Technical Validation

Reduce Risk with CrowdStrike Falcon Identity Protection

By Jack Poller, Senior Analyst

July 2021

This ESG Technical Validation was commissioned by CrowdStrike and is distributed under license from ESG.

Contents

Introduction 3
Background 3
CrowdStrike Falcon Identity Protection 4
ESG Technical Validation 5
Immediate Analysis of Active Directory Identities 5
Threat Detection 8
Threat Prevention 12
The Bigger Truth 16

ESG Technical Validations

The goal of ESG Technical Validations is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Technical Validations are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team's expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.

Introduction

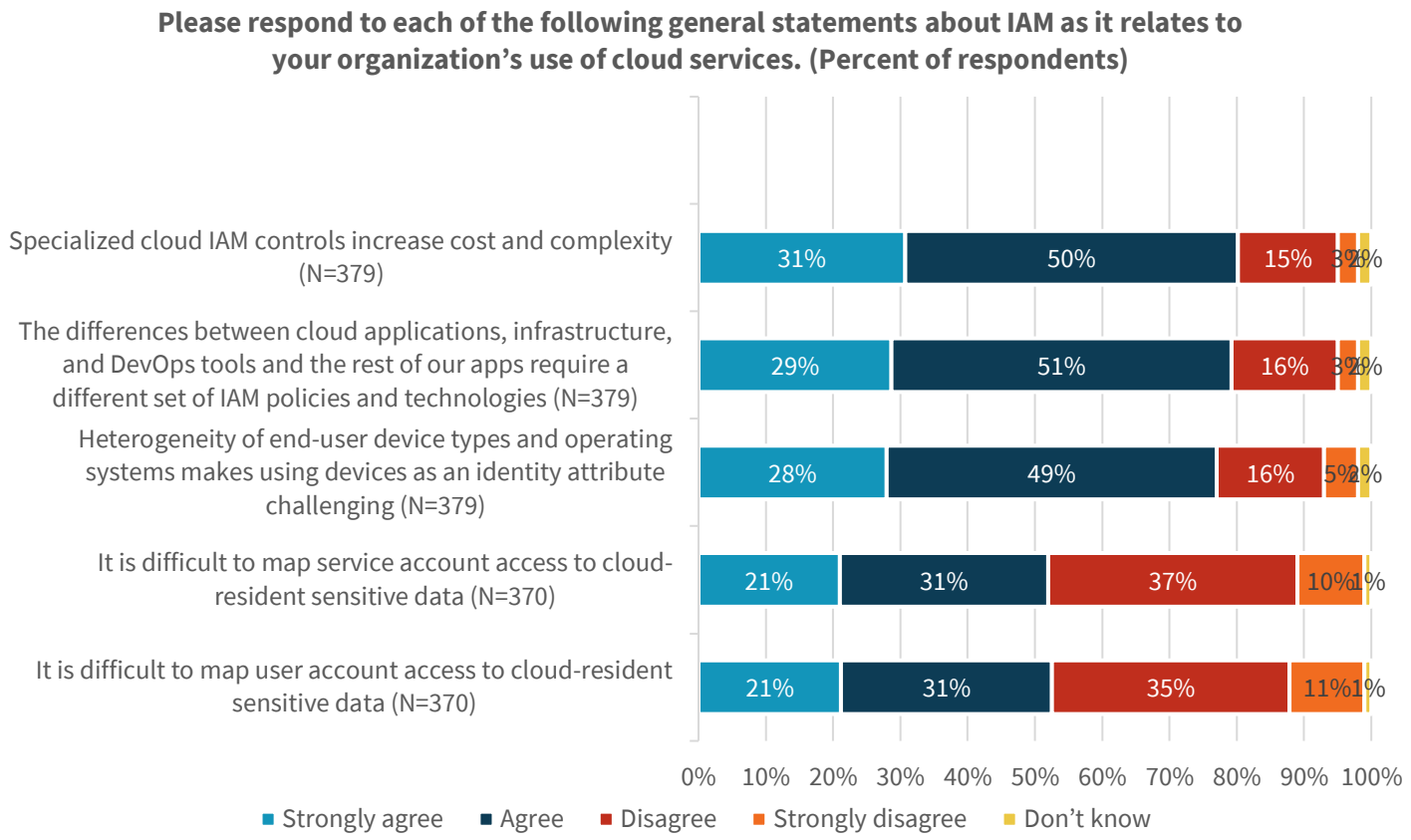
This ESG Validation Report documents how CrowdStrike Falcon Identity Protection provides zero trust security for workforce identities that's easy to deploy and use. It also discusses how Falcon Identity Protection uses automated and real-time analysis to reduce the attack surface and security costs.

Background

Increased network traffic, the proliferation of connected devices, the growth in users working from multiple locations, and the increasing sophistication of malicious actors all contribute to making network security more difficult. Indeed, according to ESG research, 85% of organizations agree that network security is more difficult than it was two years ago.[1]

The issues impacting network security contribute to the challenges organizations face in securing their user identities. Specialized cloud identity and access management (IAM) controls increase cost and complexity while cloud apps, modern on-premises infrastructures, and DevOps tools require different IAM policies and technologies (see Figure 1).[2]

Figure 1. Cloud and Device Heterogeneity Drives Identity Complexity



Source: Enterprise Strategy Group

Organizations need controls that can rapidly reduce the attack surface and improve the probability they will continue operating during and after attacks. This is why 83% of organizations will increase their investment in network security controls over the next 12-18 months.[3]

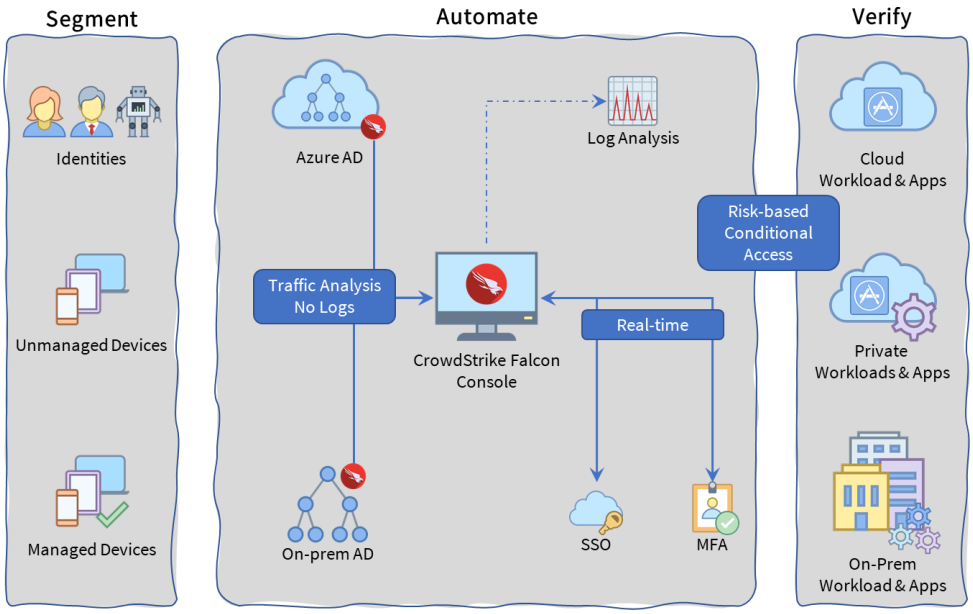
[1] Source: ESG Master Survey Results, *Network Security Trends,* March 2020.
[2] Source: ESG Master Survey Results, *Trends in IAM: Cloud-driven Identities*, December 2020.
[3] Source: ESG Master Survey Results, *Network Security Trends,* March 2020.

