CROWDSTRIKE

THE COMPLETE GUIDE TO Next-Gen Identity Security

What You'll Learn in This Guide

The Complete Guide to Next-Gen Identity Security is your essential resource for safeguarding your organization's digital identities.

Within these pages, you'll find the information you need to build a roadmap for understanding and developing a modern cybersecurity strategy to secure every identity — human, non-human, and those powering AI agents — across the full identity lifecycle. You'll uncover insights into how a unified identity protection strategy can deliver business benefits, including better security outcomes, improved operational efficiencies, and cost optimization.

This guide examines the challenges decision-makers face — such as supporting business transformation and innovation without compromising security — and provides insights into how to help your security team stop breaches and gain time to focus on their highest priorities.

Quick Tip: Understanding Identities in IT

Identities refer to user objects within a system that require access to resources. These can be broadly grouped into three categories:

- **Human identities:** These are tied to a real individual, such as employees, contractors, and partners, and are used to access various systems and applications
- **Non-human identities (NHI):** Sometimes called machine or service identities, these are used by applications or services to interact with other applications or systems. They play a critical role in automation, integrations, and backend operations.
- **AI agents:** These are autonomous or semi-autonomous systems that make decisions, interact with other systems, and take actions on behalf of users or organizations.

Securing all three types is foundational to modern identity security and to protecting your organization from the increase in identity-centric attacks.

Table of Contents

Chapter 1
The Identity Challenge

Before we can discuss the details and functionalities of safeguarding identities, it's important to first understand the threat landscape and how the need for next-gen identity security emerged.

The Rise of Identity-Based Attacks

Identity-based attacks aren't new, but they continue to wreak havoc. And the unsettling news is that adversaries often use stolen credentials to move fast and stay hidden. They're no longer breaking in — they're logging in.

This trend is partly fueled by the success of identity attacks and access brokers as well as the widespread abuse of valid credentials to gain access to victim environments. Access brokers — threat actors that obtain access to organizations and sell it to other adversaries on the dark web — are akin to facilitators in a modern-day cybercrime marketplace, and CrowdStrike observed a 50% year-over-year increase in access broker activity in 2024.[1]

[1] CrowdStrike 2025 Global Threat Report

The Shift from Breaking In to Logging In

Imagine a threat actor armed with valid credentials that allow them to effortlessly stroll into your organization's digital estate. From there, they can seamlessly navigate through the entire infrastructure, using what's known as hybrid lateral movement — where adversaries move between on-premises identity providers and the cloud, or vice versa. Cloud environments and SaaS applications are increasingly vulnerable to this tactic. The trend is underscored by the fact that 38% of organizations experienced at least one SaaS application breach in 2024.[2]

Why are these developments significant? The shift from breaking in to logging in signifies a fundamental change in how adversaries operate. They're no longer relying on brute force or complex malware to infiltrate systems. Instead, they're exploiting the credentials your organization depends on to verify your users, customers, and partners.

Today's adversaries are like digital chameleons, blending seamlessly into your environment by using stolen or compromised credentials. Once inside, they can move laterally across an organization's on-premises and cloud environments and access endpoints.

Quick Tip: Breakout Time

After gaining access to a network, adversaries seek to "break out" by moving within it, gathering information, establishing control, and pinpointing their targets. "Breakout time" refers to the time it takes them to do this.

Examples of identity-based attacks

Identity-based attacks go after user credentials, permissions, and access rights. Instead of targeting network infrastructure or devices, attackers focus on exploiting identity systems like Active Directory or cloud-based providers. Some examples include:

Credential stuffing

Cybercriminals use stolen login credentials from one system to attempt access to an unrelated system.

Pass-the-Hash

Adversaries use a hashed user credential to authenticate without needing the original plaintext password.

Phishing

Attackers trick users into revealing their login credentials through deceptive emails, messages, or websites.

Password spraying

Attackers try common passwords against a large number of accounts, hoping to find one that works without triggering account lockouts.

[2] Based on internal research and data analysis from CrowdStrike Falcon® Shield, reflecting security threats identified across customers who have experienced at least one high-severity alert.

The Speed of Modern Threats

Detecting these threats is challenging because they look like legitimate users, which is especially worrisome given how fast adversaries move. In 2024, the average observed eCrime breakout time — the time it takes for an adversary to move from an initially compromised host to another within the organization — was a mere 48 minutes. The fastest breakout time observed was 51 seconds.[3]

Market Factors Fueling Identity Attack Success

Why are identity-based attacks so successful? The answer lies in a couple of market factors. First, some businesses still take a checkbox approach to identity security, relying on incomplete incumbent tools that don't provide full protection. Further, from an operations perspective, the teams managing identity and access management (IAM) are often different from those handling security. As a result, identity is seen more as a provisioning and deprovisioning task rather than a critical component of security operations.

Opportunistic adversaries are constantly on the lookout for targets with the highest potential for exploitation. Microsoft's extensive footprint in identity management makes these customer environments a prime focus. With 90% of Fortune 1000 companies relying on Microsoft Active Directory (AD) and many also using Microsoft's cloud identity solution, Entra ID (formerly Azure AD), for multifactor authentication (MFA) and single sign-on (SSO) capabilities,[4] Microsoft's hybrid identity environment presents a vast attack surface.

The hybrid identity environment where on-premises AD integrates with Entra ID presents an opportunity for adversaries to pivot from on-premises systems to cloud environments. Once they gain sufficient permissions in AD, they can replicate accounts and modify email addresses that synchronize to Entra ID.

[3] CrowdStrike 2025 Global Threat Report
[4] Frost & Sullivan, Active Directory Holds the Keys to your Kingdom, but is it Secure?

