CROWDSTRIKE

Logged In and Undetected:

Stop Identity Adversaries with Unified Identity and Endpoint Security

CrowdStrike eBook

Table of Contents

The New Front Line of Cybersecurity: Identity Meets Endpoint

Modern adversaries have fundamentally evolved their tactics. Cyberattackers have expanded their attention beyond vulnerable user endpoints to cloud workloads. In addition to writing zero-day exploits to avoid detection at the endpoint, attackers leverage a wide range of identities — including human, non-human, AI, and SaaS — to directly access systems and bypass traditional security. In fact, 81% of interactive intrusions were malware-free from July 1, 2024, to June 30, 2025, highlighting a shift toward hands-on-keyboard attacks that seamlessly blend with legitimate user activity.[1]

As attackers have broadened their focus to include identities and identity-based attacks, so too must an organization's defenses. To protect against today's modern threats, organizations must extend their endpoint security into identity security, powered by adversary-driven threat intelligence. However, simply adding a standalone identity solution to the tech stack can be a step back in efforts to reduce cost and complexity. Worse yet, attackers thrive in the blind spots between siloed security tools, making a fragmented approach more of a liability than a defense.

By unifying cybersecurity tools and intelligence, organizations can eliminate redundancies, reduce blind spots in visibility, and centralize investigations, ultimately leading to a stronger and more efficient system of defense. With myriad security tools in the tech stack, organizations should prioritize their consolidation efforts on a security platform that can mitigate the biggest areas of risk and have the largest impact on the organization's overall risk posture.

1. CrowdStrike 2025 Threat Hunting Report

With that in mind, here are five reasons to start consolidation efforts with endpoint and identity:

- Protect the hybrid identity attack surface
- Respond to threats faster
- Stop advanced threats that circumvent traditional defenses
- Reduce costs
- Improve operational efficiencies

According to Gartner, by 2028, 30% of enterprises will adopt preventative endpoint security, endpoint detection and response, and identity threat detection and response from the same vendor, up from approximately 5% in 2024.[2]

2. Gartner, 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms (EPP), Sept 23, 2024, Evgeny Mirolyubov, Franz Hinner, Deepak Mishra, Satarupa Patnaik, Chris Silva

Reason #1

Protect All Identities Everywhere — Human, Non-Human, AI, and SaaS

The hybrid identity environment — where organizations are leveraging on-premises tools like Active Directory (AD) and cloud identity providers like Entra ID or Okta — expands the identity attack surface, introducing new risks. Once inside with valid credentials, attackers can leverage hybrid lateral movement techniques to seamlessly pivot across on-premises and cloud systems. Additionally, SaaS applications and AI-powered identities further expand the attack surface, giving adversaries additional opportunities to exploit identity gaps, weak controls, and misconfigurations across human and non-human accounts.

Unfortunately, identity-driven attacks are extremely hard to detect. When a valid user's credentials have been compromised and an adversary is masquerading as that user, it is often difficult to differentiate between the actions of the user and those of the attacker, especially without any critical adversary context.

Adversaries seamlessly exploit identity gaps across multiple environments, making unified endpoint and identity security essential. By consolidating endpoint and identity protection in a single platform, organizations gain full visibility into adversary tradecraft.

A unified approach enables real-time, high-fidelity access decisions by correlating identity signals with device trust data. For example, by integrating endpoint telemetry — such as risk scores, privilege levels, and sensor status — identity systems can dynamically enforce stronger authentication requirements, block access, or require identity verification like external authentication methods (EAMs) for hybrid resources.

Cross-domain response is another major advantage. If an endpoint detection tool flags a credential access attack using Mimikatz, a unified platform can automatically add the affected user to an identity watchlist, triggering additional security controls and adaptive policies. This seamless combination of endpoint and identity security, underpinned by rich threat intelligence, strengthens defenses against hybrid identity attacks.

"The smartest adversaries will know your environment as well as you do — in many cases, they may know it a lot better than you do, and the whole idea is to slip through the cracks, to generate fewer detections, to fly under the radar."

Mike Sentonas
CrowdStrike President

Reason #2

Respond to Threats Faster

Adversaries aren't just getting more sophisticated — they're getting faster. Every year, the time it takes for an attacker to infiltrate a target and begin moving laterally decreases. The average time it takes an eCrime adversary to break out and move laterally dropped to a mere 48 minutes in 2024 while the fastest observed time was just 51 seconds.[3] Meanwhile, as point solutions continue to stack up, the time it takes for security analysts to gain visibility — let alone begin investigating an attack — increases.