CrowdStrike Falcon Identity Protection

CrowdStrike designed Falcon Identity Protection to provide frictionless zero-trust security, real-time threat prevention, and TI policy enforcement using identity, behavioral, and risk analytics. Falcon Identity Protection increases security and reduces the attack surface by segmenting workforce identities.

Falcon Identity Protection is easy and quick to deploy because the architecture is simple (see Figure 2). The main architectural components are the management console and domain controller (DC) sensors (represented by the CrowdStrike icon), which are installed on the on-premises and/or cloud domain controllers. The DC sensors monitor and control traffic, ensuring trust through enabling positive identity authentication.

Figure 2. CrowdStrike Falcon Identity Protection



Source: Enterprise Strategy Group

Falcon Identity Protection has visibility into all identities and network traffic. This enables Falcon Identity Protection to gather more information and react faster than is possible by reviewing logs. Falcon Identity Protection can correlate events, compute identity risk scores, and apply dynamic policies such as geographic or risk-based multi-factor authentication (MFA).

The benefits of deploying CrowdStrike Falcon Identity Protection include:

- Workforce identity visibility—Falcon Identity Protection provides administrators with unified visibility and control of identities across multi-directory environments. Administrators gain visibility and control of user access with actionable insights into user behavior and risks, reducing the attack surface.
- Acceleration of threat detection and response—active monitoring and control of network communication reduces mean time to detect (MTTD) and mean time to respond (MTTR) to incidents, while reducing false positives and concomitant alert fatigue.
- Zero-trust security—Falcon Identity Protection enables administrators to develop and enforce consistent dynamic risk-based policies for every identity. Organizations can provide a frictionless login experience for genuine users while increasing security by automatically blocking, auditing, or increasing authentication efforts for high-risk identities or situations.

ESG Technical Validation

ESG validated the capabilities of CrowdStrike Falcon Identity Protection through a series of demonstration sessions. Validation was designed to demonstrate the immediate value customers get within hours of installing Falcon Identity Protection. Threat detection and threat prevention were also examined.

Immediate Analysis of Active Directory Identities

ESG started with a pre-installed demo environment containing both on-premises and cloud Active Directories. During installation, Falcon Identity Protection deploys DC sensors, which use WinDivert drivers to sniff and control traffic. The WinDivert driver can hold or pause traffic while the system waits for a positive response to an authentication challenge.

After product installation, Falcon Identity Protection crawls the Active Directories and pulls identity information into the management console for analysis. Falcon designed the system to provide insights about security risks in the environment in just a few hours, with a full analysis typically completing in a day.

We used the demo environment to understand the types of insights admins can get immediately after the service account starts monitoring the domains, including:

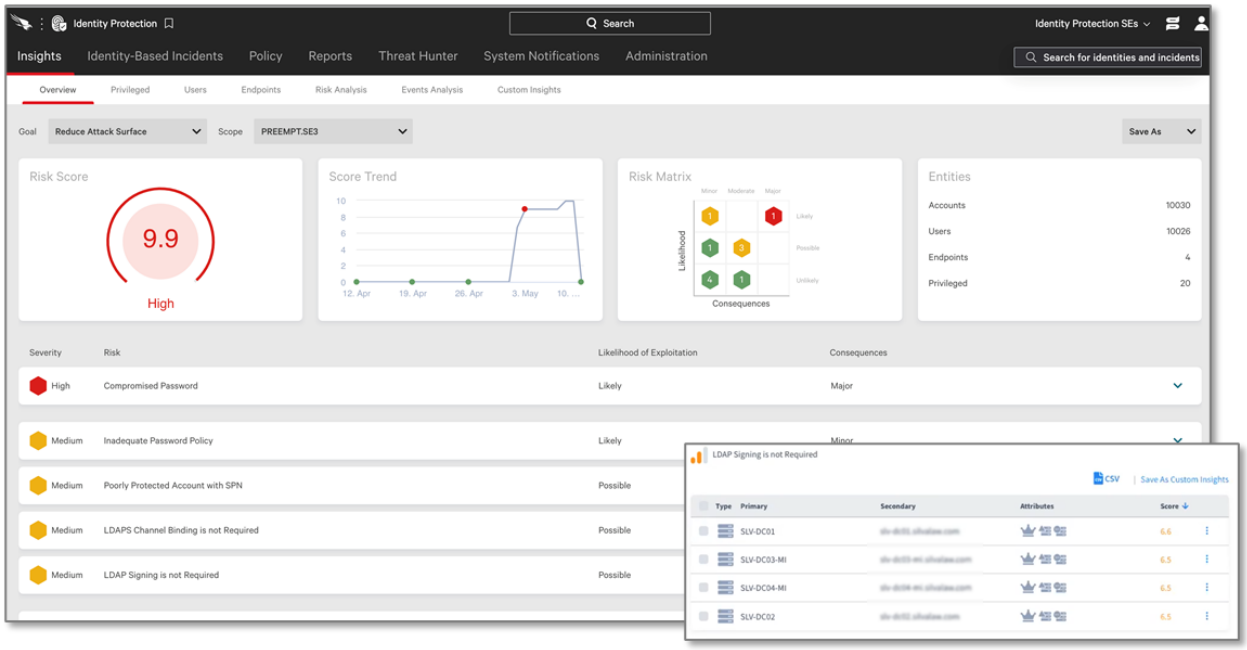
- An overview of domain-based risks and vulnerabilities.
- A risk assessment for privileged users.
- Group membership for specific users.

Falcon Identity Protection can monitor multiple domains at once, even if the domain isn't trusted. This is particularly useful for large enterprises with multiple domains as well as mergers and acquisition activity.