The COZY BEAR (aka Midnight Blizzard, APT29, and Nobelium) breach detailed on the right illustrates this risk. COZY BEAR, a Russian state-nexus adversary, compromised Microsoft's corporate systems using straightforward identity attack techniques like password spraying and credential scanning. This breach underscores how even the most robust infrastructures can be vulnerable when they become prime targets for sophisticated threats.

Additionally, SaaS applications running in the cloud represent a large opportunity for adversaries to exploit identities. SaaS cloud spend and adoption continue to increase — with enterprises owning an average of 106 SaaS applications in 2025.[5] A 2024 report from Onymos also highlighted that 45% of tech leaders experienced a SaaS cybersecurity incident in the past year.[6]

COZY BEAR

COZY BEAR was observed using credential theft to access cloud environments, including Microsoft 365 tenants, as a foundational tactic. The threat actor was able to subvert authentication with a single-sign-on (SSO) provider, with multifactor authentication (MFA) enabled, by stealing session cookies stored in Chrome browser profiles. Cookies stolen within a valid session time window can be saved in an adversary-controlled web browser installed on a compromised machine in a target environment; these can be then used to authenticate and access services.

As AI adoption accelerates, a new and largely ungoverned identity risk is emerging: AI agents. These are classified as non-human identities (NHIs) and are being deployed across SaaS environments to automate tasks, trigger workflows, and interact with sensitive systems and data. Yet in most organizations, there's no visibility or control over what these agents are doing, who authorized them, or whether they've been misconfigured, over-permissioned, or exposed to risky inputs.

Each AI agent inherits the privileges of the identity that created it — privileges that attackers can exploit if the agent or its controlling identity is compromised. That access can be used to escalate privileges, exfiltrate sensitive AI artifacts, or modify production code, turning trusted automation into a high-speed attack vector. In fact, 80% of surveyed organizations reported that their AI agents have taken unintended actions, including accessing unauthorized systems (39%), accessing inappropriate data (33%), and allowing inappropriate data to be downloaded (32%).[7] These behaviors reflect the growing risk of unmanaged automation operating without clear identity or security oversight.

[5] BetterCloud, 2025 State of SaaS
[6] Onymos, The SaaS Disruption Report: Security and Data
[7] Sailpoint, AI agents: The new attack surface

What's at Stake?

Identity-based attacks don't just put sensitive data at risk — successful attacks can also have serious financial and reputational consequences.

The average cost of noncompliance was $14.82 million USD in June 2025, marking a steep 45% increase over the past decade.[8] This highlights the escalating financial burden organizations face due to noncompliance in the midst of evolving regulations.

The financial repercussions aren't confined to penalties alone. Cyber insurance premiums often increase after a breach, and legal costs can mount as the perception of risk grows. These increases are a direct response to insurers' escalated concerns over the frequency and severity of cyber incidents originating from identity breaches. Organizations must also consider the intangible yet vital aspects of brand integrity and customer trust. A breach isn't just a hit to a brand's reputation — it can also erode customer loyalty.

Chapter 1 Recap

Identity-based attacks pose substantial risks to organizations. The market is witnessing a marked increase in attacks that no longer use malware to gain initial access, and these attacks continue to succeed. Once inside with valid credentials, attackers often have unrestricted access, leveraging hybrid lateral movement techniques to move across the organization's on-premises and cloud infrastructure.

A pivotal factor contributing to the success of these attacks is the incomplete approach many organizations take toward identity security, treating it as a mere checkbox rather than a core element of their security strategy. This oversight introduces vulnerabilities that adversaries are quick to exploit.

Compounding this issue is the opportunistic nature of today's attackers. The hybrid identity environment — spanning human, non-human, AI, and SaaS identities — creates a prime target for cybercriminals. These attackers target environments where there's a vast identity management footprint, using it as a gateway to infiltrate customer systems and exploit any weaknesses they find.

The next generation of identity security demands depth and a single-minded focus to outpace adversaries. In response to these market dynamics, a unified identity protection strategy has emerged as a bedrock of effective cybersecurity. This proactive approach ensures organizations aren't just reacting to attacks but are actively fortifying their identity infrastructure against future risks.

[8] Colligo, The True Cost of Non-Compliance

Chapter 2
The Cracks in Conventional Identity Security

Despite the alarming rise in identity-based attacks, many organizations still rely on fragmented methods to protect themselves. The gaps in traditional security operations centers (SOCs) stem from a reliance on insufficient resources and mismatched tools, often reflecting the disconnect between what identity teams manage and what security teams monitor. These shortcomings leave organizations vulnerable to identity abuse, allowing cybercriminals to sneak through the front door undetected.

In this chapter, we dive into the flaws in today's approaches and discuss why these outdated methods fail to keep up with the evolving threat landscape.

The Patchwork Approach

Identity security has evolved rapidly through the years, driven by the growing sophistication and success of identity-based threats. Early security methods were simple: Passwords and usernames were the gatekeepers of sensitive information. As digital landscapes expanded, so did adversaries' tactics, pushing organizations to explore additional identity security measures.

However, this rapid evolution invariably led to a piecemeal approach to identity security technology. Identity started as a way to manage access, not secure it. IAM solutions were built to provision users and authenticate logins — not to detect malicious behavior or stop identity abuse. As identity-based threats grew more sophisticated, organizations layered on MFA and SSO, identity threat detection and response (ITDR), privileged access, and identity auditing tools. But this approach led to a fragmented defense system. Each tool addressed a narrow piece of the problem, was often from a different vendor, and lacked the ability to communicate or coordinate.

For instance, an organization might have an IAM system that controls user access but lacks the ability to detect identity-based attacks in real time. Or they might employ identity visibility tools to monitor user behavior without integrating a directory service compliance tool to ensure all activities align with company policies. Additionally, they may have a SaaS security posture management (SSPM) tool that is not unified with identity infrastructures to provide attack path visibility across hybrid environments. This becomes even more challenging because SaaS identities often operate independently from traditional identity providers, creating fragmentation across the identity plane and making it harder to enforce consistent protections. Each of these tools is an important piece of the puzzle — but without a holistic approach, they fail to provide comprehensive identity protection.

