




The Case For Unified Endpoint and Identity Security

Securing identities in a world of
widespread credential compromise

eBook

Table of Contents

Executive Summary	3
Why Are Cybersecurity Professionals Thinking About How to Catch Imposters?	4
Part 1: The Challenge of Detecting Compromised Identities	6
Part 2: How To Unify Endpoint and Identity Security	8
Part 3: The Benefits of a Unified Endpoint and Identity Solution	10
Benefit 1: Move Left in The Kill Chain	10
Benefit 2: Weave Disparate Signals Into a Coherent Story	12
Benefit 3: Respond Faster	14
Improve Detection Without Adding Complexity by Unifying Identity and Endpoint Security	16



Executive Summary

The security of identities has become a critical concern for organizations, with 15 billion leaked credentials circulating online¹ and a 71% surge in the use of stolen credentials to access valid accounts in 2023². It's clear that attackers are increasingly exploiting compromised but legitimate credentials as their preferred method of entry.

This eBook explores the pressing need for unified endpoint and identity security to respond to this challenge. Our eBook is divided into three main parts:

1. **The Challenge of Detecting Compromised Identities**

This part explores the factors driving the increasing importance of identity as an attack vector, including the blurred boundaries of modern environments and the trend towards living-off-the-land techniques to avoid traditional detection mechanisms.

2. **How To Unify Endpoint and Identity Security**

In this part we present our three-pillar approach with a single agent for in-depth monitoring, a common data model, and a single console for coherent storytelling.

3. **The Benefits of a Unified Approach**

We demonstrate how unifying endpoint and identity security helps organizations move left in the kill chain, weave disparate signals into a coherent story, and respond faster to threats. This section also includes detailed example scenarios illustrating each benefit by comparing the effectiveness of siloed response with a unified response.

By adopting a unified security approach, organizations can significantly improve their ability to detect and respond to identity-based threats. This eBook provides actionable insights and practical strategies to help security professionals stay ahead of attackers and protect their organizations more effectively.

¹[Annual Cyber Threat Trends Report, Deloitte, 2024](#)

²[X-Force Threat Intelligence Index 2024, Security Intelligence, 2024](#)

Why Are Cybersecurity Professionals Thinking About How to Catch Imposters?

Identity has always been an attack vector, but its prevalence as a target for successful attacks has surged in recent years. Today, **abusing valid credentials** is the preferred method of access into victim environments – representing the [top infection vector in 2023](#).²

15 billion

leaked credentials
circulating online¹

71%

increase in use of stolen
credentials to access valid
accounts in 2023²

190%

more effort required
to remediate breaches
involving compromised
credentials than average³

To understand why attackers increasingly see targeting identity as the path of least resistance, let's start with a simple thought experiment.

Which individual is most likely to evade detection?

- The thief who breaks in with a lockpick?
- The thief who walks in the front door dressed in their best suit with a valid ID card?

If you answered the latter, perhaps it was because an individual who appears to belong and can blend in with the crowd is much more difficult to detect.



Attackers Don't Break In, They Log In

The parallel with cybersecurity is that organizations have become increasingly effective at detecting digital crowbars and lockpicks. For this reason, the threat landscape seems to be trending towards **living-off-the-land techniques, using OS-native commands and legitimate credentials** to avoid traditional detection tools. Other factors have exacerbated this challenge, such as the widespread availability of stolen credentials on the dark web and the blurring boundaries of the network driven by **hybrid cloud environments, remote work, and bring-your-own-device policies (BYOD)**.

