uses to assure their software — on both the development and delivery sides," Hess notes. "Security will be built in, not bolted on."

In essence, Unknown Cyber represents a technological breakthrough in how software trust is established. By bringing mathematical certainty to code verification, the company is redefining software-supply-chain security for the AI era.

Unknown Cyber
Contact
Unknown Cyber
James Hess

Open-Source Intelligence (OSINT)

Open-source intelligence (OSINT) has expanded from a specialized investigative discipline to a valuable practice used across security, fraud, and risk functions. Historically, sources were scattered across platforms, access was inconsistent and bureaucratic, and stringing together information took days. That picture has changed. Affordable and accessible OSINT tools now bring lawful collection, analysis and actionable intelligence into one place, so a single artefact — an email, alias, or phone number — can be tied to identities, infrastructure, and networks you can defend.

As communication, interaction, and activity move into digital platforms, such as social networks, forums, marketplaces, and messaging ecosystems, organizations increasingly rely on publicly available data to understand how adversaries operate, coordinate, and communicate.

Previously, OSINT was highly manual: analysts pivoted across multiple tools, sources, and disparate information, stitched together identities, and extracted evidence case-by-case. Some commercial tools attempted to scale OSINT through bulk data harvesting and centralized storage. While that approach offers coverage, it introduces issues with data provenance, legal exposure, stale intelligence, and ethical constraints, particularly in regulated environments.

Today, the shift is toward targeted, real-time OSINT that supports decision-making, not passive monitoring. Rather than face data overwhelm and manual fatigue, organizations use OSINT to answer specific investigative questions across fraud, insider threats, criminal networks, physical security, and geopolitical analysis. This increases the need for transparency in how data is collected, sourced, and applied, which is why ethical practices and integrity underpin the industry.

Public-facing digital activity has also become a meaningful behavioral signal. Criminal groups and political actors routinely coordinate in public or semi-public channels, often revealing intent through digital sources and signals. As OSINT matures, it is becoming a core source of evidence across investigations, incident response, and security operations, not a peripheral supplement.

> *Most organizations still underestimate how much threat activity is detectable through publicly available data.*
>
> — **Jonathan Couch,** CEO, **ShadowDragon**

Key Trends:

- **OSINT has shifted from manual collection to automated, targeted investigation.**
- **Real-time, selector-based collection is replacing bulk scraping and centralized data stores.**
- **Ethical sourcing and publicly available data are becoming operational requirements.**
- **AI is accelerating pattern recognition, not decision making, inferring identities or predicting behavior.**

Jonathan Couch
ShadowDragon
CEO

Jonathan Couch, CEO at ShadowDragon, describes the company's mission as "making the world a safer place by enabling every analyst and investigator with automated collection and advanced analytics of ethical OSINT."

ShadowDragon provides a comprehensive platform that allows analysts to uncover identities, behavior, relationships, and activity across publicly available online sources, including social platforms, forums, messaging ecosystems, and open websites, without accessing private accounts, bypassing protections, or harvesting data in bulk. Instead of storing or replicating large datasets, ShadowDragon performs real-time, selector-driven collection based on known indicators, such as usernames, phone numbers, email addresses, and domains. "We start with something known, collect publicly available data in real time, pass it to the user, and drop it from our system," Couch explains. "We're not downloading the internet."

The platform is built for operational investigations rather than broad monitoring or passive enrichment. ShadowDragon enables analysts to track cross-platform identities, fraud networks, illicit marketplaces, insider activity, and geopolitical operations, often where actors openly reveal intent. "The amount of criminal activity people post publicly is staggering," Couch notes. "We've seen customers identify individuals responsible for most of the fraud in entire regions simply through public data."

For enterprises, this model supports use cases beyond traditional threat intelligence, including fraud investigations, brand protection, insider-risk response, executive safety, third-party risk assessments, and geopolitical monitoring. Because data is collected in real time and not derived from pre-scraped repositories, analysts gain timely, legally defensible evidence that can support incident response, litigation, and coordination with law enforcement.

ShadowDragon supports investigative workflows by enabling analysts to pivot across selectors, correlate evidence, and integrate insights into existing case-management systems, intelligence platforms, and partner tooling. The goal is not to replace investigative judgment but to accelerate discovery with traceable, transparent evidence.

A strict ethical boundary underpins this approach: ShadowDragon does not store target data, retain user queries, or perform predictive profiling based on inferred identities. "We don't track who our clients investigate," Couch says. "Ethical OSINT means automating what analysts already do manually, not building surveillance models."

The company is expanding beyond collection to analytics that help analysts interpret unstructured data at speed, including translation, transcription, text classification, and behavioral-pattern extraction. AI is not used across the product suite other than to facilitate analysis, rather than any identity inference: "We won't use AI to guess identities," Couch explains. "It helps analysts ask better questions of the data they had already collected."

As OSINT becomes embedded in fraud prevention, national security, insider-risk programs, and cyber-physical security, ShadowDragon expects the ecosystem to consolidate around interoperable workflows rather than isolated tools. "There are too many point products," Couch says. "The future of OSINT is that it plugs directly into security, risk, and investigative operations, not a standalone discipline."

