CrowdStrike White Paper

REDUCE ACTIVE DIRECTORY SECURITY RISKS

A frictionless approach to securing your crown jewel identity store

WHY YOU SHOULD SECURE YOUR ACTIVE DIRECTORY NOW

Securing the Microsoft Active Directory (AD) identity store is the major step in protecting an organization from modern attacks, including ransomware, supply chain threats and account takeover. A common thread that connects most of the recently publicized potential breaches is the compromise of credentials whose authentication is governed by AD. The AD is one of the crown jewels in an organization, as it stores critical information such as users, groups, computers, applications, policies, contacts and, of course, the login credentials of the resources and applications that are being accessed. First released in 1999, AD is undoubtedly legacy technology; nonetheless, it is still the de facto identity infrastructure within most modern companies. With over 90% of Fortune 1000 companies using AD,[1] it isn't surprising to see this directory service being targeted by adversaries — making it a renewed priority for security teams to protect this crown jewel asset.

Today, a huge majority of endpoints are authenticated by Microsoft AD or Microsoft Azure AD. Microsoft has recently recommended that organizations shift to Azure AD to negate its on-premises AD vulnerabilities, like Golden SAML attacks. However, even if organizations move to Azure AD, which might take years, they still have to protect both their on-premises AD and Azure AD with limited visibility into who the users are, what they are up to, what the attack path looks like and how the AD/Azure AD security posture is changing. And for organizations that get into a merger or divestiture, how can they merge or separate the identities and the identity stores during and after the M&A or divestiture exercise?

Securing your AD is critical *right now*. In supply chain attacks[2] in November 2020, and in more recent ransomware attacks on critical organizations such as Colonial Pipeline and JBS, compromised credentials were the key factor in lateral movement and attack progression. According to a report by IBM and the Ponemon Institute, in 2021, compromised credentials led to compromised data, and stolen user credentials were the most common root cause of breaches.[3] More importantly, the study also highlighted that the breaches resulting from compromised credentials took the longest time — an average of 250 days — to identify.

For threat actors, ransomware has become the most lucrative attack tactic, with an estimated 300 million[4] ransomware attacks in 2020, and with a projected global ransomware cost of $20 billion USD.[5] The increase in ransomware also has a direct bearing on cyber insurance premiums and coverage. The increase in cyber insurance premiums (ranging from 10% to 30% during the latter half of 2020[6]) have been directly attributed to increasing insurer losses caused by ransomware attacks that occur with increasing sophistication and severity. Another fallout of this increase in ransomware attacks is the reduction in coverage limits, specifically in high-risk industries like **healthcare**.

CrowdStrike Falcon Identity Protection is the first cloud-native identity security solution to protect your AD/ Azure AD from modern attacks, enabling your organization to:

- Improve AD hygiene with continuous unified visibility and security control of identities across AD/Azure AD, SSO and federation services in hybrid setups
- Realize live AD attack detection and automated response
- Speed up incident detection with identity-based segmentation: auto-classify all accounts — human, service and privileged — to determine the who, where, when and why
- Ascertain and fix security gaps in privileged accounts and authentication patterns by continuously assessing risks tied to users and devices
- Enforce frictionless conditional access and risk-based multifactor authentication (MFA) even on legacy tools and applications
- Get detailed visibility and security control over encrypted protocols like NTLM and LDAP/S
- Reduce noise with the industry's highest-fidelity attack correlation and improve the mean time to detect and stop threats like ransomware and supply chain attacks

[1] ttps://www.frost.com/frost-perspectives/active-directory-holds-the-keys-to-your-kingdom-but-is-it-secure/
[2] https://www.crowdstrike.com/sunburst/
[3] Cost of a Data Breach Report 2021
[4] https://www.statista.com/statistics/494947/ransomware-attacks-per-year-worldwide/
[5] Recognize Ransomware
[6] https://www.gao.gov/products/gao-21-477

TRADITIONAL AD SECURITY IS UNABLE TO KEEP UP WITH MODERN ATTACKS

A security compromise of AD exposes the identity infrastructure and creates a very large attack surface that may lead to ransomware, data breaches and eventually damage to the business and reputation. The security team and the identity and access management (IAM) team try to secure the AD identity store, but they need to be sure that legacy and deprecated protocols (e.g., versions like NTLMv1) are not being used. And they need to know in real time if a specific service account or a stale account is executing a Remote Desktop Protocol (RDP) to the Domain Controller (DC), or trying to move laterally to critical servers by escalating privileges or using stolen credentials.