¹Annual Cyber Threat Trends Report, Deloitte, 2024

²X-Force Threat Intelligence Index 2024, Security Intelligence, 2024

³Identity-based cyberattacks on the rise, SDX Central, 2024

Unifying Endpoint and Identity Security for Greater Visibility

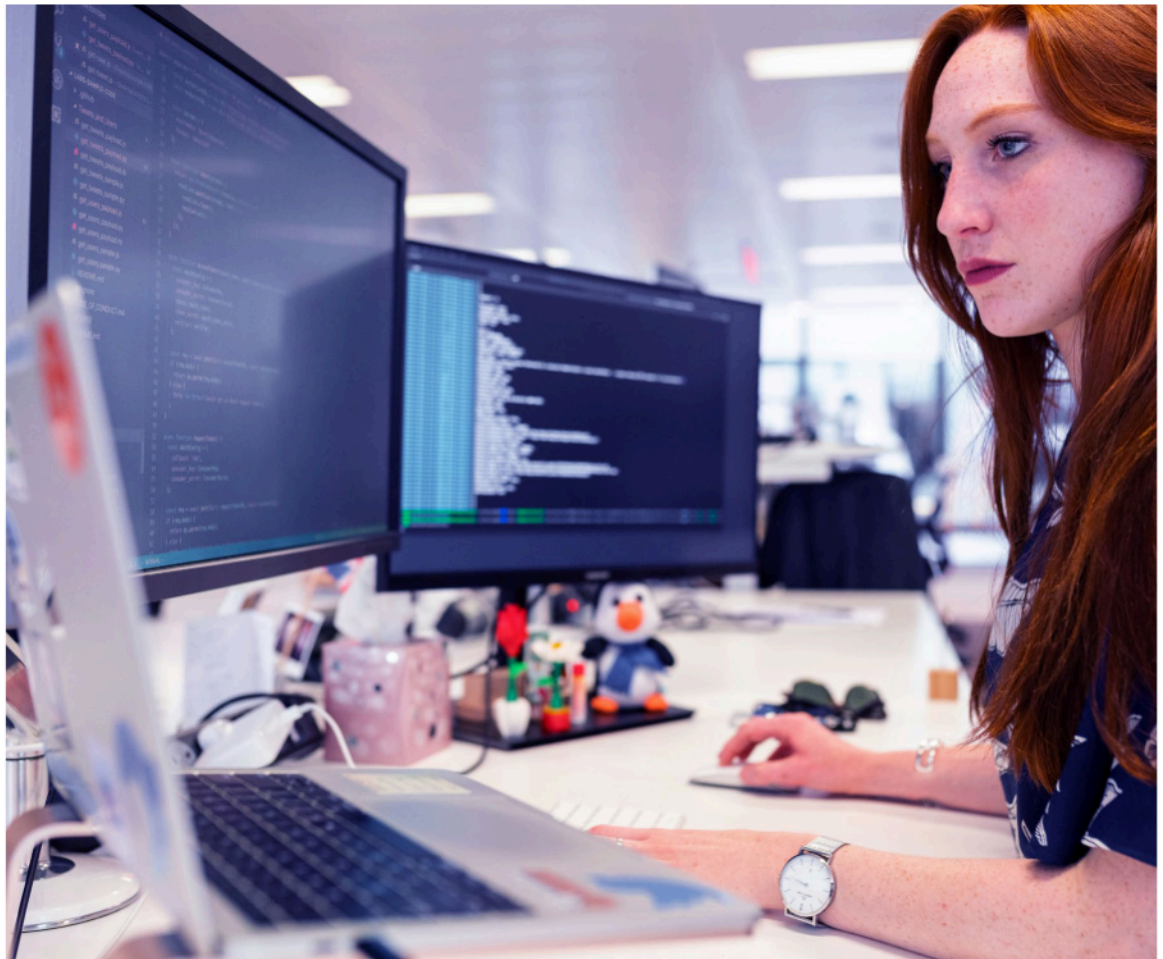
In this eBook, we offer the perspective that unifying endpoint and identity security is the path to illuminating some of these blindspots and catching imposters. Correlating events across endpoint and identity increases the probability of rapid detection by creating a complete picture of the threat with all the relevant context, creating a timeline and a story that an analyst can understand at a glance.

This view reflects an emerging consensus in the cybersecurity community; however, many organizations hesitate due to the dilemma of **how to achieve this goal at an acceptable cost** – both in dollar terms and in terms of friction imposed on users. We believe recent technology advancements make unified endpoint and identity possible for organizations of all sizes.

In the first part of our eBook, we will elaborate further on the challenges associated with identity detection today. In the second part, we will present the three pillars of our proposed approach:

1. **Common data** model to bring together every piece of context
2. **Single console** to tell a coherent story for analysts
3. **Single agent** for in-depth monitoring at the point of breach

In the third part of the eBook, we'll explore the benefits of this unified approach: allowing organizations to move left in the kill chain, weave disparate signals into a coherent story, and overall respond faster.



Part 1: The Challenge of Detecting Compromised Identities

Complex Environments Provide Adversaries with Ample Camouflage

In the introduction, we discussed the rising importance of identity as an attack vector, and the increasing tendency of attackers to impersonate legitimate users. There are several factors at play that make these tactics difficult for organizations to counter:



The blurring boundaries of the environment, with the rise of hybrid cloud environments, remote work and bring-your-own-device policies (BYOD). Users may use multiple devices and have multiple identities across different applications. Traditional detection tools may lack visibility into application-based identities.