First, we reviewed the insights overview, which provides at-a-glance summary information about domain-based risks, as shown in Figure 3. The top of the overview graphically displays risk information, including the overall risk score and risk trends, and a risk matrix mapping the likelihood of exploitation of issue against the consequences. This helps administrators triage and prioritize risk mitigation and reduction activities. Below the risk information is a prioritized list of issues showing the likelihood of exploitation and the consequences.

All the elements of the insights overview are live links, and clicking on an element drills down to provide more information. We clicked on the ***LDAP Signing is not Required*** risk and then on ***Show related entities*** to show which systems are vulnerable to that specific risk. This enabled us to quickly determine the extent of the issue and helped us prioritize remediation efforts.

Figure 3. Insights Overview



Source: Enterprise Strategy Group

Next, we clicked the ***Privileged*** tab to see insights about all privileged users (Figure 4). Falcon Identity Protection shows administrative privileges with a crown icon and has expanded the traditional definition of privileged users to include multiple categories of users such as:

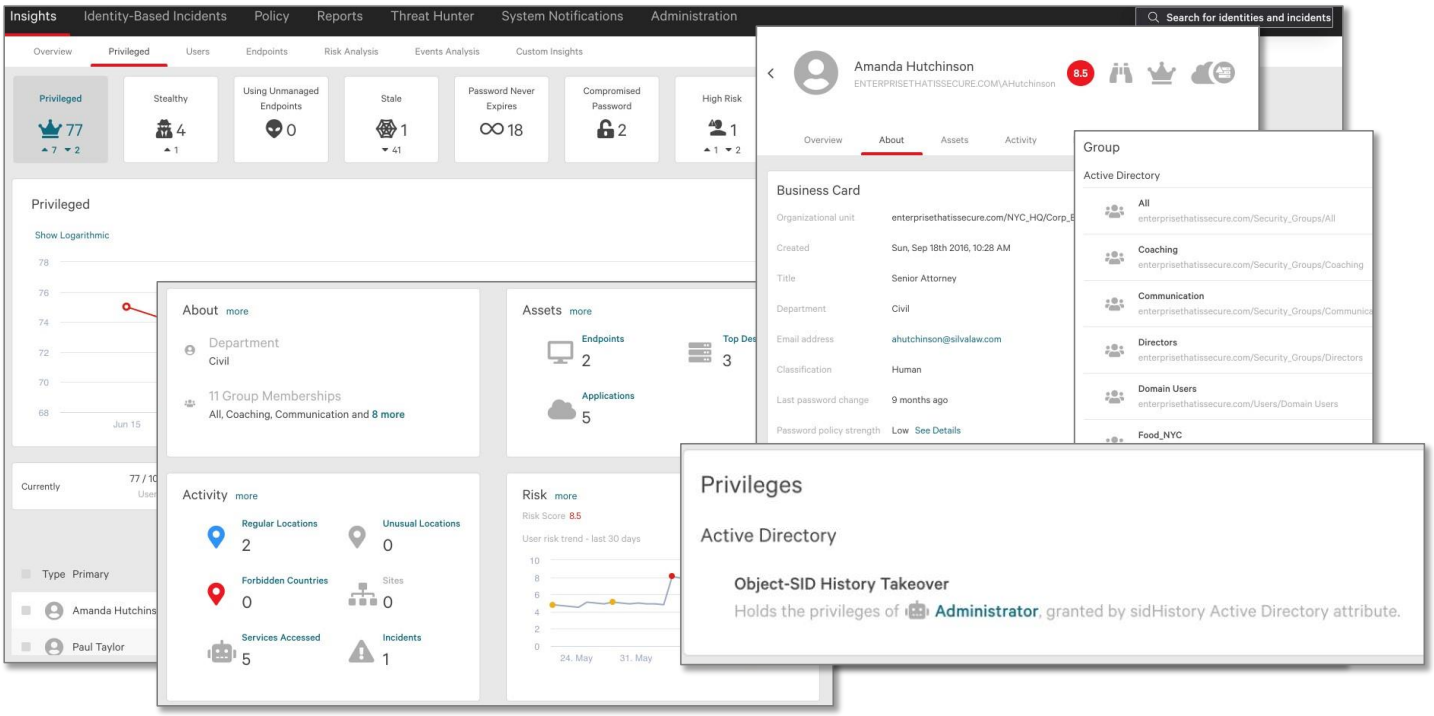
- Traditional domain administrators.
- Azure AD tenant administrators.
- Users who have local administrative rights to a large number of systems.
- Users with "stealthy" privileges who aren't domain admins but have specific administrative privileges that can be exploited by malicious actors.

We selected Amanda Hutchinson in the list of privileged users and then clicked more to expand the pane and see her complete profile, including group memberships. Even though Amanda is not a member of any administrative group, Falcon Identity Protection analyzed all rights and identified Amanda as a stealthy privileged user because she was given explicit administrative permissions under a different object SID.

Falcon Identity Protection's analysis and identification of administrative accounts helps administrators quickly audit their environment and ensure compliance with policies and regulations. Thus, organizations can apply the security principle of least-privileged access—ensuring that users are given the minimum amount of access necessary to do their jobs—and reduce the number of administrative accounts and privileged users, minimizing potential points of attack and compromise.

Next, we selected ***Domain Users*** from the list of groups that Amanda is a member of to expand the list of all members of the group. We then clicked on the group name to see the group overview, which included a list of nested groups. This gives admins visibility and control of privileges inherited from otherwise invisible groups.