Overreliance on Endpoint Protection

Endpoint detection and response (EDR) plays a crucial role in managing security threats, offering valuable insights and protection for corporate endpoints. However, relying solely on EDR for identity security can be limiting. Though EDR is effective for detecting and responding to threats at the endpoint level, it does not fully address the complexities of identity-based attacks.

Relying on EDR alone overlooks identity security for unmanaged devices, which can be a gateway for attackers. Threat actors can initiate attacks from unmanaged hosts — such as contractor laptops, rogue systems, and legacy applications and protocols — as well as parts of the supply chain where organizations lack visibility and control.

To safeguard against the full range of identity-based threats, it's important to look beyond EDR and explore next-gen identity security tools. A unified approach addresses both endpoint-specific and broader identity-related risks.

Navigating Siloed Tools

Adversaries thrive in dark places — like the blind spots between security tools. And there are a lot of blind spots: SOC teams often juggle dozens of security tools, a troublesome scenario that hinders detections and leads to delayed response times.[9]

When identity security isn't unified across key capabilities — including identity visibility solutions, ITDR, secure privileged access, and SaaS security spanning on-premises and cloud environments — security gaps can emerge. These gaps grow when identity security tools aren't natively integrated and can't use intelligence from the organization's endpoint and cloud security solutions.

[9] IDC, North America Tools and Vendors Consolidation Survey, 2023: Insights on Consolidation Plans

Without a unified security strategy, adversaries can launch cross-domain attacks. A cross-domain attack occurs when adversaries target multiple areas of an organization's security stack — such as endpoint, identity, and cloud — to evade detection. They typically use legitimate tools and compromised credentials to blend in with normal operations and move laterally across systems. This makes it difficult for security solutions to track their actions within a single domain.

These shortcomings make a compelling case for a unified approach to next-gen identity security, which removes adversaries' ability to operate between siloed security tools. Adversaries are adept at jumping from identities to endpoints, from on-premises environments to the cloud. If your identity security strategy doesn't provide a comprehensive view of the attack path, you're likely to miss signs of a breach.

Navigating separate products, agents, and consoles creates a perfect storm of inefficiency for security teams. They must manually piece together data from disparate tools to quickly detect threats, trace their origins, and contain them — all within a shrinking breakout time. On average, it takes 276 days to identify and contain a data breach that spans multiple environments, underscoring the monumental challenges security teams face in combating these threats.[10]

Chapter 2 Recap

Identity security is facing a critical moment. Despite the advances in technology, many organizations remain tethered to fragmented approaches that can't keep up with today's sophisticated threats. This patchwork approach to identity security, with its mix of isolated tools from different vendors, leaves glaring gaps in protection that cybercriminals are eager to exploit.

Relying only on EDR as a sole security strategy is another major pitfall. Though EDR systems are valuable, depending on them for identity security overlooks threats from other attack vectors and unmanaged devices, leaving significant security gaps.

Compounding the problem, security teams are often overwhelmed by the inefficiencies of managing identity security that's not unified on a single platform. This disjointed approach not only delays threat detection and response but places a heavy burden on security teams, leading to slower response times.

[10] IBM, Cost of a Data Breach Report 2025

Chapter 3
Exploring Modern Identity Security Capabilities

In this chapter, we'll establish the essential capabilities for a next-gen identity security strategy that offers unparalleled protection, streamlined management, and greater efficiency. We'll show how integrating identity, EDR, and cloud security data into a single platform can bridge visibility gaps and fortify your defenses across all attack surfaces. And, we'll explore key considerations for architecture and deployment to ensure you're equipped for the modern threat landscape.

Single Platform with Endpoint and Cloud Security

A next-gen identity security solution takes a fundamentally different approach by unifying the capabilities you need to combat adversaries from the start. It integrates comprehensive identity management into a single platform that also includes endpoint and cloud security. This integration ensures every facet of identity security operates in unison, providing a robust and unified defense against evolving threats.

Today's typical endpoint and cloud environments are inundated with new identities — human, NHI, and AI agents — especially as more organizations need to support and protect a hybrid workforce. The complexity of cloud infrastructure and remote work expands attack surfaces and reduces the visibility of new identities, making effective security even more critical.

As cloud infrastructure becomes more complex, the risks grow, with attackers seizing opportunities to exploit misconfigured instances. Navigating end-to-end identity visibility in this maze to secure the full identity lifecycle is no small feat, especially when dealing with hybrid setups, multi-cloud environments, and diverse identity stores. The more intricate your cloud setup, the trickier it is to keep an eye on every endpoint and identity.

Integrating your organization's identity security with EDR and cloud security provides you with a comprehensive defense strategy. This unified approach simplifies oversight, with a single pane of glass to see, protect, and extend conditional access, and sharpens your ability to detect and respond to threats. This turns complexity into clarity and fortifies your overall security posture.

By consolidating identity, endpoint, and cloud security into a unified platform, you gain full visibility into the attack path across all layers of your digital infrastructure. This comprehensive view enables you to see how threats traverse through identity systems, endpoints, SaaS applications, and cloud environments, providing a panoramic view of potential threats. By correlating telemetry data across these domains, you can proactively protect against identity-based attacks — no matter where they occur. This unified perspective amplifies your ability to spot and eliminate risks before they escalate, giving you the strategic edge in securing your environment.

With a unified system, you can identify and neutralize threats in real time using telemetry data from all security domains. This speeds up your response and ensures actions are based on a full understanding of the incident's impact. Plus, with increased MITRE ATT&CK® coverage, you're better equipped to outsmart even the most sophisticated attackers.

Leveraging a unified platform converts security from a tangled web into a clear strategy, ensuring all components of your security infrastructure work together. As the threat landscape evolves, embracing this unified platform approach is crucial for maintaining robust security.