Ephemeral endpoints such as virtual desktops or desktop-as-a-service. While these endpoints may be spun up and down in the cloud, the identities persist, increasing the difficulty of correlating endpoint and identity events.



Non-traditional identities, as organizations utilize machine accounts alongside human accounts. These accounts may be highly privileged while not lending themselves to defenses like Multi-Factor-Authentication MFA.



Vulnerable identity attack surface, with many interconnected parts and opportunities for misconfigurations and over-permissioning. The domain controller and identity provider play a key role, handling authentication and authorization requests, yet often there are inherent vulnerabilities, with identity infrastructure giving up valuable information in response to queries.



Identity hygiene gaps, with many organizations still lacking full visibility into permissions and struggling to keep privileges up to date and aligned to the principle of least privilege (PoLP).



The speed of lateral movement, with harvested credentials used to move rapidly across multiple devices and identities, confounding efforts to correlate different events.

These factors are some among many that have created blindspots around identity. The result is that a compromised identity is very difficult to distinguish from an ordinary user, with subtle threats going undetected.

These challenges will not be solved by the addition of a new widget. They require a fundamental shift in our approach to endpoint and identity security.

This is More Than an Authentication Problem

Many organizations have sought to counter these threats by adopting a more robust authentication solution. This could include adopting universal **multi-factor-authentication (MFA)**, implementing **zero-trust conditional access policies**, or even pursuing “**passwordless solutions**”, which avoid reliance on traditional passwords in favor of possession factors like registered devices or biometrics.

These are all steps that we welcome and recommend; however, alone they are insufficient. Identity Access Management (IAM) tools are designed to safeguard access and authenticate users but they are not a substitute for Identity Threat Detection and Response (ITDR), which protects identities by detecting threats and helping SecOps teams respond to incidents. Authentication systems can be bypassed if the attacker is able to **harvest stored credentials** and **abuse (or forge) stored authentication tokens**. Many applications have cached credentials or tokens and it is difficult for security teams to gain visibility into these vulnerabilities.

These Challenges Can't be Tackled with Siloed Solutions

All problems in the detection space must be considered against the backdrop of the profound and ongoing **cybersecurity talent shortage**. The constant and overwhelming flow of alerts makes it very challenging for analysts to distinguish urgent threats from less urgent risks or **false positives**. When you have too many alerts, and not enough people, you're forced to make prioritization decisions, and it's difficult to do so effectively without full context.

The second point to consider is how much time it takes for analysts to investigate, once the security team tackles an alert. Siloed identity and endpoint solutions contribute to a broader problem of **tool overload**, where constantly switching between tools costs analysts valuable time. Manually synthesizing information from different sources is time-consuming and can lead to missed connections. The time lost quickly adds up - the seconds lost pressing “ctrl + c” and “ctrl + v” can add up to hours as the task is repeated many times.

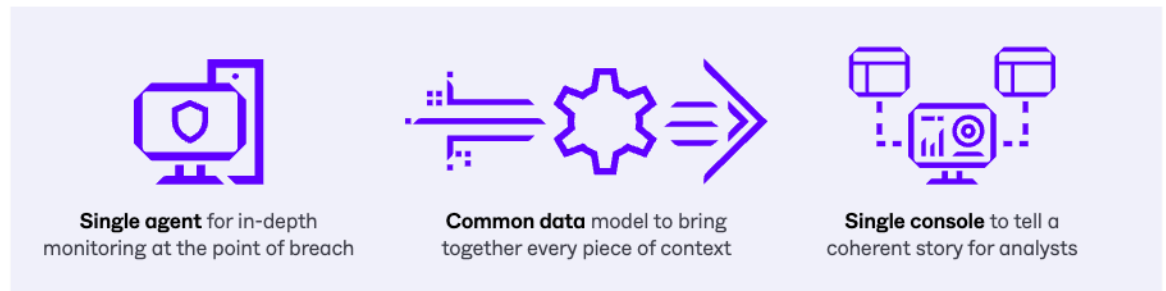
We should also consider the **human side of siloes**. Today, endpoints and identities are not only protected by separate tools, they may be also be protected by separate teams. This adds an additional layer of coordination, communication, and administration, which takes precious time and creates extra friction – with team members spending time taking notes, summarizing for their colleagues, and completing reporting tasks.

