CrowdStrike White Paper

CROWDSTRIKE

FIVE QUESTIONS TO ASK BEFORE CHOOSING SENTINELONE FOR WORKFORCE IDENTITY PROTECTION

Focus on a true platform approach with a unified view of threats across endpoints and identities

Singularity Identity is SentinelOne's answer for identity security. In March 2022, SentinelOne announced a definitive agreement to acquire Attivo Networks and has since rebranded it as Singularity Identity. While it is being positioned by SentinelOne as an integral part of its Singularity platform, rebranding does not automatically make it part of a unified platform. There are multiple considerations that should drive your decision when choosing an identity protection solution for your workforce, ranging from product architecture, integration and speed of deployment to fidelity of detections, the ability to provide real-time protection and the option to choose a fully managed offering. We encourage you to do your own research and make sure you ask the following important questions before making your choice.

1. DOES THE SOLUTION PROVIDE A TRULY UNIFIED VIEW OF THREATS ACROSS ENDPOINTS AND IDENTITIES USING A SINGLE, UNIFIED SENSOR?

Following CrowdStrike's footsteps, a number of EDR vendors have started expanding their offerings to include identity protection. This includes SentinelOne, which acquired Attivo Networks to try to plug the identity protection gap in its portfolio. However, SentinelOne Singularity (Attivo) uses a different agent and architecture than SentinelOne's endpoint sensor. This can complicate deployment without providing immediate value in terms of real-time protection. Attivo was founded on deception technology and its architecture does not lend itself to a seamless integration with the rest of the Singularity platform.

An effective, efficient solution should provide a unified view of threats across endpoints and identities without forcing a security analyst to traverse multiple consoles and manually correlate the attack signals across endpoints and identities. An integrated security platform should also provide a single sensor that will intelligently collect the appropriate signals from the device or identity store based on where it is deployed.

If you need real-time identity protection today, an unproven, disjointed solution may not be the best choice.

ADVANTAGE: CROWDSTRIKE FALCON IDENTITY PROTECTION

Falcon Identity Threat Protection — fully integrated with the CrowdStrike Falcon® platform — is the ONLY solution in the market to natively provide comprehensive protection against identity-based attacks in real time without requiring any integration or significant deployment efforts. CrowdStrike customers can simply enable the Identity Threat Protection module to immediately get protection from identity-driven attacks.

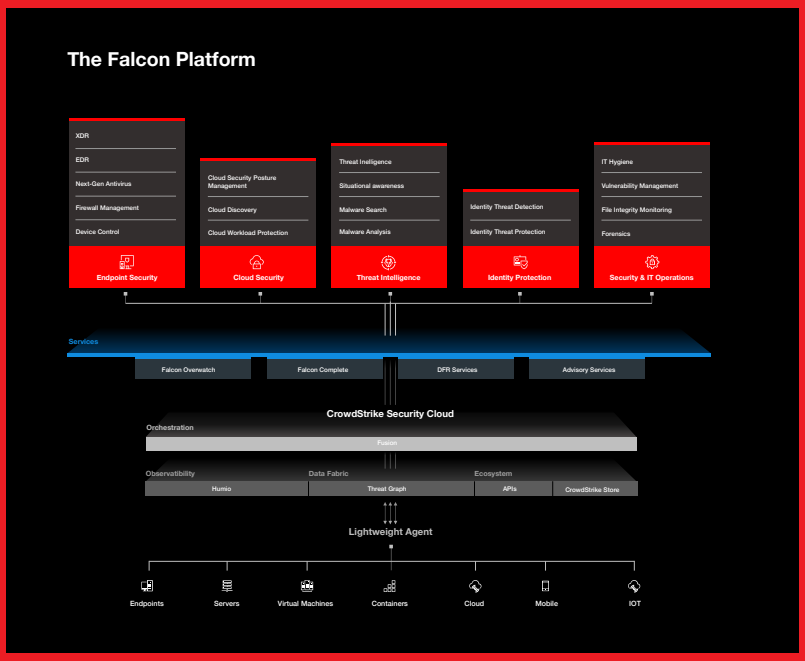


Figure 1. Falcon platform powered by the CrowdStrike Security Cloud

Since the acquisition of Preempt in 2020, CrowdStrike rapidly integrated Preempt's identity protection capabilities into the Falcon platform so customers can easily add protection from identity-based attacks without any additional deployment overhead. The same stable and reliable Falcon sensor that protects millions of endpoint devices can protect your AD domain controllers as well. It has the intelligence to pull the relevant identity data into the unified Falcon platform, which is powered by the CrowdStrike Security Cloud to correlate this threat data across customer endpoints, workloads, identities and data. This unified view and tight correlation is what allows for hyper-accurate detections of threats. The power of this native identity-protection capability was well-demonstrated in the **recent MITRE Engenuity ATT&CK Evaluation**, in which the Falcon platform shut down adversaries and stopped the breach before the test even started.