ShadowDragon positions itself as a foundational layer enabling that shift, providing real-time, ethically sourced intelligence that supports high-stakes operational decisions.

ShadowDragon
Contact
ShadowDragon
Jonathan Couch

Endpoint Security & Threat Detection

Endpoint security has become a defining battleground in modern cybersecurity. As organizations expand across hybrid networks and cloud-first architectures, attackers are exploiting gaps between devices, identities, and workloads at unprecedented speed. Credential theft, lateral movement, and hands-on-keyboard intrusions now outpace the detection capabilities of traditional signature-based tools. The endpoint is no longer an isolated asset. It is the pivot point from which adversaries can escalate privileges, evade defenses, and access sensitive data.

This environment has pushed security teams toward visibility models that capture behavior in real time rather than rely on retrospective logs. Prevention alone is insufficient. Defenders need continuous telemetry, correlated insights, and response workflows capable of matching the pace of modern threat actors. Endpoint security is evolving into a platform discipline, where identity, workload, and behavioral analytics converge to disrupt attackers before they can establish persistence. As adversaries professionalize and automate, the priority for enterprises has become clear: reduce dwell time, accelerate containment, and close the operational gaps attackers depend on.

The shift toward adversary-driven defense reflects a wider trend across the sector. Organizations are consolidating tools, simplifying detection pipelines, and relying more heavily on intelligence-led insights. The future of endpoint security lies in the ability to understand who is attacking, how they operate, and how quickly defenders can respond.

> *We're up against time when it comes to the more sophisticated threat actors*
>
> — **Zeki Turedi ,**
> Field CTO Europe, **CrowdStrike**

Key Trends:

- **Endpoint, identity, and workload security are consolidating into unified platforms.**
- **Automation is now mandatory to counter machine-speed attacks.**
- **Behavioral detection is replacing signature-based protection.**
- **Threat intelligence is becoming operational, not contextual.**

Zeki Turedi
CrowdStrike
Field CTO Europe

Zeki Turedi, Field CTO for CrowdStrike Europe, highlights how profoundly the nature of cybercrime has changed, and what this means for enterprise security strategies. “Digital forensics has always been about finding artefacts; the fingerprints and breadcrumbs of the attacker doing something they shouldn’t be doing... This time, it’s less about the investigation of what happened after the breach and more focused around making sure we can kick out the adversary as quickly as possible before the breach.”

Founded on the principle of stopping breaches rather than analyzing them retrospectively, CrowdStrike’s cloud-native Falcon platform represents this shift in practice. Instead of relying on signatures or isolated agents, the platform ingests and analyzes continuous behavioral telemetry across millions of endpoints. This allows detections to focus on how attackers behave rather than on known malware samples, closing the gap between intrusion and response.

Turedi also emphasizes that cybercrime has scaled beyond individual operators. “A lot of criminal organizations across the globe have realized that it’s a good way of making extra revenue and have invested in this space.”

This professionalization has made lateral movement one of the most dangerous stages of intrusion. As Turedi notes, “The second an adversary is moving laterally through an organization, they start rapidly crossing the network and it becomes a ‘whack-a-mole’ situation.”

CrowdStrike’s integrated approach, correlating endpoint, identity, and workload telemetry, is designed to disrupt these rapid attack paths. By unifying signals and applying adversary-focused analytics, the platform helps teams identify malicious activity earlier, reduce dwell time, and automate containment before damage escalates.

But technology alone is insufficient without secure-by-design environments. As Turedi explains, “Where we have problems is when security is an afterthought. That’s where we end up ‘Sellotape and gluing’. They have gaps that the adversary makes use of.”

For defenders, this means prioritizing architecture that closes systemic weaknesses rather than layering reactive controls. CrowdStrike’s intelligence-driven model supports this by continuously tracking adversary groups, mapping their tools and methods, and feeding that insight directly into detection logic.
Looking ahead, Turedi stresses the urgency of speed as a defining success factor for defenders. “We’re up against time when it comes to the more sophisticated threat actors. That time window is really important... If we know how quick the adversary is, we now know how quick we need to be.”

By combining cloud-delivered analytics, continuous behavioral telemetry, and adversary intelligence, CrowdStrike is shaping a new standard for endpoint resilience. In a landscape where attackers move in minutes, not days, the future of defense will be defined by how quickly security teams can detect, understand, and stop intrusions.

CrowdStrike
Contact
CrowdStrike
Zeki Turedi

Autonomous Endpoint Security

Endpoint security is evolving rapidly as adversaries deploy increasingly sophisticated techniques that blend evasive malware, automated exploitation, and identity-based lateral movement. Traditional detection and response models built around signatures and manual workflows struggle to keep pace with high-velocity attacks that leverage automation and machine learning. As enterprise environments decentralize across cloud, edge, remote workforces, and hybrid infrastructures, security teams face growing pressure to scale detection, containment, and response without proportionally increasing human effort.