End-to-End Visibility

With a next-gen identity security strategy built on a unified platform, you achieve unparalleled end-to-end visibility across your hybrid identity environments. This means integrating with on-premises AD, cloud-based identity providers such as Entra ID and Okta, and SaaS environments to gain a cohesive view. This all-encompassing visibility lets you keep a watchful eye on every identity — human, non-human, and AI agents, along with the identities powering them — from a single vantage point, eliminating blind spots where attackers can thrive.

This approach provides a framework for robust identity security posture management (ISPM) to monitor and analyze identities, access rights, and authentication processes across your entire ecosystem. This gives you insights into your identity risk profile and guidance on how to prevent identity-based attacks before they start. By maintaining this level of oversight, you can proactively address vulnerabilities and ensure compliance with regulatory requirements.

Real-Time Protection

The race against cybercrime is won by those who can act faster than attackers, and real-time protection provides that decisive advantage. Building on end-to-end visibility, the ideal solution must empower you to stop threats and fraud across both on-premises environments like AD, cloud identity providers like Entra ID, and SaaS applications. By extending real-time protection across your entire identity landscape, you gain the upper hand to outpace attackers and secure critical assets.

Equally important, a security strategy driven by a unified platform enhances your SOC practices with proactive speed and efficiency that ensure you're not just responding to threats but anticipating them. With a unified system, you can harness threat telemetry from across identity, endpoint, and cloud environments to deliver accurate and effective real-time protection. This integrated approach means that as soon as an anomaly is detected, the system can immediately cross-reference this behavior with identity and endpoint data.

For example, if an endpoint suddenly shows activity that deviates from established patterns — like a user logging in from a new geographic location or at an odd hour — this behavior is flagged as suspicious. The unified platform instantly disseminates this information across all security layers, enabling swift and coordinated responses like isolating the endpoint, enforcing MFA, or implementing other escalated security measures. Real-time protection should also extend to privileged actions, ensuring elevated access is granted only when needed and automatically revoked the moment risk levels change.

By integrating real-time telemetry and automated responses, your security framework can detect and address threats as they arise and adapt to evolving attack vectors. This rapid, cohesive response is crucial in the race against the adversary.

Risk-Based Conditional Access

Risk-based conditional access is essential for navigating today's complex threat environment. Conditional access is a set of customizable rules that determine whether access to corporate data is granted or denied based on factors such as device type, location, unusual behavior, device settings, and various other conditions. This capability allows you to dynamically manage access based on real-time risk assessments, helping to ensure that your security measures are responsive and intelligent.

At the core of risk-based conditional access is the ability to detect and respond to anomalous authentication activities as they occur. Your system continuously monitors account sign-ins to determine the likelihood that a sign-in was performed by someone other than the authorized account holder. By identifying risky access attempts in real time, you can slam on the brakes before any threat can shift into high gear.

When risky authentication behavior is detected, risk-based conditional access activates MFA to add an extra layer of security. MFA requires users to provide additional verification, such as a one-time code sent to their phone, before granting access. So even if a threat actor tries to exploit a vulnerability, they face an additional hurdle. Risk-based conditional access helps ensure that your system preserves a smooth user experience for those who don't pose a risk while remaining vigilant against adversaries.

Essential Architecture Elements

A cloud-native identity security solution leverages the inherent benefits of the cloud, such as elastic scalability, rapid performance, and minimal administration overhead. This means you can deploy it quickly and efficiently, avoiding the burdens of traditional on-premises solutions.

Cloud-native architecture enables your next-gen identity security solution to grow with your organization and dynamically adjust to handle evolving data and security demands. The solution's elasticity enables you to process and analyze data at scale so you can maintain swift performance to detect emerging threats in real time. With this architecture, you're equipped to address evolving security challenges without the need for constant manual intervention or costly upgrades.

And when it's built to be AI-native, that's when the real acceleration happens. Agentic AI helps detect threats faster and triage them automatically — surfacing high-risk identity behaviors like credential theft, privilege abuse, and anomalous activity in real time. It enables dynamic detection and response that alerts and acts simultaneously, with real-time remediation built in to reduce manual effort and stop identity-based attacks faster.

Another crucial element is ease of management. The solution should be intuitive and straightforward to deploy so your organization can quickly start realizing its benefits. A user-friendly interface and streamlined management processes reduce the learning curve for your staff, enabling them to focus on priority initiatives rather than getting bogged down in complex configurations or ongoing maintenance tasks. It's not just about making their lives easier — it's about unleashing their potential to drive innovation and security excellence.

Chapter 3 Recap

In today's digital battlefield, securing your organization demands more than just vigilance — it requires a strategy that's both dynamic and unified. A modern identity security strategy hinges on a unified platform that natively integrates identity, EDR, and cloud security data. This single platform approach bridges visibility gaps and fortifies defenses across your attack surface, delivering robust protection and streamlined management.

A next-gen identity security strategy requires a holistic approach that encompasses advanced authentication methods, precise authorization controls, and efficient identity life cycle management. These elements work in harmony to eliminate security gaps, bolster defenses, and ensure only the right people have access to sensitive data and resources.

Next-gen identity security flips the script on traditional identity security measures by transforming your approach from reactive to proactive — enforcing real-time threat protection, applying conditional access based on risk, and eliminating standing privileged access with just-in-time enforcement. By unifying identity protection across endpoint protection and cloud security, your system can detect and neutralize threats as soon as they arise. Swift, automated responses to anomalies help keep your defenses sharp and your data safe.

Risk-based conditional access takes security a step further by dynamically managing access based on real-time risk assessments. Detecting anomalous authentication activities and enforcing MFA ensures your security measures are smart and effective, maintaining productivity while keeping bad actors at bay.