The AD architecture is over two decades old, built prior to the establishment of Zero Trust principles, and this widely used authentication architecture poses a risk as the systemic weaknesses in credentials have been carried over and spread across Microsoft's cloud directory services. The architectural limitations of Microsoft Active Directory Federation Services (ADFS) played a key role as the threat actor executed the Golden SAML attack in the notorious supply chain attack in November 2020.[7]

In addition, Microsoft itself pointed out that this supply chain attack started "on-premises," and customers that haven't migrated to the cloud will continue to be victims of such attacks in the future.[8] This does not mean customers that migrate to Azure AD will necessarily be better protected from these attacks, as attackers can use stolen on-premises AD credentials to gain access to Azure AD. And as stated earlier, even if organizations move to Azure AD, they still have to protect both their on-premises AD and Azure AD due to Microsoft's architectural limitations. A case in point is the most recent attack: The Azure AD password brute-forcing flaw[9] has no fix (as of October 2021) and essentially enables threat actors to endlessly perform single-factor, brute-force attacks without alerting the IAM or security teams to these malicious sign-in events.

Security and IAM teams may be insufficiently equipped to detect and stop attacks like these. With traditional and siloed AD security tools, it's difficult for them to get a timely grasp on:

- Identifying the user accounts (including service, privileged and stale accounts) that are part of an ongoing breach, and those whose risks are high and need to be constantly monitored
- Identifying suspicious account activities and movements across the network
- Accounts whose passwords need to be reset automatically or according to best practice recommendations and compliance standards
- Enforcing step-up authentication — MFA based on a combination of deterministic and risk-based factors
- Controlling and monitoring logins on systems, applications and tools (and also on common tools and unique combinations like RDP over NTLM) through risk-based MFA (for example, desktops are not covered by cloud-based MFA solutions)

[7] https://www.crn.com/slide-shows/security/crowdstrike-ceo-george-kurtz-takes-big-swings-at-microsoft-sentinelone/2
[8] https://www.intelligence.senate.gov/sites/default/files/documents/os-bsmith-022321.pdf
[9] https://arstechnica.com/information-technology/2021/09/new-azure-active-directory-password-brute-forcing-flaw-has-no-fix/

The limitations of traditional and siloed AD security tools increase the overall attack surface for identity-based attacks. These challenges are a few of the reasons why 80% of the attacks are credential-based.[10] Though AD and IAM teams may use several tools to secure AD, the real need is to secure both AD and Azure AD from a unified console to enable them to holistically understand the who, where, when and why for every authentication and authorization request, and the risks facing the organization, and also enable them to extend risk-based MFA/ conditional access to legacy applications to significantly reduce the attack surface.