In this context, platforms that combine real-time visibility, machine-speed automation, and unified control across endpoints and workloads are gaining traction. Modern cyber defense increasingly requires tools that move beyond reactive alerting toward autonomous threat management, where detection, prioritization, and response can occur with minimal analyst intervention. Organizations are consolidating security tools to reduce complexity, improve signal quality, and shorten time to resolution, recognizing that speed and context are now foundational to resilience.

This evolution reflects a broader shift across cybersecurity. Fragmented point solutions are being replaced by integrated platforms that unify prevention, detection, response, and threat intelligence. SentinelOne's approach to autonomous security aligns with this shift, emphasizing large-scale telemetry and AI-driven analytics to stop attacks before they escalate.

> *We're trying to simplify our AI for our customers in a bid for them to be able to better digest it*
>
> — **Meriam El Ouazzani,** Regional Sales Senior Director - Middle East, Türkiye, and Africa, **SentinelOne**

Key Trends:

- **Endpoint, identity, and workload security are consolidating into unified platforms.**
- **Automation is now mandatory to counter machine-speed attacks.**
- **Behavioral detection is replacing signature-based protection.**
- **Threat intelligence is becoming operational, not contextual.**

Meriam El Ouazzani
SentinelOne
Regional Sales Senior Director - Middle East, Türkiye, and Africa

Meriam ElOuazzani, Regional Sales Director at SentinelOne, highlights the role of artificial intelligence in reshaping how enterprises defend against modern threat actors. Addressing the gap between innovation and real-world adoption, she explains, “Everybody is talking about AI, but I think where the disconnect comes from is the fact that no one has been able to show them how to use AI in cybersecurity domain. We’re trying to simplify our AI for our customers in a bid for them to be able to better digest it.”

This focus on usability reflects SentinelOne’s broader objective of enabling security teams to benefit from advanced automation without adding operational friction or cognitive overload.

ElOuazzani describes how SentinelOne is advocating for enterprise-wide security strategies that remove silos between tools and teams. Rather than deploying isolated solutions for endpoint, cloud, and identity security, organizations are increasingly prioritizing unified platforms that simplify management and accelerate response. As she notes, “We are providing an end-to-end cybersecurity platform, and we’re no longer looking at solutions sitting inside silos, we’re bringing them all together under the one platform... It is much easier for the customer in terms of automation and management, and it is designed to accelerate simplicity.”

A central component of this strategy is SentinelOne’s integration of generative AI capabilities, including Purple AI, into the Singularity platform. By enabling natural-language interaction with security data, these tools accelerate investigation and response workflows while reducing reliance on highly specialized expertise. ElOuazzani highlights the operational impact of this shift, stating, “Purple AI allows us to use simple language and we can implement and transform that into complex queries... Traditionally, before the advent of AI... you would’ve required an analyst to do that process.”

As organizations adapt to hybrid work models, cloud expansion, and rising identity risk, demand continues to grow for security platforms capable of operating across endpoints, identities, and cloud environments. While endpoint protection remains foundational, enterprises increasingly require defenses that address automation-driven attacks and identity abuse, priorities that SentinelOne continues to incorporate into its platform roadmap.

By combining autonomous threat hunting, AI-enhanced analytics, and unified platform orchestration, SentinelOne is helping organizations reduce dwell time and operational complexity. In an environment where adversaries increasingly rely on automation, the ability to detect, interpret, and respond at machine speed is becoming a defining requirement for modern cyber defense.

SentinelOne
Contact
SentinelOne
Meriam El Ouazzani

Overview

Across the areas explored in this report, a consistent shift is underway. Cybersecurity is moving away from static controls and isolated tools toward models built around continuous verification, shared context, and rapid response. As infrastructure becomes more distributed and attackers more coordinated, effectiveness is increasingly determined by how well security systems operate together under pressure.

Authentication is transitioning from passwords and one-time codes toward cryptographic and hardware-backed verification. Endpoint security is converging around behavioral telemetry and machine-speed response as dwell times continue to compress. Software supply chain protection is evolving from process-driven assurance toward verifiable integrity at the code and binary level. Network visibility remains critical, even as defenders confront the risks that exposure itself can introduce. At the same time, human behavior continues to shape outcomes, reinforcing the need for security models that address both technical and organizational factors.

Taken together, these developments point to a broader realignment in cybersecurity. Trust is no longer assumed but continuously established. Speed has become a defining variable, and architectural decisions increasingly determine whether defenders can detect, understand, and contain threats in time. The direction is clear: security is becoming more integrated, more automated, and more deeply embedded into infrastructure, setting the foundation for how cyber defense will operate in the years ahead.

Explore case studies, research, and product resources from each contributor

Yubico
→ View case studies

Metomic
→ View case studies

SecureCo
→ View case studies

Corelight
→ View case studies

Axiado
→ View case studies

ShadowDragon
→ View case studies

Unknown Cyber
→ View case studies

usecure
→ View case studies

CrowdStrike
→ View case studies

SentinelOne
→ View case studies