Consolidating endpoint detection and response (EDR) and identity security in the same platform provides full visibility of the attack path, enabling faster, more precise detections of potential breach attempts across the digital estate. By centralizing cross-domain telemetry in a single console and providing a single underlying data fabric, a unified platform empowers analysts to spend less time pivoting between tools and more time acting on high-fidelity alerts.

3. CrowdStrike 2025 Global Threat Report

This enhances a security team's ability to quickly detect and address vulnerabilities or suspicious activity with greater accuracy and fewer false positives. Additionally, with automation at scale, threats are detected and neutralized in real time — without adding to the team's workload.

Unifying identity and endpoint security enables up to 85% faster response times, potentially offsetting thousands of investigation hours annually.[4]

4. These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

Reason #3

Stop Advanced Threats that Circumvent Traditional Defenses

As attackers sharpen their strategies, they are increasingly targeting weak points for initial access, making the threat landscape harder to defend. In 2024, for example, 52% of vulnerabilities observed by CrowdStrike were related to initial access, while access broker advertisements increased by 50% year-over-year.[5]

Modern attacks increasingly bypass traditional security controls and exploit valid credentials across hybrid environments. Further complicating threat detection is the rapid expansion of identity-based attack vectors, allowing attackers to move effortlessly across environments by leveraging human, non-human, AI, and SaaS identities.

For example, CrowdStrike observed PERCUSSION SPIDER selling high-value domain administrator credentials across critical sectors such as government, oil and gas, and technology. This adversary specializes in obtaining and selling privileged access, often via underground forums and private communication channels, with ransomware operators among its buyers. While endpoint protection defends against ransomware deployment and spread, identity protection is critical for stopping threats that exploit valid credentials to monetize compromises.[6]

5 CrowdStrike 2025 Global Threat Report

6 Outpacing Adversaries: Defending Against Identity-Based Threats

Unifying endpoint and identity security under a single platform is the only effective way to get full visibility into attack paths covering all aspects of adversaries' tactics, techniques, and procedures. Unifying endpoint and identity telemetry and leveraging real-time correlation of threats with threat intelligence and adversary tradecraft enable organizations to stop the full attack life cycle. Furthermore, this unified approach with a single sensor provides flexibility to enforce security policies at either the endpoint or the identity level to quickly stop an attack.

Reason #4

Reduce Costs

The push to protect identities while reducing costs is accelerating the process of combining endpoint and identity security, which maximizes effectiveness and streamlines expenses.

By leveraging the endpoint security budget for a unified solution, organizations eliminate the need for separate identity security line items. This consolidation allows unified protection for all identity types — human, non-human, AI, and SaaS identities — through the same agent deployed for endpoints. Additionally, a unified platform that correlates identity threat data with endpoint data and advanced threat intelligence provides more robust, proactive protection.

Teams also gain the deep visibility needed to proactively address identity hygiene issues and implement stronger controls, ultimately lowering audit and compliance costs.

By consolidating endpoint and identity protection, organizations can save:

- **Up to $2 million USD over three years**
- **Up to 75% in compliance and support costs[7]**

7 These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

Though cost reduction is often a primary driver for consolidation, it is easy to underestimate the hidden costs that arise from operating multiple tools.

Organizations with plans to consolidate have nearly 50 security tools on average across their entire estate.[8] Consolidating endpoint and identity protection allows for cost reduction by:

- Eliminating legacy systems and redundant tools
- Streamlining the supply chain
- Centralizing vendor management
- Centralizing product support
- Reducing the operational overhead associated with deploying, updating, and managing the cybersecurity tool stack

Combining endpoint and identity protection can also help reduce cyber insurance premiums, which have increased in recent years as a result of the rise in ransomware and identity-based attacks. Ryan Melle, SVP/CISO of Berkshire Bank, says, “CrowdStrike helps improve our risk posture and subsequently our insurability because of its strong reputation and leadership in the space.” For Berkshire Bank, the partnership with CrowdStrike is valuable because it delivers ongoing platform enhancements to address evolving security challenges, particularly in Zero Trust and identity protection.[9]

8 IDC Survey, How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans?

9 Berkshire Bank Accelerates Digital Transformation and Multi-Channel Customer Services with CrowdStrike

Reason #5

Improve Operational Efficiencies

Staff shortages and the sheer volume of work security organizations face require them to operate as efficiently as possible. But the operational complexity of managing multiple tools introduces one inefficiency after another. Managing separate identity, SaaS, and endpoint solutions adds vendor complexity, varied negotiations, and fragmented updates, highlighting the need for unified security. Furthermore, to overcome the difficulty of orchestrating automated responses across multiple standalone tools, analysts often need to manually correlate threats across endpoints and identities.

