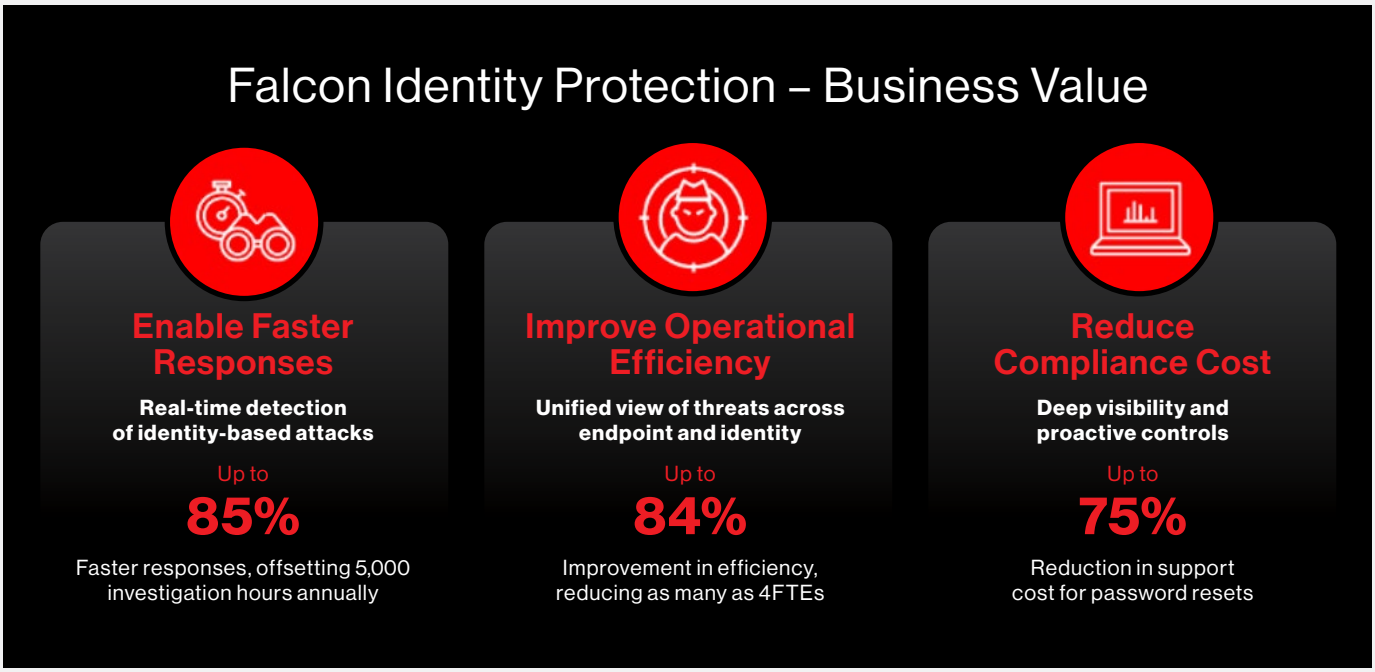
CrowdStrike White Paper

CROWDSTRIKE

Top Reasons to Add Falcon Identity Threat Protection to Your Cyber Defense Portfolio Now

Identity-based attacks are the number one cybersecurity threat facing organizations today. In fact, over 80% of cyber incidents involve the misuse of valid credentials to gain access to an organization's network.

CrowdStrike Falcon® Identity Threat Protection, a module of the CrowdStrike Falcon® platform, detects and stops identity-driven breaches in real time across a complex hybrid identity landscape, with a single sensor and a unified threat interface with attack correlation across endpoints, workloads, identity and data. Here are five expected benefits you can get by adding identity protection to your cybersecurity threat portfolio today.*



1. Enables up to 85% faster responses to threats

Traditional endpoint-only solutions miss identity threats, and the current approach of manually correlating threats across endpoint and identity with multiple standalone tools — AD hygiene tools, Windows Event Logs, PAM, UEBA, SIEM and more — slow down responses from the SOC team. With the unified CrowdStrike Falcon platform, Falcon Identity Threat Protection customers are able to see full attack paths and correlate threats within a single console. This can result in **up to 85% faster responses** and real-time protection, offsetting thousands of hours of post-breach investigation every year.

2. Increases operational efficiency by up to 84%

CrowdStrike Falcon is **a cloud-native solution with a single sensor** that can be deployed anywhere in the customer environment, simplifying the collection of telemetry (from endpoint or identity). A large retail distributor **consolidated 5+ tools** (typical of many companies) into one to manage identity threats with Falcon Identity Threat Protection. SOC consolidation with one platform and sensor eliminates standalone tools and agents, resulting in direct savings of tool and operational costs. And, by removing the need to employ disparate log ingestion, real-time detection can reduce total maintenance hours and **increase operational efficiency by up to 84%**, reducing headcount by roughly four FTEs.

3. Reduces compliance and support costs by up to 75%

Deep visibility into compromised passwords, over-privileged accounts and service account misuse enables customers to proactively address Active Directory hygiene issues and establish proactive controls, thereby reducing compliance costs. In one case, a CISO reported a **75% reduction in support password resets and associated costs,** 8% reduction in phishing susceptibility and 32% reduction in unnecessary user access rights. A large telecom provider reported improving Cybersecurity Maturity Model Certification (CMMC) compliance posture by using Falcon Identity Threat Protection to extend multifactor authentication (MFA) everywhere, including legacy applications.