CrowdStrike's integrated platform approach also extends to a broad ecosystem of partners enabling customers to operationalize Zero Trust with reduced cost and complexity leveraging pre-built integrations for any deployment model (including on-premises, hybrid cloud, and SaaS) and for traditionally difficult to secure entities (remote users, legacy systems, and unmanaged devices).

2. BEYOND DETECTION, WILL YOU GET REAL-TIME PROTECTION FROM IDENTITY-BASED THREATS BASED ON A FLEXIBLE POLICY ENGINE?

While accurate detection of identity-based attacks is important, it is not enough. The real value of an identity protection solution is getting real-time protection from identity-based attacks so adversaries can be stopped in their tracks. Offering only lures and misdirections as deception capabilities is not enough to guarantee that you have successfully blocked the adversary. You should look for a powerful, flexible policy engine that comes with pre-baked, risk-based conditional policies that can immediately block the adversary or require multi factor authentication (MFA) challenge.

These actions are even more critical to protect your on-premises Active Directory environment, which is often considered the weakest link in an organization's cyber defenses. It is not enough if the vendor can only trigger Azure AD conditional access. For a truly frictionless experience, your identity protection solution should have proven integrations with a wide array of MFA providers and identity access management (IAM) solutions so you are not constrained to a specific solution.

ADVANTAGE: CROWDSTRIKE FALCON IDENTITY PROTECTION

Falcon Identity Threat Protection not only provides hyper-accurate detections, it provides real-time protection, leveraging a rich, powerful policy engine that can enforce risk-based conditional access. This enforcement includes alerts, MFA challenges and blocking the adversary in real time.

Falcon Identity Threat Protection's insights are powered by 40+ conditions such as user roles, human or service accounts, behavior and access patterns, location, endpoint type and risk scores. These conditions are dynamically analyzed to enable real-time decision making and can be configured to trigger conditional access/MFA from multiple vendors — both on-premises and in the cloud — including Okta, Ping, Duo and others. CrowdStrike's conditional access is wider and deeper, taking signals from across a complex, hybrid identity landscape, adding to increased fidelity in detecting and preventing identity-related threats in real time.

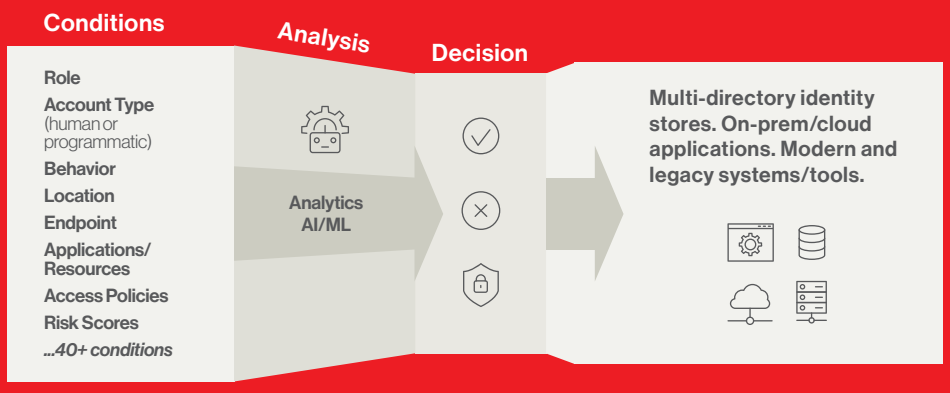


Figure 2. Flexible Conditional Access with Falcon Identity Threat Protection

3. DOES THE SOLUTION OFFER A TIGHT CORRELATION BETWEEN IDENTITY AND ENDPOINT SIGNALS TO PROVIDE CLEAR ATTACK PATH VISIBILITY?