PROTECTING YOUR AD STARTS WITH FALCON IDENTITY PROTECTION

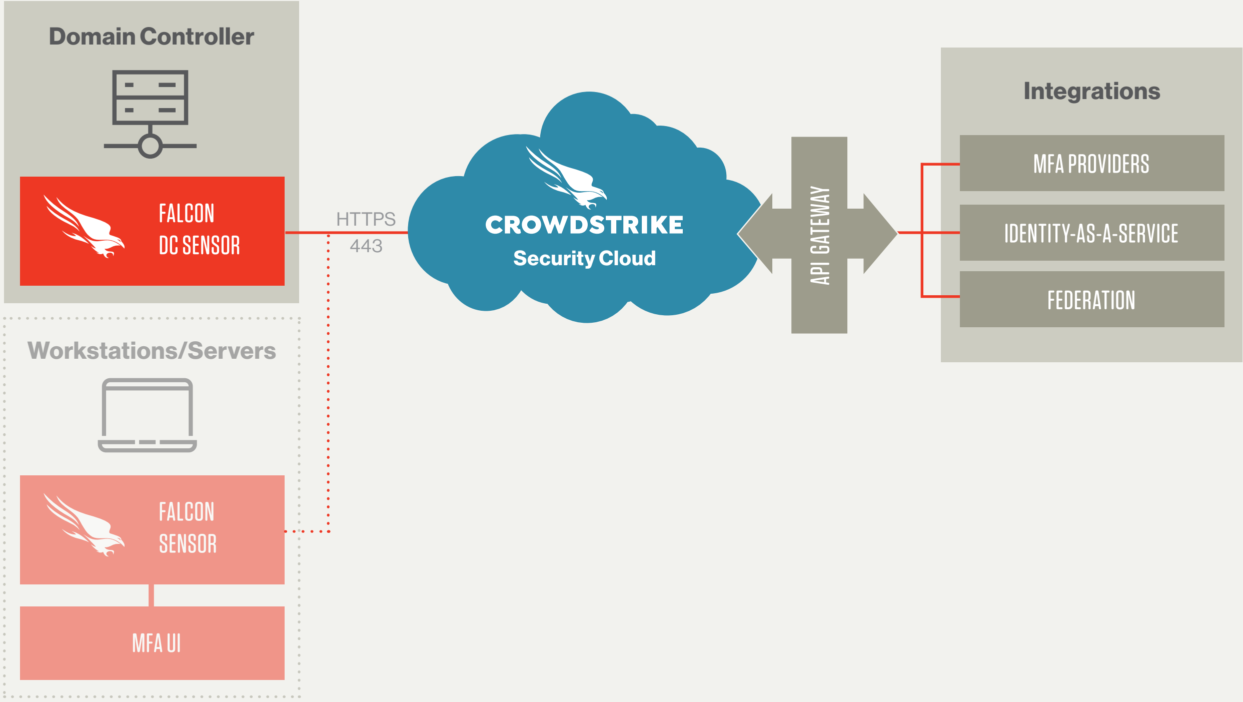
Organizations traditionally have invested in perimeter security controls to protect the enterprise from north-south traffic. For east-west traffic, they use microsegmentation solutions that have become popular over the last couple of years. Due to digital transformation, the explosion of users and applications, and Zero Trust initiatives, the perimeter is moving closer to the resources. Since a majority of modern attacks are based on credentials, identity is not only the most important element in Zero Trust — identity is the **new perimeter**. CrowdStrike Falcon Identity Protection wraps security around every identity, whether on on-premises AD, cloud AD or Azure AD.

Falcon Identity Protection, part of the CrowdStrike Falcon® platform, is built around a continuous risk scoring engine that analyzes security indicators present in authentication traffic in real time. Adhering to Zero Trust principles, the risk scores are developed inside-out — around user roles, user-defined authentication policies and identity stores — instead of the traditional outside-in sources. Falcon Identity Protection is the only cloud-native Zero Trust solution to protect AD — the weakest link in your cyber defense.

[10] https://www.forrester.com/report/The-Forrester-Wave-Privileged-Identity-Management-Q4-2018/RES141474

EASY DEPLOYMENT AND FASTER TIME TO VALUE

Falcon Identity Protection is simple and straightforward, requiring only a lightweight sensor on the domain controllers (DCs); the CrowdStrike Falcon sensors talk to the CrowdStrike Security Cloud, which does all of the heavy lifting. Falcon Identity Protection is managed from the unified Falcon console.