The Takeaway

As we've established, identity threats are subtle. Attackers are doing everything they can to blend in with legitimate users. SecOps teams need the full picture, with all possible context, to correlate the signs and detect these threats early.

Part 2: How To Unify Endpoint and Identity Security

Our approach to unifying endpoint and identity has three key pillars. In this section, we'll explore all three in detail. In part 3 we'll lay out the benefits of this approach and bring them to life through example scenarios.



Single Agent for In-Depth Monitoring at the Point of Breach

Don't give adversaries an uncontested playground on the endpoint

Many organizations are responding to the increase in identity threats and stolen credentials by seeking to **harden the domain controller**. This makes sense as a starting point, but alone, it is insufficient and leaves substantial risks unaddressed. Although this approach gives organizations greater protection against reconnaissance via the domain controller, it does not give any visibility into the signs of compromised identity on the device itself. This gives an attacker an opportunity to conduct malicious activities somewhat uncontested on the endpoint, such as **harvesting stored credentials**, mapping the network, searching for vulnerabilities, and establishing persistence.

So, what is the alternative?

Historically, monitoring identities on the endpoint has been challenging

Most organizations are eager to gain more granular, real-time identity data, but have hesitated to install an ITDR agent on every endpoint. An additional agent imposes a heavy cost, including the dollar cost of the tool, the performance impact on the device, and the time cost of installing, updating, and managing the software. However, there's no longer the need to install a new agent just for identity. Today, single-agent solutions enable organizations to unify endpoint and identity protection, which provides the additional visibility and protection of an ITDR agent, without the added friction and cost.

Single agent for unified management

Collecting endpoint and identity telemetry from a single source enables an **unmatched level of correlation** between the two. This unlocks greater context for detection and triage, since multiple connected events may indicate greater risk than any single event would individually. A single agent enables organizations to **confront attackers at the point of breach** – and respond to the intrusion before they have an opportunity to inflict further harm through reconnaissance or lateral movement. This **reduces the blast radius** of attacks and enables faster remediation. A single agent is also simpler from a management perspective, with a single installation to cover all hardware types and use cases across EDR and ITDR, and a single mechanism to define and apply policies. Overall, a single agent leads to faster, more accurate detections and **lower total cost of ownership (TCO)**.

Common Data Model to Bring Together Every Piece of Context

Wrapping identity telemetry into the broader security solution

Attackers will do their best to blend in with ordinary users and mask their activities. When tools are siloed, the signs of compromise may not individually be sufficient to warrant a response, whereas when seen collectively and in context, they may be deemed more urgent. This means **it is crucial that identity telemetry be correlated with other signals**. A common data model facilitates easier correlation and analysis of data from different sources, reducing the complexity of data integration and management, while unlocking a more complete, contextualized picture to support detection.

Completeness versus openness

When it comes to bringing endpoint and identity together, many vendors will seek to highlight the breadth of their portfolio, essentially saying “choose us because we cover all the bases.” This doesn’t necessarily deliver a good outcome for customers. Firstly, many vendors offer an endpoint and identity solution but this does not mean that they are **well integrated**. Secondly, most customers want to avoid **vendor lock-in**, and they certainly don’t want to limit their options just for the sake of having a complete solution. We would argue that for this reason, **openness is more important than completeness**, and advise customers to consider solutions built on an open platform with open standards for data export and ingestion. This gives customers a path to integrate their tools without forcing them to lock in with a single vendor.

Example

The **Open Cybersecurity Schema Framework (OCSF)** is a vendor-agnostic schema that aims to standardize and streamline the way cybersecurity data is structured and shared across different security tools and platforms.

Single Console to Tell a Coherent Story for Analysts

The challenge of forming a complete picture across endpoint and identity

Phrases like “single-pane-of-glass” have become something of a painful cliché in cybersecurity. It’s a promise that has never been fully realized. In the prior section, we talked about the importance of a common data model; however, aggregating a large quantity of data from different sources isn’t enough to efficiently evaluate or investigate an alert. **The mark of a true single console approach is coherence**. Analysts are looking for solutions that automatically correlate linked signals and events to tell them a story they can understand at a glance. In the context of endpoint and identity, this could mean linking all the actions taken by a particular identity across different devices or applications. Instead of looking at individual endpoint events, the analyst can also see **adjacent identity events**, with breadcrumbs to thread them together. Visibility into identity is particularly crucial in the context of **lateral movement**, where we might see an attacker using credential harvesting or privilege escalation to move towards a desired target. To fully eradicate the threat, security teams need to understand where and how additional identities were compromised.