When an adversary launches an attack combining various tactics, techniques and procedures (TTPs) across endpoints, devices and identities, it is extremely important that your identity protection solution can tightly correlate the signals it receives from these different sources with indicators of attack (IOAs) and threat intelligence to rapidly detect the threat, determine the attack path and stop the adversary in real time. It is not enough to slow down the adversary with cloaking technology and send signals to a platform that has no ability to understand or correlate those signals with other threat data in real time. Without tight correlation, these identity alerts only add to the noise, leaving the customer with the difficult, time-consuming task of correlating threat data across endpoints and identity to determine the attack path. And in the event of an actual attack, where every second is precious, you cannot afford this delay.

ADVANTAGE: CROWDSTRIKE FALCON IDENTITY THREAT PROTECTION

Falcon Identity Threat Protection, part of the Falcon platform, is the ONLY identity protection solution in the market that is deeply integrated with a broader security platform that can leverage real-time IOAs, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections. It is powered by the CrowdStrike Security Cloud — one of the world's largest unified, threat-centric data fabrics — which correlates trillions of security events per day with IOAs, the industry's leading threat intelligence and enterprise telemetry from across customer endpoints, workloads, identities and data.

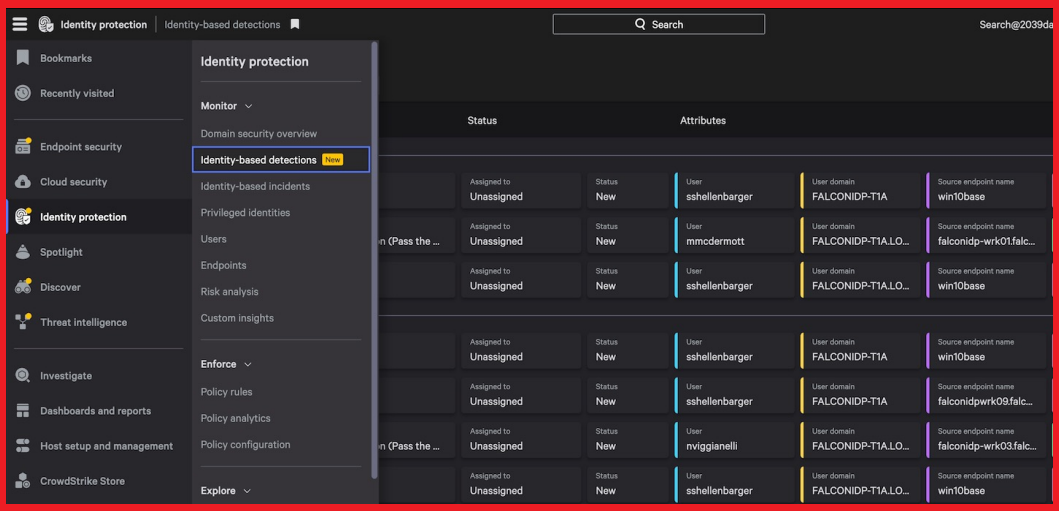


Figure 3. Falcon's standard Detections interface used for identity threat detections

This tight correlation not only allows identity threat detections to be shown in the Detections interface used by the rest of the Falcon platform, it also enables the unified sensor to take immediate action either at the endpoint or identity level to quickly block the adversary. For example, the Falcon sensor can block the authentication operation from an endpoint that may have been compromised or block an endpoint used by a user that is determined to be risky. This integrated approach also allows an organization to extend protection to unmanaged endpoints like a temporary contractor's laptop.

4. DOES THE SOLUTION PROVIDE THE OPTION TO HAVE A FULLY MANAGED SOLUTION COVERING ENDPOINTS AND IDENTITIES WITH EXPERT MANAGEMENT, MONITORING AND REMEDIATION, AND IS IT BACKED BY AN INDUSTRY-LEADING BREACH PREVENTION WARRANTY?

Technology alone is not a silver bullet to stopping breaches. Sophisticated attacks targeting the crown jewels of an enterprise often require a mix of technology and human expertise to mount an effective defense, ensuring defenses are optimized and response to threats can come in minutes. While any vendor can loosely use terms like artificial intelligence (AI) and machine learning (ML) to describe their technology, it takes a mature cybersecurity leader to recognize that AI/ML by itself cannot replace human expertise. And SentinelOne can certainly not provide the peace of mind that comes with a completely managed solution with expert management and monitoring of endpoints and identities, especially if you do not have the in-house resources to take on adversaries.

ADVANTAGE: CROWDSTRIKE FALCON IDENTITY THREAT PROTECTION

CrowdStrike is the only security-focused vendor to offer a fully managed identity threat protection solution that provides expert management, monitoring and remediation to deliver frictionless, real-time identity threat prevention — all backed by an industry-leading Breach Prevention Warranty.