Falcon Identity Protection installation is independent of Falcon Endpoint Protection modules. However, if Falcon Endpoint Protection modules are already installed ("Falcon installed"), then Falcon Identity Protection can immediately:

- Digest the Falcon Zero Trust Assessment (ZTA) score to enforce policies based on the source and destination ZTA score
- Provide a popup on end user workstations to select the MFA they want to authenticate with
- Detect local admins on endpoints

Falcon Identity Protection provides several benefits from day one, even in hybrid environments:

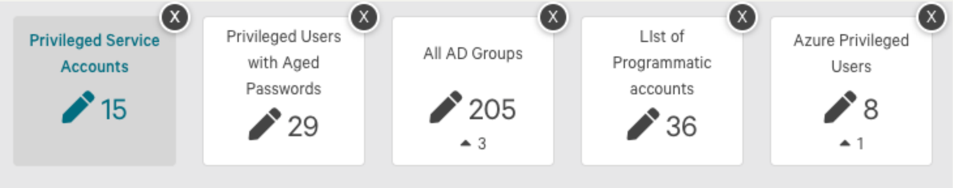
- Falcon DC sensors can be deployed at scale in hours, not days
- Sensors are only on the domain controllers
- Frictionless security with minimal policies is powered by automation and analytics from the CrowdStrike Security Cloud
- It enables instant detection and prevention of identity-related incidents without the overhead of looking into logs, managing terabytes of data and threat feeds
- It includes built-in integrations with MFA providers, IDaaS and federation/SSO solutions like ADFS, PingFederate and Okta

GET INSTANT VISIBILITY INTO AD HYGIENE TO DISCOVER GAPS

In hybrid environments, a holistic view of the accounts, activities and risks is important for timely detection of identity threats. In a siloed approach, security and AD teams must manually connect the dots and could take days to determine AD gaps.

The key questions your AD team must be able to answer are: “How many service and stale accounts are there in AD?” “What are the gaps around privileged accounts?” and “What are these accounts up to, right now?”

Using **identity segmentation**, Falcon Identity Protection provides real-time insights into every account in hybrid environments — the human and privileged users and the service accounts — along with insights into what these accounts are doing, what their privileges are, whether they are compromised, and which applications they are accessing and from which endpoint and location.

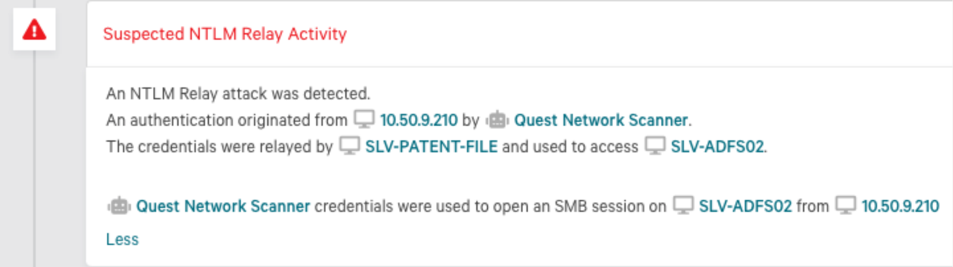

X
Privileged Service Accounts
15
X
Privileged Users with Aged Passwords
29
X
All AD Groups
205
3
X
LIst of Programmatic accounts
36
X
Azure Privileged Users
8
1

Falcon Identity Protection monitors every new credential added (e.g., through a merger), every credential increasing in risk, and credentials that are compromised, according to the continuously changing security context (e.g., a genuine user logging on to critical servers from an endpoint running Windows 7 or other unsupported operating systems).

AUTOMATICALLY ASSESS THE AD THREAT LANDSCAPE TO MITIGATE HARD-TO-DETECT IDENTITY INCIDENTS IN REAL TIME

Instant visibility into AD hygiene enables security teams to quickly evaluate their current identity security posture and determine lateral movement — the key technique used in most ransomware and supply chain attacks. Of course, feeding authentication logs into their existing security information and event management (SIEM) and other log-based solutions will provide some key pieces of information relating to modern attacks, but to hunt for the proverbial needle in the haystack takes time and correlation rules, resulting in false positives — which favor the attackers, who can then proceed with their techniques and tactics undetected. (And as mentioned, breaches resulting from compromised credentials take the longest to detect.) There’s another disadvantage of feeding authentication logs to your SIEM: the **increase in licensing costs** due to increased log storage volume.