A single console also delivers a host of more holistic benefits. It supports alert triage, enabling automated assessment of risk, so that teams can apply a **meaningful system of prioritization** as they tackle alerts – rather than relying on heuristics. Furthermore, it offers a **unified interface for investigation**, providing a shared view should multiple roles need to coordinate.

Part 3: The Benefits of a Unified Endpoint and Identity Solution

Benefit 1: Move Left in The Kill Chain

Detect and remediate threats at the point of breach, reducing the blast radius of threats and accelerating response.

Challenge

As we discussed in section 1, many organizations lack visibility into compromised identities and credential harvesting on the endpoint. Organizations try to make up for this blindspot by layering protection to guard against lateral movement rather than **detecting identity compromise at the point of breach**. This gives the adversary greater freedom to conduct malicious activities on the first device they land on, resulting in breaches that are harder to detect, are more time consuming to eradicate, and have a larger blast radius.

Solution

Deeper Visibility Into Compromised Identities

Today, it's possible for organizations to **combine ITDR and EDR on a single agent**, delivering identity telemetry without the friction of installing and maintaining an additional agent. This single agent collects granular, real-time identity telemetry, which provides **additional visibility** required to detect compromised identities at the point of breach.

Deeper identity telemetry and insights could include:

- **Authentication patterns**, with log data capturing authentication events, including source IP, user account, and authentication method
- **Elevation of user privileges**, especially if it bypasses normal access controls such as changes in group memberships, role assignments, or permissions
- **Access to sensitive resources**, such as accessing critical files or databases, especially during non-business hours
- **Suspicious PowerShell commands or scripts**, such as modifying registry keys or accessing LSASS memory

These deeper insights support more effective detection and provide additional context for conditional access policies, which can automatically force reauthentication or suspend credentials in response to suspicious patterns. Furthermore, because all this telemetry is connected using the same mechanism as endpoint signals, events are automatically correlated to create a more complete picture for detection and investigation. An ITDR agent on the endpoint can also help prevent lateral movement using domain controller intercept. This capability enables the security team to detect suspicious queries sent to the domain controller from the endpoint and intercept the response, replacing it with deception (e.g. presenting fake domain admin credentials which trigger an alert if used).

Greater Solution-Native Deception Capabilities

Unifying endpoint and identity security with a single-agent approach creates opportunities for solution-native deception capabilities on the endpoint. Whereas traditional deception has proved too expensive and labor-intensive for many organizations, **solution-native deception is built into the agent itself and doesn't add cost or friction.**

Deception not only diverts the attacker away from privileged credentials and critical assets, it also adds additional tripwires at the point of breach to support faster detection. These tripwires provide **high-fidelity true positives.** For example:

- **Honey tokens** are fake credentials stored on the endpoint which are indistinguishable from real cached credentials. If someone attempts to log in using these credentials, the login will fail and an alert will be sent immediately to the SOC.
- **Canary files** are fake files installed on the OS which no legitimate user would touch. If they are manipulated, the agent will detect this and alert the SOC.
- **Shadow copy deception** comes into play if an adversary attempts to delete shadow copies. An agent can recognize these attempts and give a deceptive response to make the attacker think they have succeeded while raising an alert.

Example Scenario

A ransomware group uses social **engineering** to trick an employee into visiting a malicious website. The compromised website exploits a browser vulnerability that allows the adversary to **steal stored credentials** and gain initial access. The attacker uses PowerShell and Windows Management Instrumentation (WMI) to **establish persistence** on the endpoint. Once on the machine, the attacker uses **OS-native tools** like "cmdkey" and memory dump through Task Manager to extract stored credentials. The attacker's goal is to identify and compromise privileged users. The attacker attempts to use Remote Desktop Protocol to **map the network** and gain access to other machines. After this, the adversary turns their attention to the domain controller, attempting to **gain access to privileged accounts.**

Responding with siloed identity and endpoint

In a siloed configuration, the attacker's actions have not generated sufficiently compelling alerts to drive a rapid response from the SecOps team. The team eventually detects the attack once the attacker targets the domain controller, and the team is successful at blocking further lateral movement. That said, the attacker has already succeeded in **compromising multiple devices, harvesting credentials, and performing extensive reconnaissance.** Furthermore, because the signal associated with the detection is not correlated with other events in the kill chain, it will be **time-consuming for the team to fully remediate the attack,** as they painstakingly reverse engineer each step the attacker executed.