The architecture of your identity security solution is paramount. A cloud- and AI-native approach offers seamless scalability, intelligent automation, and real-time threat response — all within a solution that's easy to manage and quick to deploy. By pairing elasticity with AI-powered detection and agentic triage, your identity security system accelerates time-to-value and adapts as quickly as threats evolve — keeping your defenses sharp and your team ahead.

Chapter 4
Identity Protection Use Cases

If you're a security professional, you understand better than anyone that the SOC serves as the nerve center of your organization's defense against the relentless tide of cyber threats. A unified identity security solution represents a technology leap forward and enables your SOC to improve operational efficiencies and deliver better security outcomes.

In this chapter, we dive into real-world use cases that show the true power of unified identity security. It's not simply about managing access to company resources — it's about leveraging identity to fortify the layers of your security strategy. By understanding and applying these use cases, you'll see how a comprehensive identity security framework can transform the way your SOC operates, driving efficiency and delivering the security outcomes that keep breaches at bay.

Preventing Privileged and Service Account Misuse

Valid user and service account credentials are a treasure trove for adversaries. When attackers get ahold of your privileged accounts, the stakes are even higher because they offer broader access to sensitive resources across your digital estate. With stolen or compromised credentials and phishing ranking among the top attack vectors, it's clear the current methods of protecting service and privileged accounts are falling short. For the third year in a row, phishing was among the top attack vectors. Vendor and supply chain compromise followed closely behind, overtaking compromised credentials as the number two attack vector.[11]

[11] IBM, Cost of a Data Breach Report 2025

When attackers gain access to credentials, they can slip through poorly configured environments with ease, sidestepping the need for complex malware. This direct access allows them to identify and exploit over-privileged users, roles, and even service accounts, further entrenching themselves within an organization's digital infrastructure. What makes this even more dangerous is their ability to deploy legitimate remote management tools instead of detectable malware, making their attacks stealthier and harder to interrupt.

Privileged Account
A user account with more access rights and permissions than a standard account. It allows users to make significant changes to a system, such as modifying configurations or accessing sensitive data. Since these accounts are more dangerous when abused, it's especially important to prevent unauthorized use.

Modern identity blocks adversaries by enforcing least privilege access without adding complexity. Just-in-time access for privileged users is an increasingly adopted strategy, providing users with elevated access only when needed and revoking it the moment risk levels change. This not only reduces the attack surface but also eliminates the risks of standing privilege.

A unified identity security solution takes the guesswork out of defending against misuse of privileged access and service accounts by delivering comprehensive control over access. It continuously monitors privileged access across both on-premises and cloud identities, enabling enforcement of risk-based access policies in real time. By securing machine-to-machine interactions and cloud integrations, it safeguards all non-human identities, ensuring even the most complex workflows are protected.

By centralizing and automating identity defenses, you can ensure over-privileged access is consistently curtailed and strict access controls are maintained. For instance, if the platform's threat intelligence detects a compromised password for a privileged account, the system can automatically enforce MFA to immediately secure the account. Additionally, when privileged users access sensitive assets like domain controllers or servers via Remote Desktop Protocol (RDP), a next-gen identity security platform can dynamically apply enhanced security measures, such as adaptive access controls or session monitoring, to mitigate risks before they escalate.

Thwarting Lateral Movement

Adversaries have honed their skills in moving effortlessly across an organization's systems and environments, leveraging tactics — like escalating privileges — that work seamlessly across operating systems. This growing expertise in lateral movement poses a significant threat, especially as attackers increasingly pivot from on-premises to cloud environments — a trend highlighted by the sizable 136% increase in cloud environment intrusions observed in the first half of 2025 compared to all of 2024.[12] Adversaries can expertly shift from on-premises AD to Entra ID in the cloud, demonstrating their advanced maneuvering tactics. The ability to navigate multiple platforms and pivot actions to meet their objectives underscores the urgency for fast, proactive, and intelligence-driven protection measures.

If an attacker infiltrates your environment, a unified identity security strategy becomes crucial in halting their movements by restricting access to your resources. Adopting a platform that integrates your security controls lets you tap into powerful tools and telemetry to spot signs of lateral movement and enforce identity-driven protection measures.

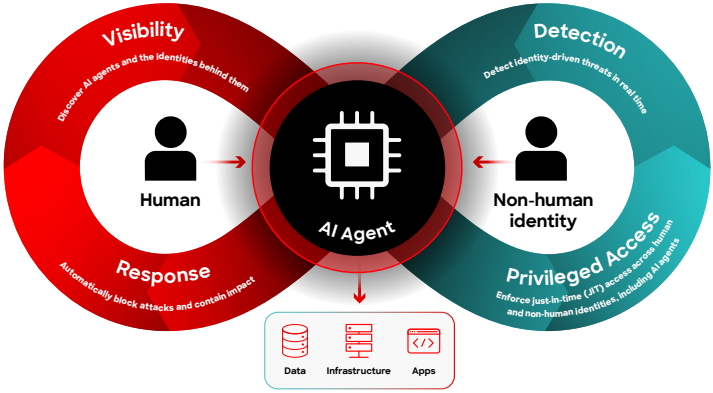
For example, a next-gen identity security platform can detect unusual user behavior like logins from unexpected locations and seamlessly activate policies that initiate additional authentication requests. Similarly, the platform allows you to enforce extra authentication steps for stale or inactive accounts, preventing unauthorized access to your organization's systems and data through potentially compromised, forgotten, or stale accounts.

By integrating these advanced capabilities, a unified identity security solution proactively thwarts lateral movement and keeps attackers from freely navigating your digital landscape.

Quick Tip: Lateral Movement

After gaining initial access, attackers move across an organization's environment to compromise additional systems and steal valuable information. The term comes from the way hackers move sideways from device to cloud resources and other systems.