Figure 4. Privileged Users Insights



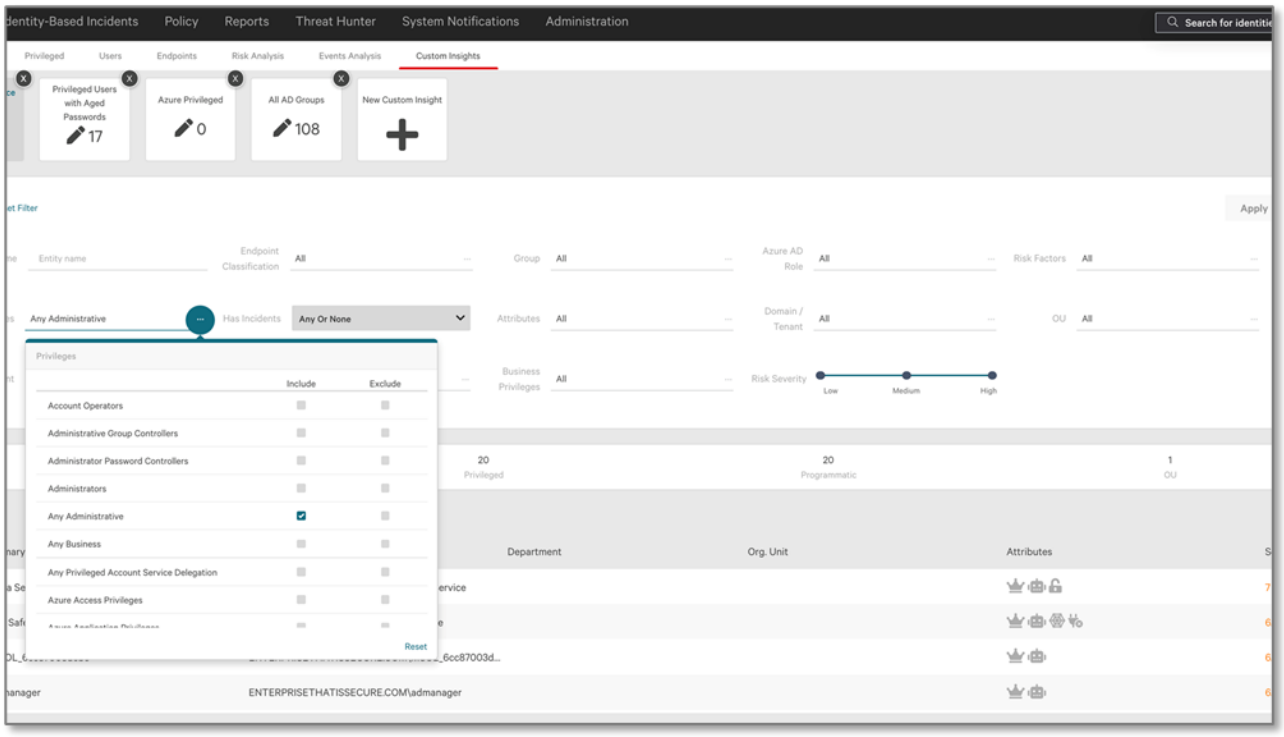
Source: Enterprise Strategy Group

When Falcon Identity Protection analyzes account attributes in Active Directory, it uses various account parameters such as whether the user has a phone number to differentiate between human user accounts and machine or service accounts. Analytics and traffic pattern monitoring based on data obtained from the DC sensors helps refine the determination of the account type. For example, if traffic patterns show a predictable and consistent stream of one activity immediately after another, the account is probably a programmatic user and thus a service account. If traffic is erratic or less predictable, it's probably a human user.

We selected the ***Custom Insights*** tab and created a custom filter for service accounts, as shown in Figure 5. We clicked on the filter icon at the top right to show filter options and selected accounts with any administrative privileges. We noted that we could also filter by domain, OU, department, group, and other identity parameters. We could also include or exclude those attributes. For example, we could exclude a particular domain or department from the filter.

These types of custom insights enabled us to identify potential avenues of attack and reduce risk by reducing privileges or disabling unused privileged service accounts.

Figure 5. Custom Insights



Source: Enterprise Strategy Group

Why This Matters

Understanding user privileges is critical, especially when applying the security principle of least-privileged access to reduce the attack surface and organizational risk. Active Directory, through nested groups, custom privileges for each user and entity, and other techniques, obfuscates privileges, making it extremely difficult for admins to identify overprivileged or misprivileged users.

ESG validated that shortly after installation, Falcon Identity Protection had analyzed the AD and provided actionable insights about domain-based risks and vulnerabilities as well as user and group privileges. Using these insights, we identified users with stealthy privileges—users without admin credentials but with explicit privileged rights. We also created custom insights to identify unused service accounts with admin credentials. These insights enabled us to ensure users were granted only the access they needed, reducing organizational risk.

Threat Detection

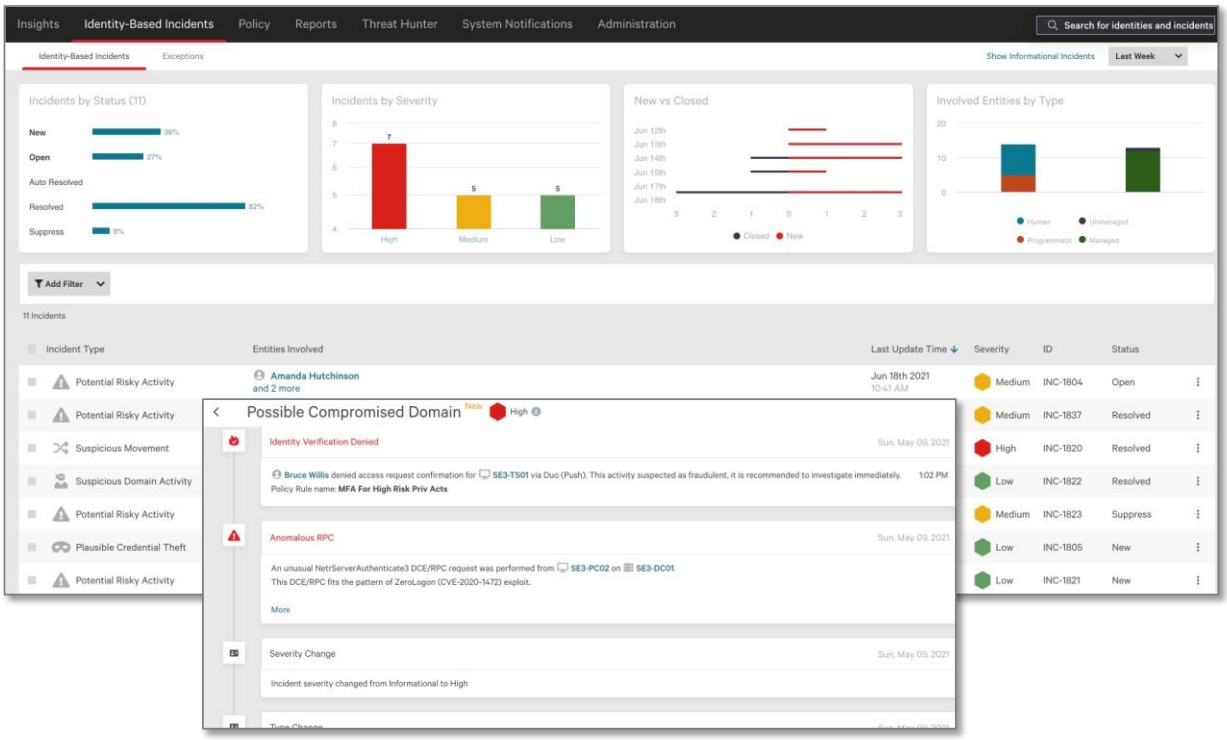
CrowdStrike Falcon Identity Protection captures and analyzes user behavior and network traffic for indicators of attacks (IOA) and indicators of compromise (IOC). Multiple related events are correlated and aggregated into a single actionable incident, which reduces the number of alarms and helps admins identify root causes for remediation.