Responding with unified identity and endpoint

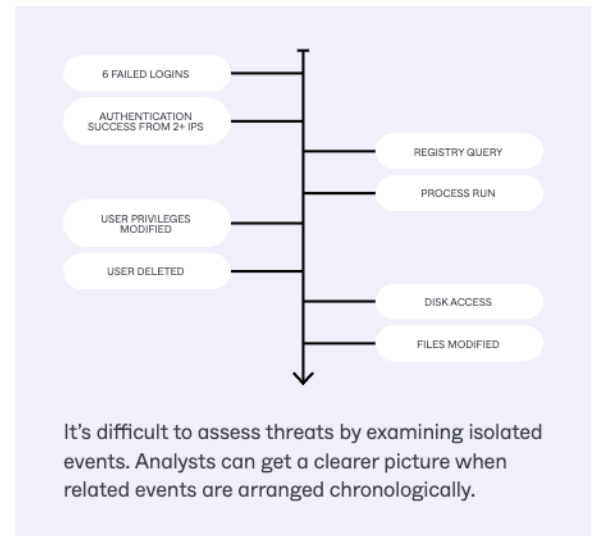
As soon as the attacker logs in using the stolen credentials, suspicious signals are registered, and the identity and endpoint telemetry are **automatically correlated.** As the attacker attempts to steal cached credentials, real credentials and production systems are hidden and replaced with **deceptive credentials and decoy systems.** When the attacker attempts to use the decoy credentials, this raises an urgent alert, and triggers immediate auto-remediation measures. The SOC team reviews the alert alongside all the related events and context, which enables them to **quickly eradicate the threat.**

Benefit 2: Weave Disparate Signals Into a Coherent Story

Correlate linked events across identity and endpoint to support detection of credential compromise.

Challenge

The increasing abuse of legitimate credentials and the trend towards living-off-the-land techniques reflect an effort on the part of adversaries to **avoid traditional detection mechanisms**. Detecting these subtle threats requires effective correlation of signals, since **subtle indicators may individually appear innocuous but collectively merit an urgent response**. Triage is a critical step in this context to assess which alerts to prioritize. However, both triage and investigation are made more complicated when relevant alerts reside in siloed tools for endpoint and identity, requiring analysts to do considerable manual work to assemble a full picture.



Solution

Unifying endpoint and identity security equips analysts with full context on a given alert, enabling **automated triage and more** rapid investigation. As we discussed in the prior chapter, a single agent unlocks deeper identity telemetry and automatically correlates endpoint and identity events. The use of a **common data model** enables a more seamless fusion of data from different sources – including tools from multiple vendors. Finally, **a single console presents this information through a unified interface which analysts can use to investigate and respond**.

Correlating signals into a coherent story

Organizations can use behavioral AI tools to correlate different signals into **contextualized, linked representations of connected activity on a system**. Chronology and relationships are established, such as parent-child processes or the use of a particular account to run a command on a particular machine. This linking is particularly critical, since attacks can span many identities and devices through **lateral movement**. Threats are assessed as a linked series of events, not just a single process or file. Behavioral AI detection logics compare these series with **attack patterns** such as ransomware, credential harvesting, privilege escalation, and more.

User and Entity Behavior Analytics (UEBA) is a key component of this process, collecting data on normal user behavior as a point of comparison to detect anomalies – such as a user suddenly downloading significantly larger files. This also extends to machines - for example, a server receiving an unusually high number of requests. A unified solution is critical here, as it analyzes **multi-dimensional data to support higher-fidelity anomaly detection**.

Vulnerability and exposure management

Unifying identity and endpoint security gives a more complete picture for vulnerability and exposure management. Organizations can pursue deep discovery and vulnerability assessment from the footprint of a single agent – including assessing vulnerabilities of the identity infrastructure, such as the domain controller. **Credential protection** can also be implemented through the agent, whereby applications prevent saved credentials from being accessed by other applications running on the same machine. Furthermore, using a single console provides a **unified workflow** to configure identity and endpoint policies with no disconnected experience. It also allows for the integration of new sources of intelligence, such as **dark web scanning for compromised credentials**, and taking auto-remediation actions for vulnerable accounts, like requiring a password reset, requiring reauthentication, or disabling the affected account.