[12] CrowdStrike 2025 Threat Hunting Report



Securing AI Agents and the Identities Behind Them

The explosion of AI agent adoption is reshaping enterprise operations. From automating workflows to generating code and accessing business systems, these agents are being rapidly deployed — often by individual employees or teams acting outside of IT or security oversight. But each AI agent in your environment creates a new NHI that often inherits broad privileges and interacts with sensitive data, applications, and code repositories.

The rapid pace of adoption has outstripped governance. Most organizations have no idea how many AI agents are running in their environment, what they're doing, what they can access, or who directed them to act. That lack of visibility creates real risk. Notably, 79% of surveyed security leaders believe AI agents will introduce new security challenges into their organization's environment.[13]

A next-gen identity security platform brings this unmanaged attack surface under control. By discovering AI agents across SaaS applications, mapping their access to sensitive systems and data, and linking them to the human or non-human identities behind them, the platform gives your security team the insight needed to assess risk and take action.

For example, the platform can identify AI agents that were created with excessive permissions or that integrate with version control systems and critical business apps. If an agent starts behaving suspiciously like attempting to exfiltrate data or modify code, the system can trigger automated containment, such as revoking access, applying just-in-time policies, or escalating the incident for further review.

With identity security for AI agents built in, the platform closes a critical gap — it protects the agents themselves and the identities behind them. You gain the control you need to safely scale AI use, without introducing new blind spots or pathways for attackers to exploit.

[13] Salesforce, State of IT: Security

Pen Test Preparation

Penetration testing, or pen testing, is a crucial security practice. A pen test simulates real-world attacks on your systems, empowering you to uncover and address vulnerabilities before adversaries can exploit them. Think of a pen test as a cybersecurity dress rehearsal where you can catch the flaws in your defenses before adversaries do.

This proactive approach prepares you for compliance audits and provides a clear snapshot of your security posture's resilience. With regular pen tests, organizations position themselves to proactively identify and mitigate vulnerabilities, which helps them stay ahead of evolving threats.

A unified identity security solution elevates your readiness for these critical security assessments by strengthening your access controls, identifying potential vulnerabilities, and elevating your overall identity security stance. By aligning access rights with user roles, a modern solution ensures each user has exactly the access they need. Likewise, it addresses the growing threats of supply chain attacks and the exploitation of trusted accounts by applying advanced authentication methods and integrated identity life cycle management practices.

Security Posture Management

Attackers thrive on exploiting hidden vulnerabilities in your identity landscape, slipping through cracks left by fragmented security tools. This is where unified security posture management comes into play — a proactive security approach that empowers you to stop identity-based attacks before they even start.

Identity security posture management (ISPM) involves continuously monitoring and analyzing identities, access rights, and authentication processes across your digital ecosystem. By doing so, you can get real-time insights into your organization's identity risk profile and actionable guidance on how to mitigate those risks.

A unified identity security solution that includes ISPM and SaaS security posture management (SSPM) supports your posture management strategy by bringing all identity data into one view, whether you're managing SSO or MFA or tracking digital identities across cloud service providers. This end-to-end visibility gives you the power to spot risks, reduce vulnerabilities, and respond to threats with robust measures, such as enforcing MFA or biometric verification. If your organization uses AD, a unified solution helps you manage your AD and cloud identity provider, SaaS application security hygiene, and SSPM with real-time alerts on rogue users and credential movements, ensuring nothing slips through the cracks.

With this level of visibility and control, your next-gen identity security platform not only enables you to act on critical insights but ensures impeccable hygiene across your network and cloud-based identity stores.

Chapter 4 Recap

A next-gen identity security solution redefines how you approach security, giving you the edge to outmaneuver attackers before they can make a move. It's not just about locking down access — it's about anticipating identity risks and turning your identity infrastructure into a fortress. By modernizing your identity protection with a holistic approach, you can tackle real-world use cases — whether that's cutting off lateral movement, tightening the reins on privileged accounts, securing AI agents and the identities behind them, or shoring up your defenses before and after a pen test.

Unified identity security puts you in control, offering full visibility into your identity landscape and equipping you with the capabilities to respond instantly to emerging threats. From managing AD hygiene to securing SaaS apps and fortifying cloud identities, this approach helps you stay one step ahead at every turn.

Chapter 5
Transforming Identity Security with CrowdStrike

When it comes to identity security, the stakes have never been higher. Protecting your digital identities is vital. As identity-based attacks escalate, so does the pressure to ensure your defenses can handle whatever comes your way.

Choosing the right security partner is key. In a landscape where new threats surface constantly, you need a partner who's not just keeping pace but at the forefront of driving innovation. That's why forward-thinking organizations choose CrowdStrike for their next-gen identity security.

Unify Your Security Operations on One Platform

With the CrowdStrike Falcon® platform, you can safeguard your business with industry-leading, comprehensive security from the company that understands adversaries better than anyone. You can rest easy knowing experts from the leading security provider are working around the clock for you.

Your team can leverage one unified platform to seamlessly oversee every layer of security — from secure privileged access and ITDR to SaaS security, correlating across endpoint, cloud telemetry, and next-gen security information and event management (SIEM) — all through one agent and one console.

Unlock comprehensive protection against identity-based and cross-domain attacks from a unified platform that delivers faster detections, automated response, and proactive threat hunting.