First, ESG reviewed the incident dashboard, as shown in Figure 6. The dashboard provides an at-a-glance summary of incidents, including statistics on incidents by status and by severity and the different types of entities involved (human or

programmatic, managed or unmanaged). The dashboard also displays a list of incidents, which identifies the incident type, involved entities, time, severity, and status.

We selected a ***Possible Compromised Domain*** incident to drill down for more information, and Falcon Identity Protection displayed details, including the aggregated and correlated events in the incident. In this case, the system detected an anomalous RPC that fit the pattern of the ZeroLogon exploit. Following the policy, the system requested multi-factor authentication, and the user denied the MFA request. Thus, Falcon Identity Protection created the possible compromised domain alert from these events.

Figure 6. Incident Dashboard

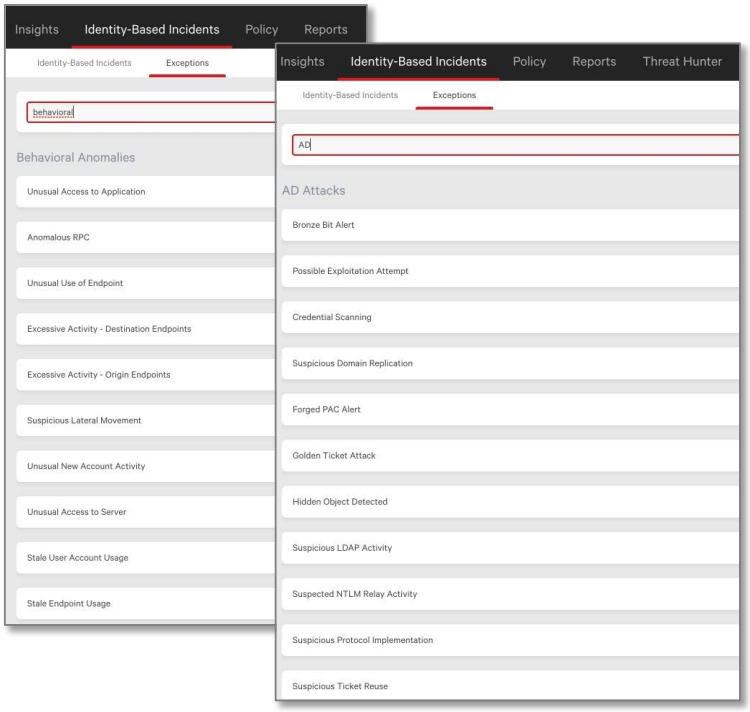


Source: Enterprise Strategy Group

Falcon Identity Protection automatically identifies an extensive set of IOA/IOC that appear as behavioral and geographical anomalies and various attacks against AD, including DC Sync attacks, Golden Ticket attacks, Kerberos attacks, NTML Relay attacks, and many others. Most of these attacks are hard to detect through log analysis; Falcon Identity Protection can detect these attacks because it monitors network traffic and user behavior.

Next, we selected the Exceptions tab view, which displays custom exceptions that can help admins to exclude known activities and prevent those activities from triggering incidents, as shown in Figure 7. False positives are a huge burden on businesses because they can take up a lot of an admin's time. For example, a vulnerability scanner might trigger an alert for multiple login attempts, but the scanner's activity is not a real threat. Admins can create incident exceptions to make sure they get alerts only for actual threats.

Figure 7. Incident Exceptions

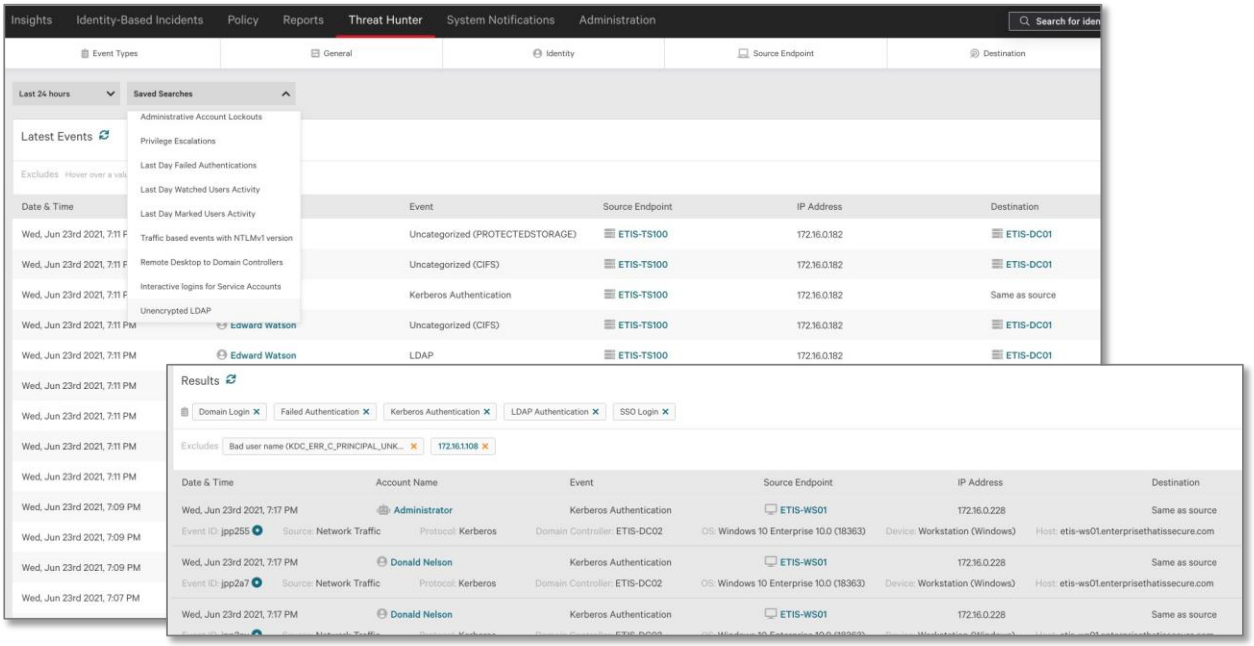


Source: Enterprise Strategy Group

Next, we selected ***Threat Hunter,*** which enabled us to search the event log, as shown in Figure 8. Using built-in searches, we searched for unencrypted LDAP events to find users and systems that are using insecure unencrypted authentication methods. Once identified, we could increase security and reduce risk by reconfiguring systems and policies to permit only encrypted authentication. We prioritized our activity by further filtering the list to show only privileged users, as these represent the highest risk to the organization.