Falcon Identity Protection performs user behavior analysis based on traffic and authentication patterns, instead of looking into logs, to determine hard-to-detect threats such as ransomware, lateral movement, RDP to DC, interactive logins of service accounts and more. Traditional user and entity behavior analytics (UEBA) solutions typically provide detection capabilities through the complicated methods of log collection, analysis and continuous tuning of rules, but they cannot prevent threats in real time.



Suspected NTLM Relay Activity

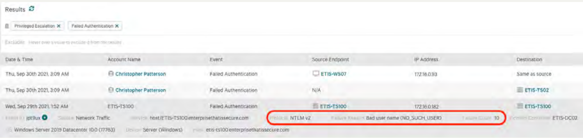
An NTLM Relay attack was detected.
An authentication originated from 10.50.9.210 by Quest Network Scanner.
The credentials were relayed by SLV-PATENT-FILE and used to access SLV-ADFS02.

Quest Network Scanner credentials were used to open an SMB session on SLV-ADFS02 from 10.50.9.210

Falcon Identity Protection automatically evaluates user trust in real time to determine whether access has to be given to specific resources — meaning the analysis is done before the authentication request hits the AD. By analyzing hundreds of behavioral patterns, Falcon Identity Protection creates the baselines tied to identities. Incidents such as lateral movement, risky behavior, suspicious movements, unusual endpoint usage, privilege escalation, interactive logins by service accounts, malicious RDP attempts, encrypted protocol usage and many others are detected in real time without the time deltas required for log transmission, storage and processing.

REDUCE INVESTIGATION TIME WITH INTUITIVE THREAT HUNTING

Combining the power of unified visibility across AD and Azure AD, Falcon Identity Protection provides an integrated threat hunting solution to investigate specific events in detail. One of the most common incidents related to ransomware and supply chain attack progression is privilege escalation, combined with failed logins.



Results

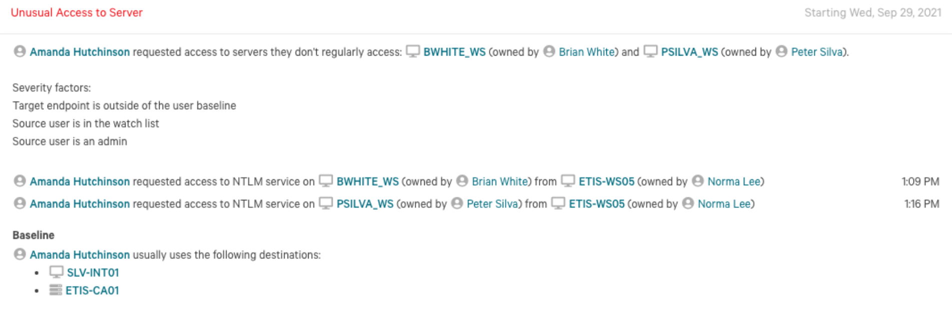
Date & Time	Account Name	Event	Source Endpoint	IP Address	Destination
Thu, Sep 30th 2021, 3:09 AM	Christopher Patterson	Failed Authentication	ETIS-WS07	172.16.0.93	Same as source
Thu, Sep 30th 2021, 3:09 AM	Christopher Patterson	Failed Authentication	N/A		ETIS-TS02
Wed, Sep 29th 2021, 1:52 AM	ETIS-TS100	Failed Authentication	ETIS-TS100	172.16.0.182	ETIS-TS100

Event ID: jpt9ux Source: Network Traffic Service: host/ETIS-TS100.enterprisethatissecure.com Protocol: NTLM v2 Failure Reason: Bad user name (NO_SUCH_USER) Failure Count: 10 Domain Controller: ETIS-DC02
OS: Windows Server 2019 Datacenter 10.0 (17763) Device: Server (Windows) etis-ts100.enterprisethatissecure.com

For example, because privileged users pose a much higher risk than most others, you can hunt for threats in Falcon using “Privileged Escalation” as the user account event and “Failed Authentication” as the authentication event to find all such events. Further, the threat hunter helps the teams see the number of failed logins, and deep dive and pivot to related incidents without writing scripts or using disparate tools.