The Falcon platform empowers your organization to:

- Consolidate tools and streamline security operations with a cloud-native, single-platform architecture
- Experience up to 85% faster threat responses driven by full attack path visibility that enables you to stop breaches in their tracks[14]
- Realize up to 84% improvement in operational efficiency[14]
- Coordinate response across your infrastructure and drive remediation actions through tight integration with the Falcon agent

Up to

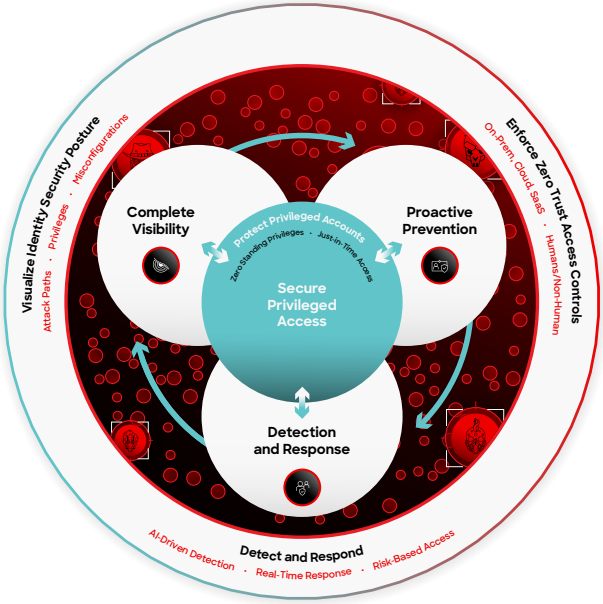
85%

faster responses to threats with full attack path visibility

Up to

84%

improvement in operational efficiency



[14] These numbers reflect the median inputs provided by customers during pre- and post-sale motions that compare the value of CrowdStrike with incumbent solutions and are not guaranteed. They are intended to demonstrate potential value compared to incumbent solutions and do not represent promised outcomes. Actual value realized will depend on individual customer module deployment and environment.

Pioneering Identity Threat Detection and Response

CrowdStrike Falcon® Next-Gen Identity Security, built on the unified CrowdStrike Falcon platform, goes beyond IAM and legacy privileged access management (PAM) tools — which were built for access not security — to secure every identity (human, non-human, and AI agents) across the full identity lifecycle. Purpose-built from the ground up to stop adversaries, it eliminates siloes and avoids the complexity of fragmented tools. CrowdStrike seamlessly combines secure privileged access, real-time identity threat detection and response, and SaaS security in the industry's uniquely unified, AI-native cybersecurity platform to stop identity-based attacks before they start.

This comprehensive approach empowers you to see potential attack paths and visualize risk with unparalleled clarity.

Falcon Next-Gen Identity Security empowers your security team to:

- **Gain full visibility and protection** across hybrid environments — on-premises, cloud, SaaS, and workloads — so adversaries have nowhere to hide and nothing to exploit
- **Close blind spots** across human, non-human, and AI identities — see the identity, understand it, and secure it, before impact
- **Eliminate noise and false positives** with high-fidelity detections so you can focus on real threats and respond with precision
- **Automatically baseline user behavior** with AI-driven detection across your identity estate, detecting and alerting you to abnormal activity in real time
- **Eliminate tool pivots** and manual correlation by using a single, unified platform that saves time and resources to identify active risks
- **Automate responses** at machine speed so your security operations move faster than adversaries
- **Dynamically revoke privileges,** block access, or enforce identity verification mid-session based on real-time risk and contextual signals — before damage is done

Enforce Just-in-Time Privileged Access

Falcon Next-Gen Identity Security introduces a modern approach to privileged access control — delivering real-time, risk-based enforcement of privileged actions without the complexity of traditional PAM solutions. Built natively into the Falcon platform, it enables just-in-time access to both on-premises and cloud-based privileged roles, reducing standing privilege and helping you shut down the paths adversaries use to escalate access.

This approach ensures the right person gets access to the right resource for the right reason — and only for the right amount of time. As soon as risk signals change, access can be revoked in real time to stop escalation attempts and contain potential damage.

Falcon Next-Gen Identity Security removes the need for credential vaults, reduces deployment friction, and delivers immediate time-to-value by securing privileged access directly within the identity attack path.

Leading Capabilities that Modernize Your Identity Threat Security

With Falcon Next-Gen Identity Security, you can detect and stop identity-driven breaches in real time across your entire hybrid identity landscape. By consolidating identity threat protection into a single, powerful platform, CrowdStrike empowers you to strategically reduce identity risk, eliminate gaps, and take control of your entire identity attack surface.

This approach not only streamlines your security operations but also strengthens your overall defense strategy, enabling proactive protection across your entire ecosystem. No more juggling separate tools that add complexity — just one trusted partner with an ever-growing partner ecosystem to safeguard your organization.

Falcon Next-Gen Identity Security empowers you to proactively reduce your identity attack surface with:

- **Unified identity visibility:** Falcon Next-Gen Identity Security unifies visibility across on-premises AD, cloud-based identity providers like Entra ID and Okta, and SaaS applications. This single, holistic view eliminates silos, empowering you to manage and protect identities across your entire environment with confidence.
- **Automated identity classification:** Automatically classify all identities — whether human or service accounts — so you can quickly assess your landscape and ensure that the right protections are in place for all of your identity types.
- **Enhanced identity hygiene:** Gain deep insights into the health of your identity stores, uncovering potential misconfigurations, stale accounts, and potentially compromised credentials that can leave you vulnerable to attack. By maintaining robust identity hygiene, you reduce your attack surface and enhance overall security.
- **Comprehensive attack path identification:** Identify potential attack paths, enabling you to close off vulnerabilities before adversaries can exploit them.
- **Dark web credential insights:** Leverage real-time insights into compromised credentials circulating on the dark web, allowing you to take swift action — including automatically enforcing MFA or disabling or locking an account — to prevent unauthorized access and reduce your risk of a breach.
- **Attack path-aware policies:** Create and enforce security policies that correlate directly with identified attack paths and known adversary tactics, techniques, and procedures (TTPs). This ensures your defenses are aligned with the latest threat intelligence.
- **Cloud and AD vulnerability mitigation:** Address inherent vulnerabilities in your cloud and AD identity stores by applying focused security measures that are tailored to your environments.