The solution combines CrowdStrike's leading Falcon Identity Threat Protection with the expertise of the Falcon Complete™ managed detection and response team, which manages and actively monitors Falcon for customers, investigating and surgically remediating incidents in minutes. Managed identity threat protection helps organizations to run an effective and mature identity security program without the burden, costs and time associated with building one internally.

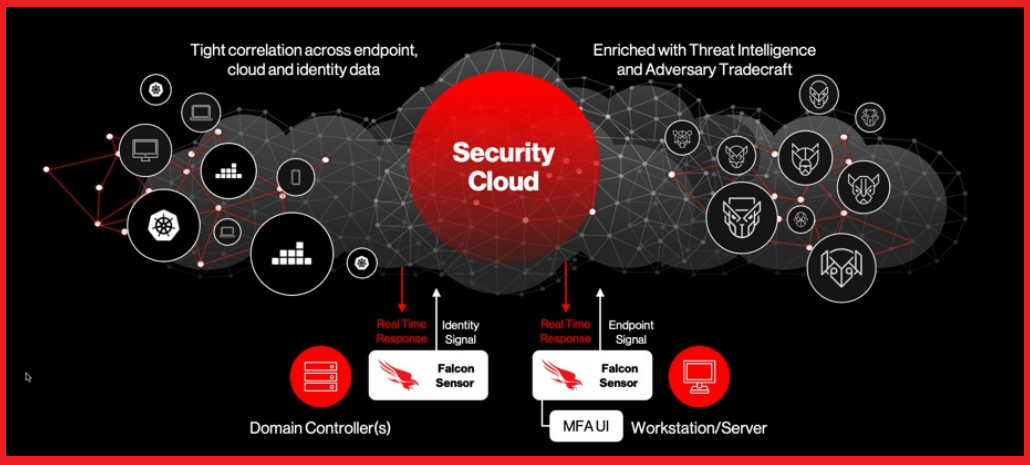
Download the **Falcon Identity Threat Protection Complete** data sheet for more details.

5. IS DECEPTION EVEN THE RIGHT STRATEGY FOR YOUR ORGANIZATION TO GET IMMEDIATE REAL-TIME PROTECTION FROM AD ATTACKS?

While deception technology sounds good on paper, it is difficult to operationalize and achieve quick time-to-value, especially as adversaries are relentlessly attacking your weakest links: your Active Directory deployment. Attivo was founded on deception technology and the Singularity Identity offering is a complex deployment with agents, honeypots, decoys and baits that require a thorough understanding of a customer's environment as well as deep knowledge of adversary behavior and tradecraft. (Attackers have been bypassing honeypots for over 25 years.) In addition, SentinelOne uses the words "deception" and "protection" interchangeably when describing its Singularity Identity product, which can be quite confusing. Deception is trying to lure the adversary away from your crown jewels via baits and decoys. But that should not be confused with real-time protection that blocks the adversary or throws an MFA challenge as soon as an identity-based threat is detected.

ADVANTAGE: CROWDSTRIKE FALCON IDENTITY THREAT PROTECTION

CrowdStrike Falcon Identity Threat Protection provides real-time protection against identity-based attacks without relying on a complex deployment of lures, decoys and baits.



With a frictionless deployment architecture that uses the same lightweight Falcon sensor on AD domain controllers as on your endpoints, it provides immediate value through real-time detection and prevention of AD attacks. You do not have to spend multiple trial-and-error cycles with deception technology hoping you have made the right design assumptions to successfully misguide the adversaries from reaching your crown jewels. The power of Falcon Identity Threat Protection is its sheer simplicity, which not only provides direct visibility into all authentication traffic but also the ability to take immediate action to block the adversary in real time.

NEXT STEPS

Request a demo of the CrowdStrike Falcon Identity Protection solution, and discuss in detail with our specialists how it offers better workforce identity protection than SentinelOne Singularity Identity and how it takes a high-fidelity, less complex and frictionless approach to protecting your workforce identities — one that will enable you to proceed on your Zero Trust journey.

Download **this whitepaper** to learn how Falcon Identity Protection reduces AD security risks and protects your organization from ransomware and supply chain attacks.

Methodology: This comparative analysis of SentinelOne Singularity Identity's identity protection capabilities was conducted in May 2022, based on publicly available information published by Attivo/SentinelOne.

ABOUT CROWDSTRIKE

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates upward of 1 trillion endpoint-related events per day in real time from across the globe, fueling one of the world's most advanced data platforms for security.

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** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

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