DETECT AND INVESTIGATE ATTACKS AGAINST AD AND IDENTITIES

Attackers steal user credentials through a variety of methods such as unauthorized devices (unknown or unmanaged from within or outside the organization's network), credential stuffing, password spraying, phishing, compromised applications and more. In almost all of these attacks, the idea is to gain access to an endpoint or server and then move laterally as an authenticated user to crown jewel applications or databases. Falcon Identity Protection detects and alerts on these suspicious activities and many more, and also recommends the correct mitigation to stop the attack progression.



Unusual Access to Server

Starting Wed, Sep 29, 2021

Amanda Hutchinson requested access to servers they don't regularly access: BWHITE_WS (owned by Brian White) and PSILVA_WS (owned by Peter Silva).

Severity factors:
Target endpoint is outside of the user baseline
Source user is in the watch list
Source user is an admin

Amanda Hutchinson requested access to NTLM service on BWHITE_WS (owned by Brian White) from ETIS-WS05 (owned by Norma Lee) 1:09 PM
Amanda Hutchinson requested access to NTLM service on PSILVA_WS (owned by Peter Silva) from ETIS-WS05 (owned by Norma Lee) 1:16 PM

Baseline

Amanda Hutchinson usually uses the following destinations:

- SLV-INT01
- ETIS-CA01

PROTECT AGAINST NTLM RELAY ATTACKS

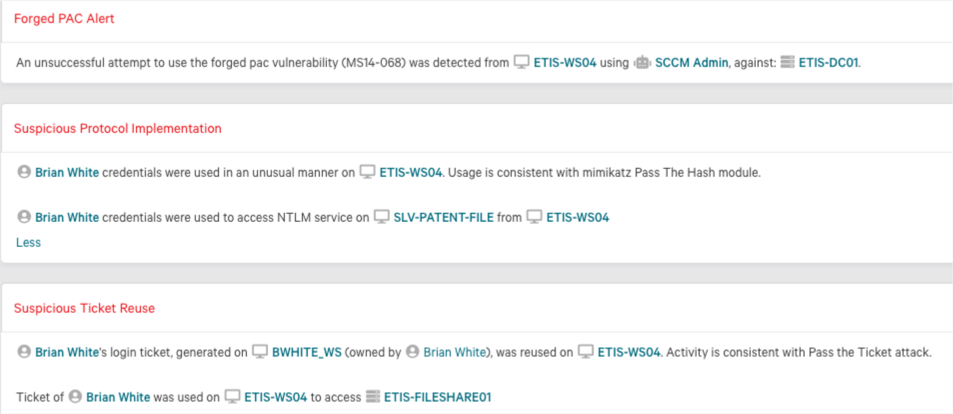
NTLM is one of the oldest authentication protocols and still poses one of the greatest threats for AD environments. Though Microsoft released several mitigations such as SMB server signing, NTLM relay has been one of attackers' favorites, as evident from CVE-2015-0005 to several recent LDAP/S relay vulnerabilities. Falcon Identity Protection can detect NTLM usage in real time and with simple policies, and can stop authentication actions using this protocol. **Watch this webcast** on how the CrowdStrike Zero Trust team was able to abuse NTLM and bypass all NTLM relay mitigations, and hear their recommendations on how to protect your AD.

MONITOR AND STOP UNAUTHORIZED RDP USAGE

RDP to DC has to be critically monitored — and by default, only members of the Domain Admins group can perform this action. One way to protect DCs is to trigger identity verification every time any user tries to authenticate. An attacker can use an unmonitored service account, conduct privilege escalation and then RDP to DC. CrowdStrike Falcon Identity Protection can **detect and stop** this activity in real time.