4. Reduces the risk of stolen credentials leading to a breach by up to 57%

With eight out of 10 attacks involving stolen or compromised credentials, reducing the risk of stolen credentials has a direct impact on improving risk posture. Falcon Identity Threat Protection's ability to detect identity specific threats allows customers to identify high-risk accounts and possible attack paths across their entire environment, reducing the attack surface. Recently, the CISO for a hospitality chain shared how Falcon Identity Threat Protection immediately revealed 250,000 possible attack paths in the company's environment and how 93% of them could be fixed with three specific configuration changes. CrowdStrike Business Value Assessments have shown a **reduction of up to 57% in the risk of stolen credentials** leading to a breach. This has also been demonstrated by successful penetration tests done by customers that had failed the same tests prior to deployment of Falcon Identity Threat Protection.

5. Improves cyber insurability and reduces premiums

As adversaries continue to exploit weak identity security controls to launch attacks, **cyber insurance companies are emphasizing** the need to tighten controls to reduce cyber risk. With ransomware being one of the key factors for cybersecurity insurance, insurers have reiterated the need for organizations to harden AD, enforce MFA across applications including legacy ones, protect privileged and service accounts, and deploy endpoint detection and response (EDR) as prerequisites for cyber insurability. Customers that have deployed Falcon Identity Threat Protection say it has positively impacted their cybersecurity insurance program and reduced premiums.

What CrowdStrike customers say

"After deploying Falcon Identity Threat Protection, we did another penetration test and immediately saw the benefits of the enhanced visibility."

Ryan Melle
SVP, CISO, Berkshire Bank
(**Read case study**)

"Since deploying Falcon Identity Threat Protection, we've had a massive uplift in what we can see with regard to credentials, privileged identities, different attack paths and how we can mitigate them."

Steven Townsley
Head of Information Security, Mercedes-AMG Petronas F1 Team
(**Watch video**)

"Within two hours of deploying Falcon Identity Threat Protection, we identified 10 privileged accounts with compromised passwords and began resetting them immediately."

CISO of a county in the Washington, D.C. area
(**Read blog post**)

"We got the value out of Falcon Identity Threat Protection within the first minute, when we got to see 250,000 possible attack paths and 93% of them could be fixed with just three configuration changes."

CISO of a multinational hospitality chain

"It is just easier to keep one pane of glass for the majority of your SOC than look across 13 different consoles and pages to analyze and track something down."

CISO of an agribusiness and food company

Identity Protection Is Essential, Not Optional

The CrowdStrike 2023 Global Threat Report shows that identity attacks are on the rise, with a **112% growth in access broker ads** on the dark web in 2022. Microsoft Active Directory continues to be the soft underbelly for adversaries to go after, with over 90% of organizations relying on it.[1] A recent meta-data analysis of millions of accounts (human, service, privileged) by CrowdStrike revealed a **staggering 50% of the organizations have privileged accounts with a compromised password**.

Compounding this problem, identity breaches are notoriously hard to detect, requiring an average of **around 250 days to identify**[2] without the right tools. During that time, adversaries can move laterally undetected in your environment and launch catastrophic attacks. With average breakout time **down to 84 minutes in 2022**, according to the CrowdStrike 2023 Global Threat Report, organizations do not have the luxury to wait for a serious identity breach to occur. In fact, the adversary may already be in your environment and you may not be aware of it.

There could be serious consequences of ignoring identity-driven threats, including total domain compromise of your AD infrastructure, crippling ransomware attacks and catastrophic business outages. According to IBM and the Ponemon Institute, the **global average total cost of a data breach is $4.35 million USD ($9.44 million USD average cost of breach in the United States)**.[3] With **8 out of 10 attacks** involving stolen or compromised credentials, deploying identity protection will have immediate impact, potentially saving you millions of dollars and protecting your brand and reputation from irreversible damage.

Remember, adversaries are not waiting for you to put on your gloves before they throw their punches. Stop the breach today with Falcon Identity Threat Protection.

Contact your CrowdStrike account representative or request your complimentary Active Directory Risk Review.

[1]Frost & Sullivan, "Active Directory Holds the Keys to your Kingdom, but is it Secure?"

[2]IBM and Ponemon Institute, "Cost of a Data Breach Report 2022"

[3]IBM and Ponemon Institute, "Cost of a Data Breach Report 2022"

*Expected results and actual outcomes are not guaranteed and may vary for every customer. Expected benefits 1, 2 and 4 are based on aggregated averages from over 100 Business Value Assessment (BVA) and Business Value Realized (BVR) cases conducted with CrowdStrike Enterprise customers and completed by CrowdStrike's Business Value team from 2018 to December 2022. BVAs are a projected ROI analysis based on the value of CrowdStrike compared to the customers incumbent solution. BVRs are a realized ROI analysis for customers deployed for 6+ months using customer inputs and recorded telemetry. Expected benefit 3 is based on data shared by a customer directly with CrowdStrike.

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.**

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

Start a Free Trial

Learn more at **www.crowdstrike.com**