A CrowdStrike Falcon Identity Protection customer using Threat Hunter discovered that their self-service password reset service account was using unencrypted LDAP and passwords were transmitted in clear text.

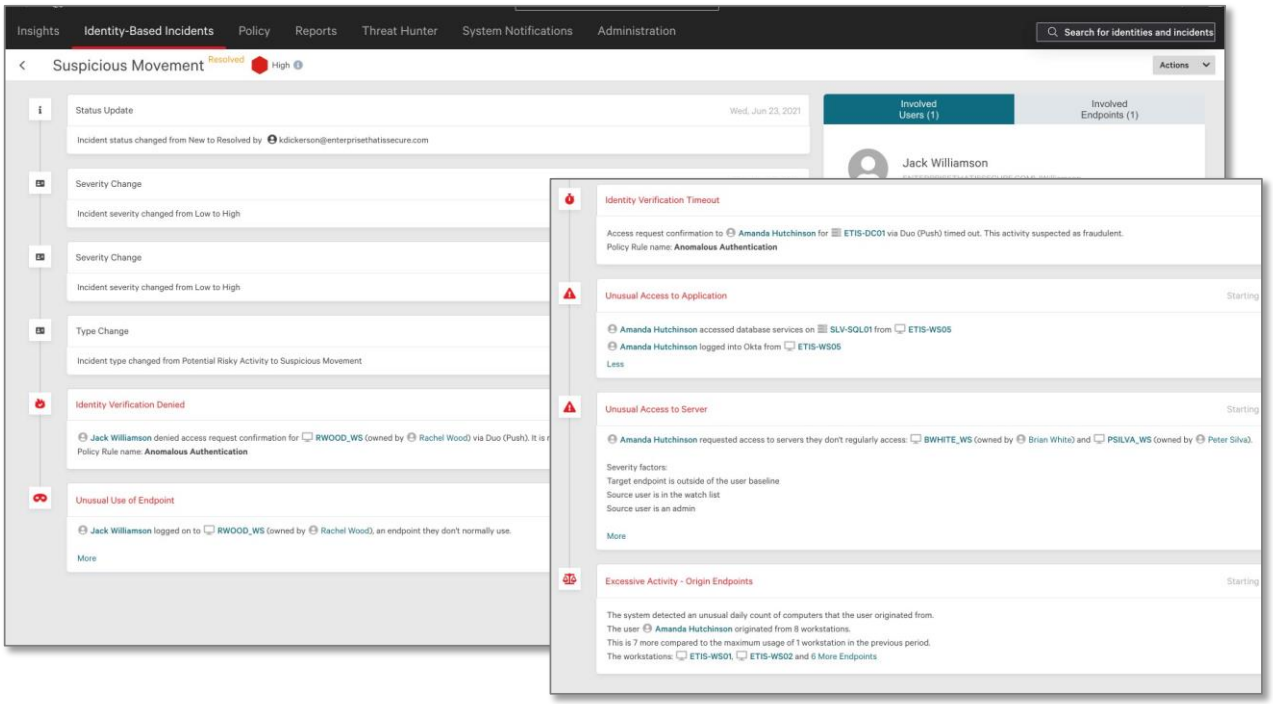
Figure 8. Threat Hunter



Source: Enterprise Strategy Group

Finally, we looked at how events are correlated and aggregated into incidents. We selected a ***Suspicious Movement*** incident and reviewed the timeline of events included in this incident, as shown in Figure 9. The events included excessive activity, where the system detected an unusual daily account of computers the user originated from; unusual access to server, where the user requested access to servers they don't regularly access; unusual access to application; and identity verification timeout.

Figure 9. Event Correlation and Aggregation into Incidents



Why This Matters

Malicious actors are becoming more sophisticated and are crafting more devious, evasive, targeted attacks that exploit identities for access. Simultaneously, IT isn't getting easier—according to ESG research, three-quarters (75%) say IT has become more complex in the last two years.[4] Organizations are searching for security controls that provide multiple methods of threat detection and prevention to increase security effectiveness and operational efficiency.

ESG validated that CrowdStrike Falcon Identity Protection captured and analyzed user activity and network traffic to identify IOA and IOC. Multiple events were correlated and aggregated into incidents, reducing the number of alerts and concomitant alert fatigue. We found that using the threat hunting environment was intuitive, requiring no training. Searching and filtering was quick, and incident records contained relevant information, enabling us to identify and remediate root causes of attacks.

Threat Prevention

CrowdStrike Falcon Identity Protection includes the ability to create policies for user segmentation, conditional access, and other activities that help admins prevent threats and activities such as lateral movement. Policies can be based on identity characteristics and on dynamic risk analysis from real-time activities using information gathered by the DC sensors.

Falcon Identity Protection builds a baseline of each user's activity including the systems they regularly access, and this baseline is used in developing the user's risk score. Other factors include geographic location, time of day, and more. Anomalous behavior dynamically changes the risk score. For example, a user that typically uses three to four systems suddenly connecting to 25 systems might be an indication of lateral movement of malware, and the Falcon Identity Protection may raise that user's risk level.

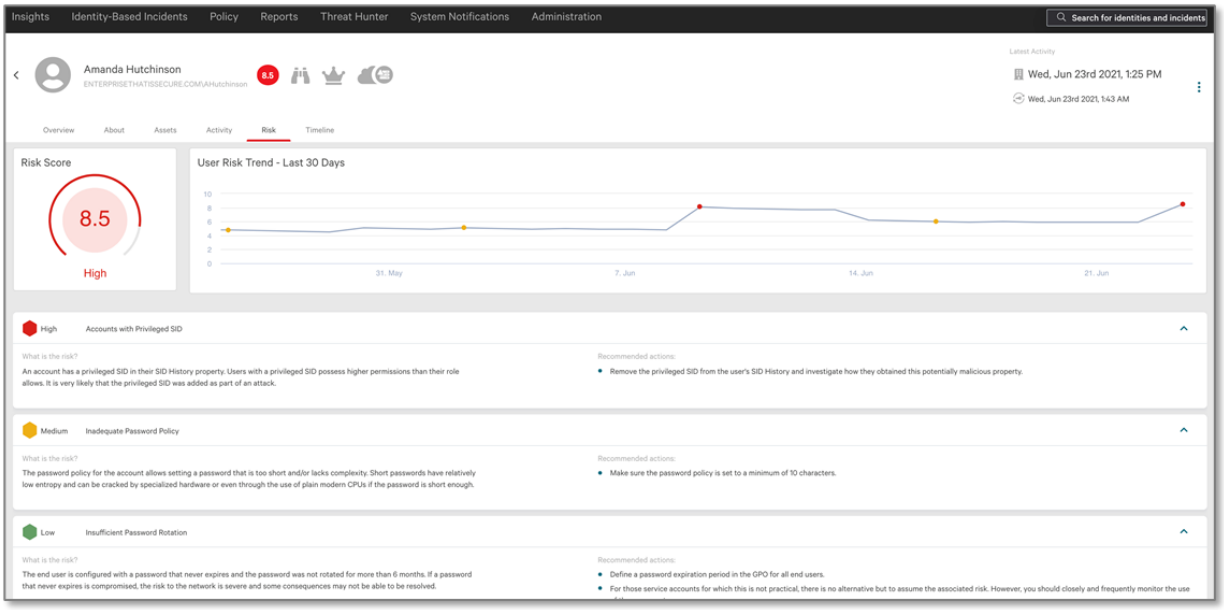
Using this behavioral analysis enables Falcon Identity Protection to detect and prevent ransomware attacks. Ransomware and other malware often start with credential scanning and credential stuffing to compromise a weakly protected identity. Other malware targets the DC directly with pass the hash, NTLM relay, and other protocol-related attacks. These techniques appear as anomalous behavior, and administrators can configure Falcon Identity Protection policies to trigger MFA or block these attacks.