STOP GOLDEN TICKET AND PASS-THE-HASH (PTH) ATTACKS

Kerberos is the default authentication protocol that Microsoft has been using for the past two decades. In a Golden Ticket attack, the threat actor leverages the Kerberos authentication protocol vulnerability and uses tools like Mimikatz to gain access to any resource, including AD. Incidentally, this was also one of the key techniques used by the attackers during the November 2020 Sunburst attack. **Watch this video** to see how Falcon Identity Protection detects and mitigates this attack.



Forged PAC Alert

An unsuccessful attempt to use the forged pac vulnerability (MS14-068) was detected from ETIS-WS04 using SCCM Admin, against: ETIS-DC01.

Suspicious Protocol Implementation

Brian White credentials were used in an unusual manner on ETIS-WS04. Usage is consistent with mimikatz Pass The Hash module.

Brian White credentials were used to access NTLM service on SLV-PATENT-FILE from ETIS-WS04

Suspicious Ticket Reuse

Brian White's login ticket, generated on BWHITE_WS (owned by Brian White), was reused on ETIS-WS04. Activity is consistent with Pass the Ticket attack.

Ticket of Brian White was used on ETIS-WS04 to access ETIS-FILESHARE01

The pass-the-hash (PhH) attack has been in vogue since 1997 and still is one of the techniques used by attackers to capture password hashes and use them to authenticate to other endpoints or servers using the already vulnerable NTLM protocol. Falcon Identity Protection detects and stops Golden Ticket, Silver Ticket, PtH, Forged PAC, and related techniques and tactics used to compromise your AD security posture.

STOP KERBEROASTING

Kerberoasting is an attack technique, documented in **MITRE ATT&CK® TTPs**, where the primary goal is to crack weak service account passwords. These compromised accounts are used for lateral movement, privilege escalation and persistence. In a typical Kerberoasting attack, the threat actor scans for accounts with service principal names (SPNs) and requests Kerberos tickets for any service, using a variety of tools such as the built-in PowerShell and external tools like JohnTheRipper and Hashcat. Kerberoasting is hard to detect and is usually mitigated by increasing password complexity and by limiting the privileges of service accounts. Falcon Identity Protection detects and alerts on accounts with compromised passwords and poorly protected SPNs that are vulnerable to Kerberoasting attacks so you can create policies around such accounts to either challenge them with MFA or block when trying to access critical applications or resources.

DETECT AND STOP LATERAL MOVEMENT

After compromising user identities, attackers try to escalate user privileges or look for other users with admin privileges. The attackers then move laterally across the network, compromising endpoints and servers until they find the crown jewel database to exfiltrate or, as in most **ransomware** attacks, encrypt. CrowdStrike Identity Protection detects and stops lateral movement threats in real time.

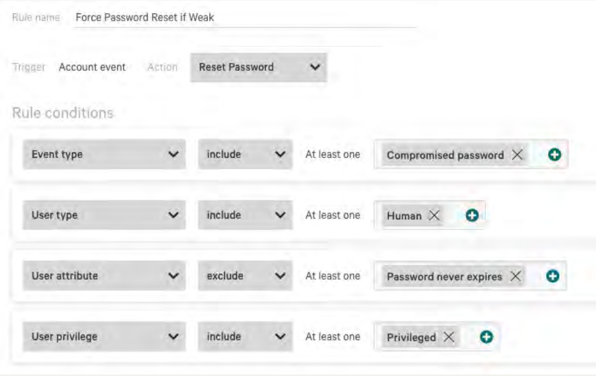
The above are just a few of the many identity-related threats that Falcon Identity Protection can detect and stop, without using time-consuming log processes, analysis, storage and management.