Example Scenario

An attacker compromises an employee's personal Google Chrome account and **steals a copy of all saved credentials**. After reviewing the stolen credentials, the attacker discovers a work-related credential that is used to access a corporate email account. The attacker publishes the credential **for sale on the dark web**. Days later, the credential is purchased by a skilled threat actor that is highly focused on initial access. Using a combination of social engineering and MFA fatigue, the malicious threat actor gains access to the corporate network over a VPN and **enrolls a new, personal device that is unprotected**. Once connected to the company's internal network, the attacker begins performing **reconnaissance**, mapping the network and querying Active Directory for exposures and misconfigurations. The attacker discovers, and succeeds in exploiting, an improperly configured Access Control List (ACL) to **escalate permissions** and gain access to a privileged account. The attacker uses the now compromised, privileged account to create additional privileged accounts for later use if needed. Using a new privileged account, the attacker adds the unprotected endpoint to the domain, installs malicious software to **establish persistence**, and **discovers critical assets and sensitive data**. After stealing copies of the sensitive data, the attacker attempts to encrypt the original content. The encryption attempt is blocked and an alert is sent to the SOC.

Responding with siloed identity and endpoint

This example includes **several suspicious indicators**, such as the repeated failed MFA authentications, the addition of new MFA authentication devices, the traffic between the unprotected device and the corporate resources, and finally the modifications made to access privileged accounts and create new privileged accounts. **Individually, some of these signals might have been deemed suspicious, but none was suspicious enough to raise the alarm and drive an immediate review**. By the time the SecOps team starts fighting back, the attacker has already compromised multiple accounts and devices, installed tools for persistence, and stolen sensitive data. The SecOps team is now in a **race against time** to eradicate the threat before valuable data is encrypted and critical assets are rendered useless.

Responding with unified identity and endpoint

A **unified platform** that performs continuous **dark web scanning for exposed corporate credentials** would have automatically reset the user's passwords within the MFA platform and the Active Directory environment. An alert would have been raised to the SOC before the attacker attempted to gain access to the corporate network. And, best of all, the attacker would have wasted money purchasing an invalid credential on the dark web. If the credential had not been published to the dark web, and the attack played out as described, **all signals associated with the attack would be correlated into a single event**, including the suspicious authentication attempts, the network traffic generated by reconnaissance and lateral movement, and the commands executed throughout the attack. **This allows the SecOps team to detect and respond to the threat much earlier within the attack sequence**. Additionally, the correlated identity and endpoint data rolled up into a single event decreases the precious amount of time it takes to determine what, when, and where the attack occurred, as well as its impact.

Benefit 3: Respond Faster

Gain greater visibility into attack patterns and responder with more automatic and rapid remediation actions.

Challenge

Once an adversary has breached and organizations defenses, they take steps to **establish persistence** and **move laterally** that create a complex trail for SecOps teams to unravel. Furthermore, today relevant information and **response actions are siloed across different tools** for endpoint and identity. This makes it difficult for organizations to rapidly eradicate threats.

Solution

As we've discussed in the prior two sections, a unified identity and endpoint solution supports faster detection by providing more complete context and correlating events across endpoint and identity. It also places identity detection capabilities closer to the point of breach. Faster detection contributes to a faster overall response, but **a unified solution also has an impact on remediation.**

A unified solution supports effective remediation by providing a **single interface from which to effect a coordinated response.** This streamlines the incident response workflow and **reduces context switching** between tools. The use of a single agent also supports **improved automation**, as on-agent remediation reduces the need to build automations that string together multiple tools. Automated response playbooks can include actions based on ITDR alerts – for example suspicious logins on a device can trigger automatic endpoint isolation. The same principle can apply in reverse. For example, if suspicious executable activity is detected on a device, not only can the device be isolated, automated actions can be taken to remediate the compromised identity, such as reset passwords, log out active sessions, and notify the affected user.

A unified solution also provides **holistic visibility to help security teams understand the full scope of an incident** and map the attack path, identifying all affected devices and accounts. A single agent is helpful here, since both identity and endpoint telemetry is captured by a single source, enabling **easier correlation of events.** Furthermore, the agent can be used to map vulnerabilities such as stored credentials which can help the team identify where lateral movement has taken place.