ESG reviewed the risk score and profile of Amanda Hutchinson, a high-risk user, as shown in Figure 10. The risk tab showed the users their historical risk trend; hovering over a dot on the graph listed the risks that contributed to the risk score on that date. Clicking on a risk expanded the description of the risk.

Risk scores range from 0-10 and change dynamically. Amanda's high-risk score (8.5) was based on a combination of her attributes, such as accounts with privileged SID, and her activity that includes excessive activity, unusual access to a service, and identity verification timeout.

[4] Source: ESG Research Report, *2021 Technology Spending Intentions Survey*, January 2021.

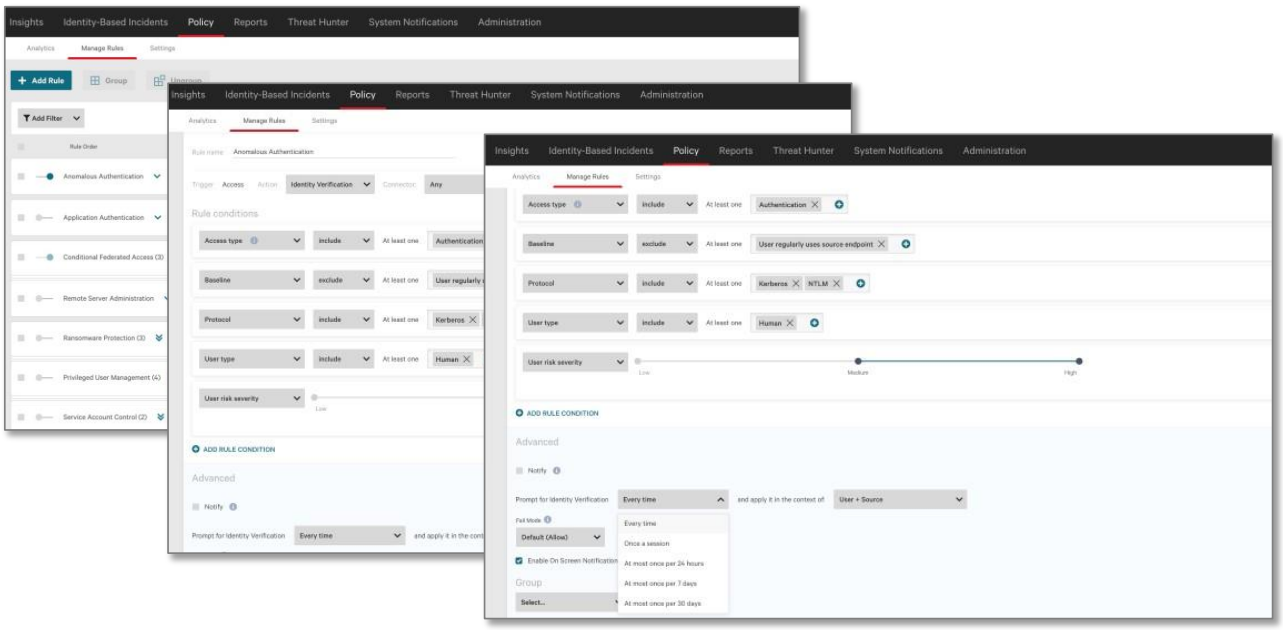
Figure 10. User Risk Score



Source: Enterprise Strategy Group

Next, ESG selected the ***Policy – Manage Rules*** tab, which displayed the ordered list of policies, as shown in Figure 11. We then defined a new policy to limit lateral movement using MFA. Falcon Identity Protection provides an easy-to-understand policy editor, and we specified when the policy was triggered and a series of rule conditions that required MFA when a human user is required to authenticate to a system they don't regularly use. We also specified that authentication required Kerberos or NTLM protocols. To avoid MFA fatigue, we selected to prompt for identity verification at most once every seven days. If the user establishes a pattern of regularly using this system, it becomes a trusted system and the user no longer gets an MFA request. We also created a policy requiring MFA at most once every 24 hours for high-risk human users.