You can detect identity-based attacks in real time with:

- **Real-time detection of anomalous behavior:** Baseline normal user behavior and detect anomalies at both the authentication and endpoint layers. For instance, if a user logs in from the U.S. and minutes later attempts to log in from France — an "impossible travel" scenario — Falcon Next-Gen Identity Security will immediately detect this suspicious activity and initiate escalated identity protection measures.

- **Comprehensive detection of complex identity attacks:** Detect sophisticated, identity-based attacks across your entire environment. This includes recognizing lateral movement across identities and endpoints as well as more advanced hybrid lateral movement from on-premises AD to cloud-based identity providers like Entra ID. By catching these complex attack patterns in real time, you can neutralize threats before they cause damage.

- **Proactive identity threat hunting:** CrowdStrike® Falcon Adversary OverWatch™ delivers 24/7 cross-domain threat hunting and credential monitoring to help you defend against identity-based threats. By leveraging unified visibility across identity, cloud, and endpoint, expert CrowdStrike hunters detect early signs of compromised credentials and track lateral movement between cloud and endpoint. Falcon Adversary OverWatch also monitors criminal forums on the dark web for stolen credentials and forces MFA challenges or password resets through Falcon Next-Gen Identity Security to prevent unauthorized access.

You can stop breaches with:

- **Real-time threat protection for on-premises, cloud, and SaaS identities:** Leverage Falcon risk scores, device trust data, and threat intelligence to enable risk-based access decisions, providing inline threat prevention within authentication flows.

- **Risk-based conditional access:** Use modern, phishing-resistant MFA to enhance security and automatically remediate anomalous activity while still supporting business productivity. By dynamically applying MFA based on risk factors, you can ensure that only authorized users gain access to sensitive resources, reducing the burden on your SOC team.

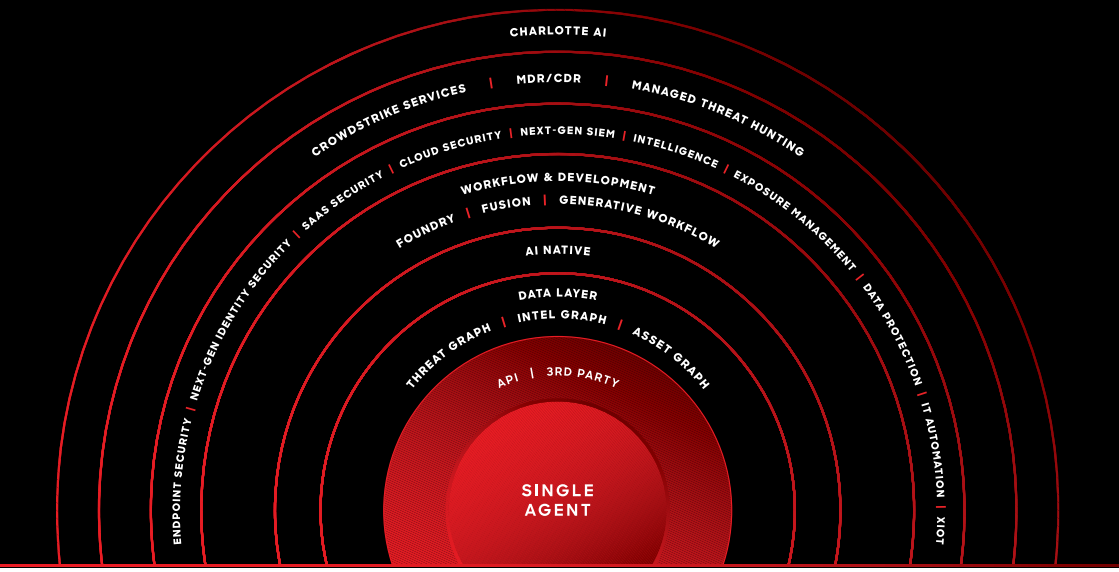
- **MFA support for your legacy systems:** Extend MFA to areas that are difficult to protect with conventional methods, including your legacy systems that often lack built-in identity security controls.

- **Broad identity authentication support:** Enjoy the freedom to choose and extend MFA across all major IAM providers. This includes support for FIDO and phishing-resistant authentication options like YubiKey and HYPR, ensuring flexibility and enhanced security across your entire authentication landscape.
- **Policy-based responses:** Equip your SOC team with the tools it needs to focus on the most critical detections and automatically remediate identity threats in real time.
- **Threat Intelligence:** CrowdStrike Falcon® Adversary Intelligence helps protect against identity-based attacks by continuously analyzing and identifying adversaries' tactics and targeting patterns to detect threats before they escalate. Integrating threat intelligence with identity protection enables real-time blocking of suspicious access attempts, reducing the risk of unauthorized access.

Augment Your Team with Managed ITDR

Many organizations facing resource constraints are turning to managed service providers to handle security operations. If you're looking for the best of both worlds — top-tier ITDR capabilities paired with expert management — CrowdStrike has you covered.

CrowdStrike Falcon® Complete Next-Gen MDR provides unmatched security for your identities and identity stores. Combined with Falcon Next-Gen Identity Security, the Falcon Complete team actively monitors Falcon solutions for you, investigating and surgically remediating incidents in minutes. By leveraging managed identity threat protection, your organization can implement a robust and mature identity security program without the heavy lifting, costs, and time required to develop one internally.



The Falcon Complete Next-Gen MDR team is composed of seasoned security professionals who are:

- **Experts in the Falcon platform:** The team ensures your identity environment is continuously optimized to combat the latest threats and achieve the best levels of performance and protection.
- **Experts in incident response:** The team comes to you with multiple years of experience in digital forensics and incident response (DFIR).
- **Experts in threat hunting:** CrowdStrike's 24/7 human threat hunting uncovers the faintest trace of malicious activity in near real time.
- **Experts in threat intelligence:** CrowdStrike's global threat intelligence team brings critical context to the response process.

Ready to modernize your identity security? Request a free Identity Security Risk Review

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: https://www.crowdstrike.com/

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

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