Unlock on-agent auto-remediation capabilities

Some organizations are investing in rollback remediation, which allows them to turn back the clock and restore compromised machines to the last known good state. This is made possible by automatically capturing VSS snapshots at regular intervals and protecting them from alteration or compromise. An agent delivers this capability, and rollback can be triggered automatically in response to threats.

Generative AI

A unified solution also provides the data foundation necessary for the adoption of generative AI capabilities. One of Generative AI's powers is its ability to **search and summarize across datasets**, but this is only possible if the data is normalized and accessible. Unifying endpoint and identity provides generative AI tools with visibility across both, and by extension the ability to deliver context and connections across the two.

A few of the **key benefits** include:

- **Automated triage:** Assign an initial risk assessment to a given event to help analysts prioritize and perform contextual enrichment.
- **Natural language investigation:** Translate a natural language prompt into the desired query language and suggest relevant follow-up questions.
- **Event summaries:** Summarize an event in natural language to support coordination across teams and reduce the burden of writing communications.

Example Scenario

A state-sponsored hacking group is engaged in a **prolonged espionage campaign**. They have compromised a number of low-level employee accounts by purchasing credentials on the dark web. They use Windows Registry run keys to **achieve persistence without leaving a file on the disk**, creating a registry entry that executes a PowerShell command each time the system starts. They also target Active Directory, **creating hidden accounts and modifying permissions to achieve domain dominance**. The group reaches a high value target and begins exfiltrating data, using HTTP traffic to blend in with legitimate communication.

Responding with siloed identity and endpoint

Although the SecOps team is able to detect and block the data exfiltration, by this point **the blast radius is large**. Earlier warning signs were detected, such as unusual authentication data from various accounts, unusual domain controller queries, and the creation of new registry keys. However, **because these signals were detected and investigated in siloes, none individually warranted an urgent response** and the team was not able to construct an overall picture of the attack that was in progress. The analysts handling the initial alert **struggle to assess the extent of the damage** and identify the many compromised accounts and devices that have contributed to the attack. This creates ambiguity around the appropriate path of escalation. This also delays the necessary personnel surge in response to the urgent alert. Once additional team members do engage, **valuable time is lost writing communications to summarize the situation and coordinate tasks**. Painstakingly, the team constructs queries and reviews logs attempting to reverse engineer the attack and take remedial action. During this time, the adversary continues to maneuver. The team is forced to blanket isolate a number of devices, **causing disruption to ordinary users**.

Responding with unified identity and endpoint

The team has an early warning when unusual PowerShell commands raise alerts and are correlated with the compromised identity. From there, they **use generative AI to quickly construct a threat hunting query**, utilizing threat intelligence to tailor their query to known tactics associated with the state-sponsored group. They are able to assemble a clear story, **illuminating the path of lateral movement and discover hidden and compromised accounts**. The analysts who discovered the alert pull in additional team members, sharing the event summaries created by generative AI to **quickly bring the team up to speed**. From here, the group works to push a policy to the affected endpoints and suspend compromised accounts from a **single interface**.

Improve Detection Without Adding Complexity by Unifying Identity and Endpoint Security

The increased prevalence of compromised credentials as an attack vector and the growing risks associated with identity demand a fundamental shift in approach. The cybersecurity industry is moving towards unified endpoint and identity, but there are few vendors that can give customers the visibility they need to detect imposters at an acceptable level of cost and minimal friction.

SentinelOne offers a path forward based on three principles:

1. **Single agent** for in-depth monitoring at the point of breach
2. **Common data** model to bring together every piece of context
3. **Single console** to tell a coherent story for analysts

With this approach, organizations can move left in the kill chain, weave disparate signals into a coherent story, and respond faster overall.

Check out our website to learn more about some of our key products for endpoint and identity security:

- [Singularity Platform](#)
- [Singularity Endpoint](#)
- [Singularity Identity](#)

Innovative. Trusted. Recognized.

Gartner

A Leader in the 2024
Magic Quadrant for
Endpoint Protection
Platforms

**MITRE
ENGenuity**

Industry-leading ATT&CK Evaluation
+ 100% Detections. 88% Less Noise
+ 100% Real-time with Zero Delays
+ Outstanding Analytic Coverage, 5 Years in a Row

**Gartner
Peer Insights**

96% of Gartner Peer Insights™
EDR Reviewers Recommend
SentinelOne Singularity





Contact Us

sales@sentinelone.com

+1-855-868-3733

sentinelone.com

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

© SentinelOne 2025