Figure 11. Policies – Manage Rules

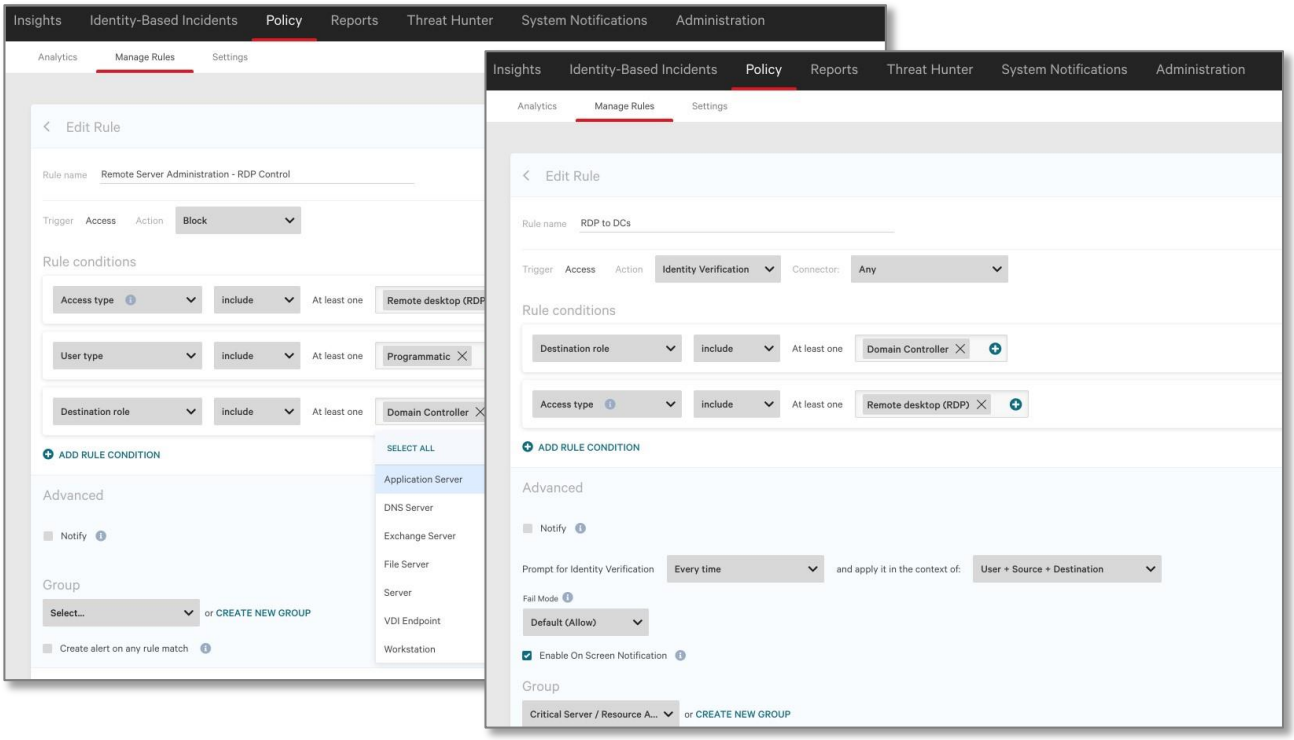


Source: Enterprise Strategy Group

Next, we created a policy to block remote desktop (RDP) access for programmatic users and service accounts (see Figure 12). We added a condition to exclude a specific service account that might need RDP access, and we could have customized further by destination and source attributes, user-based attributes, and date and time.

We then created a service account segmentation policy to allow access only from specific vCenter servers. Because a vCenter service account should only be used for vCenter servers, we blocked access from the vCenter service account unless the source is coming from one of three specified vCenter servers. This policy segments the service account and makes sure it can authenticate only to specific vCenter servers.

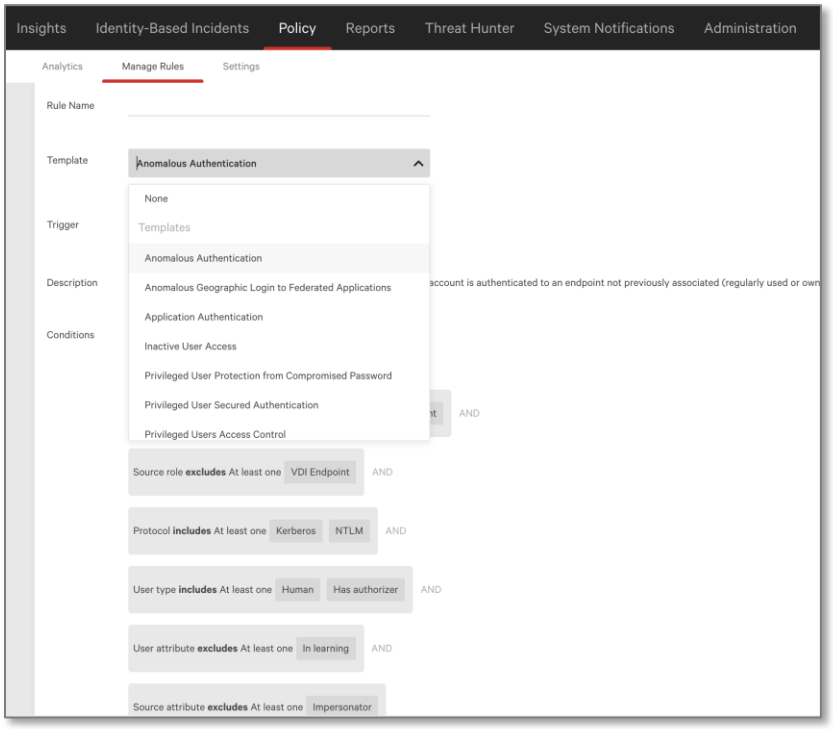
Figure 12. Policy to Prevent Service Accounts from Using RDP



Source: Enterprise Strategy Group

Next, we reviewed the policy templates that come with Falcon Identity Protection (Figure 13). Admins can use the templates as a starting point and then tailor policies to their specific circumstances.

Figure 13. Policy Templates



Source: Enterprise Strategy Group

Why This Matters

Consistent application of policies across the organization helps prevent threats and attacks. However, the need to have both on-premises and cloud identities, the increase in remote users driving access to a diverse range of applications, and the sharing of data with external third parties hamper consistency and provide significant IAM challenges.

ESG validated that admins can use CrowdStrike Falcon Identity Protection to quickly and easily create complex dynamic policies to prevent threats. Policies can incorporate a dynamic risk score that incorporates both identity characteristics and dynamic behaviors. Thus, admins can create policies that require MFA for anomalous behavior such as the first login to a new system, require MFA for high-risk users, or block remote desktop protocol access for programmatic users and service accounts. Options such as requiring MFA only once per seven days reduce user friction, and these types of polices help prevent threats by increasing security for risky operations.

The Bigger Truth

Many cybersecurity teams spend the majority of their efforts addressing high-priority issues and emergencies, often neglecting both long-term strategic initiatives and short-term tactical actions to reduce their attack surface.

ESG's validation shows CrowdStrike Falcon Identity Protection to be efficient and effective, providing immediate value with Active Directory and Azure AD identity analyses that rapidly identified identity issues such as high-risk and over- and misprivileged accounts. With direct access to both identity activity and network traffic, Falcon Identity Protection was able to detect identity-related threats that would otherwise be impossible to find with log-based analyses. We found developing policies was quick and easy, and policies could leverage dynamic risk scoring. This enabled us to prevent threats by requiring MFA for risky users or activities.

Falcon Identity Protection enabled us to tackle tactical issues quickly and easily such as identifying stealthy admins and reducing overprivileged accounts. We could also rapidly tackle strategic issues such as implementing the principle of least-privileged access.

The results presented in this document are based on evaluation in a controlled environment. Due to the many variables in each organization's infrastructure, it is important to perform planning and testing in your own environment to validate the viability and efficacy of any solution.

If your organization's objective is to gain more complete visibility into identities, effectively reduce identity-based risk, and increase operational efficiency, it would be smart to take a close look at CrowdStrike Falcon Identity Protection.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

 www.esg-global.com

 contact@esg-global.com

 508.482.0188