The answer to this problem is consolidation.

Organizations that deploy a consolidated endpoint and identity platform can see up to an 84% improvement in efficiency, reducing headcount by as many as four full-time employees.[10]

10 These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on the individual customer's module deployment and environment.

A single, cloud-native platform alleviates critical operational pain points associated with managing multiple standalone tools. A consolidated endpoint and identity platform enables security teams to deploy thousands of agents in a matter of minutes without requiring time-intensive configuration. A unified platform also makes it possible to rapidly deploy new protections — such as defenses for identity security — via a single agent.

After adopting CrowdStrike, Land O'Lakes realized the following efficiencies[11]:

- 92% faster at investigating and responding to identity-related attacks and anomalies
- 90% less time spent manually auditing identity hygiene
- 85% less time prioritizing vulnerabilities
- 80% reduction in accounts with excessive permissions
- Consistent removal of stale accounts
- Immediate and automated response to compromised passwords

Note: Consolidation does not mean simplifying tools. Consolidation simplifies the user experience, putting the most relevant information at the analyst's fingertips while still enabling detailed threat hunting and investigation.

11 Endpoint and Identity Security: A Critical Combination to Stop Modern Attacks

“CrowdStrike’s endpoint and identity protection are like peanut butter and jelly … they’re good by themselves but when you put them together, you’ve got something special.”

Jason Strohbehn
Deputy CISO, The State of Wyoming

“The fact that we can deploy CrowdStrike EDR and identity protection from the same platform and sensor saves us time while closing security gaps.”

Steve Tieland
Director of Corporate Security Operations, Pegasystems

Bonus Reason

You Can Get It from an Industry Leader

The security market evolves rapidly, so to adapt and stay ahead of emerging threats, it's important to partner with a vendor that's at the forefront of innovations. For this reason, leading organizations around the world choose CrowdStrike.

CrowdStrike is a global security leader offering organizations a unified platform from a single, trusted security partner. The CrowdStrike Falcon® platform unifies endpoint and identity telemetry along with advanced threat intelligence and adversary tradecraft expertise, delivering real-time threat detection and response to stop attacks in their tracks.

CrowdStrike deploys a lightweight agent to endpoints that seamlessly bridges the gaps between cloud, endpoint, and identity protection. This means organizations don't have to rely on disjointed agents or compromise on endpoint performance.

The Falcon platform consolidates security management into a single, unified console, allowing teams to see and stop advanced threats across their entire IT landscape. It also delivers intuitive context and anticipates analyst workflows, empowering teams to accelerate from detection to remediation and improve overall security effectiveness.

Logged In and Undetected:
Stop Identity Adversaries with Unified Identity and Endpoint Security

CrowdStrike pioneered EDR, shaping the foundation of today's Falcon platform — a single agent and single platform delivering comprehensive protection across endpoint security, IT hygiene, identity security, cloud security, data protection, adversary threat intelligence, elite threat hunting, and more — shutting down the most advanced adversaries in record time. And CrowdStrike's unique adversary-driven approach uncovers the most elusive threats with tactical precision, delivering high-quality, context-rich detections with minimal false positives.

CrowdStrike Falcon® Next-Gen Identity Security detects and stops identity-driven breaches in real time across human, non-human, AI, and SaaS identities. A single sensor and a unified threat interface with attack correlation protects identities across endpoints, cloud workloads, SaaS applications, identity stores, and data repositories.

With CrowdStrike, organizations can avoid the burden of juggling separate licenses and tools, which can introduce multiple supply chains to learn, manage, patch, and maintain as well as multiple potential sources of vulnerabilities. With CrowdStrike, organizations have a single trusted security partner and an ever-growing partner ecosystem to manage their security.

Sign up for an Identity Security Risk Review

With Falcon Identity Protection, a composite organization reduces the risk of a breach by 50% and achieves a 310% ROI, with a payback period of under six months and $1.26 million USD in total benefits over three years.[12]

12 Forrester, The Total Economic Impact™ Of CrowdStrike Falcon Identity Protection

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **www.crowdstrike.com**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

Follow us: **Blog | X | LinkedIn | Facebook | Instagram**