ENABLE FRICTIONLESS CONDITIONAL ACCESS WITH SIMPLE RULES

Falcon Identity Protection provides continuous visibility into AD and Azure AD identities. The automated risk assessments empower your security and AD teams to clearly visualize the identity attack surface and detect modern attacks such as ransomware and supply chain threats. When these modern threats are detected, your teams can leverage Falcon Identity Protection's **risk-based conditional access** to stop the attacks in real time. For example, to take preventative action on accounts that are part of an AD attack, simply create a policy that puts any account that is part of a Golden Ticket attack into a watchlist, and a second policy that blocks access or triggers MFA when these accounts try to access a resource. While these actions are audited, the security team investigates if these accounts have been compromised.

Frictionless conditional access means dynamically authenticating identities through strict policies that are enforced only when the risk increases or thresholds (baselines) are passed. This ensures a consistent login experience (and productivity) for genuine users while at the same time challenging risky users (including service accounts). Also, this approach reduces the number of incidents by auto-resolving authentication incidents — challenging users when an anomaly is detected — thereby making security frictionless for security operations center (SOC) teams.

Another advantage for AD teams is reducing the number of password reset requests and failed logins, as this approach reduces MFA fatigue. Conditional access rules are simple and in natural language, and kick in in real time to allow, stop, audit, reset password or step-up authentication by triggering MFA.



Rule name Force Password Reset if Weak

Trigger Account event Action Reset Password

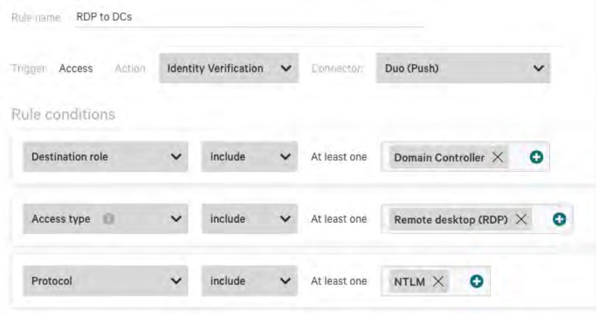
Rule conditions

Event type	include	At least one	Compromised password
User type	include	At least one	Human
User attribute	exclude	At least one	Password never expires
User privilege	include	At least one	Privileged

The rules can be based on a variety of parameters — like protocol used (NTLM, LDAP, Kerberos), behavior baselines, individual user risk score and device risk score (source and destination risk score) — to verify identities using MFA.

EXTEND MFA TO INCREASE SECURITY COVERAGE

Conditional access policies and risk-based MFA are not limited to only modern and cloud-based applications and resources. With Falcon Identity Protection, you can extend identity verification to any resource or application that cannot usually be integrated with the MFA solution deployed.



Rule name: RDP to DCs

Trigger: Access Action: Identity Verification Connector: Duo (Push)

Rule conditions

Destination role	include	At least one	Domain Controller
Access type	include	At least one	Remote desktop (RDP)
Protocol	include	At least one	NTLM

You can also extend MFA to legacy and proprietary applications and systems — tools like PowerShell and protocols like RDP over NTLM.

NEXT STEPS: SECURE YOUR ACTIVE DIRECTORY FROM MODERN ATTACKS

Organizations that want to secure AD/Azure AD and want rapid incident visibility and response into identity-related threats should consider running a proof of concept (POC) right away. Even if you are in the middle of a breach or scrambling to identify the gaps because one of your contractors or suppliers has been breached, Falcon Identity Protection takes only a few hours — not days — to install the lightweight Falcon agents and give you holistic visibility of your identity threat landscape.

After the installation, you will see:

- Continuous and unified visibility of your AD/Azure AD threat landscape
- Continuous assessment of identities to answer the “who, when, why and where” and identity segmentation to limit the attack surface
- Real-time identity protection with risk-based identity verification (risk-based MFA), even for legacy systems and tools
- Enforcement of frictionless policies based on user behavior and risk, devices used, applications accessed and many other signals — all tied to context to improve alert fidelity and response

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.

Request a Demo

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