

HOW CROWDSTRIKE ALIGNS WITH THE **AUSTRALIAN CYBER SECURITY CENTRE** (ACSC)

Essential Eight Maturity Model


Introduction

The Australian Cyber Security Centre (ACSC) has developed prioritised mitigation strategies, in the form of the Strategies to Mitigate Cyber Security Incidents, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies is the Essential Eight.

The Essential Eight has been designed to protect Microsoft Windows-based internet-connected networks. While the principles behind the Essential Eight may be applied to cloud services and enterprise mobility, or to other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments. In such cases, the CrowdStrike controls listed in this document also apply beyond Windows environments.

The Essential Eight Maturity Model, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on the ACSC's experience in producing cyber threat intelligence, responding to cybersecurity incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.





This document shows how CrowdStrike and **CrowdStrike Store** partners align to Maturity Level Two of the **Essential Eight Assessment Process Guide** for each of the eight mitigation strategies. As organisations progress through the Maturity levels, the capabilities described in this document may also be applicable in addressing the Control Description Test IDs. For more information on how you can configure CrowdStrike Falcon® in line with the Test Methodology, please engage your Account Team who can provide a step-by-step process.

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. | Learn more: <https://www.crowdstrike.com.au/>

Follow us: [Blog](#) | [Twitter](#)

© 2023 CrowdStrike, Inc. All rights reserved.

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

CrowdStrike Store Partners



Application Control

01

ML2-AC-01 - (Workstations & Internet-facing servers) A dedicated application control solution is implemented.

ML2-AC-02 - (Workstations & Internet-facing servers) The system is only able to execute approved executables.

ML2-AC-03 - (Workstations & Internet-facing servers) The system is only able to execute approved software libraries.

ML2-AC-04 - (Workstations & Internet-facing servers) The system is only able to execute approved scripts.

ML2-AC-05 - (Workstations & Internet-facing servers) The system is only able to execute approved installers.

ML2-AC-06 - (Workstations & Internet-facing servers) The system is only able to execute approved compiled HTML files.

ML2-AC-07 - (Workstations & Internet-facing servers) The system is only able to execute approved HTML applications.

ML2-AC-08 - (Workstations & Internet-facing servers) The system is only able to execute approved control panel applets.

ML2-AC-09 - (Workstations & Internet-facing servers) The system is logging the application control product when it allows and blocks execution.

The rise of fileless attacks, which are carried out entirely in memory, is making it hard for traditional security solutions to detect them. In 2022, 71% of all attacks were malware-free.¹

The method of protection against fileless attacks through application control lists all trusted processes to block unknown ones from executing. However, fileless attacks exploit vulnerabilities in legitimate, allowlisted apps or use OS executables, making it impossible to block essential apps for both users and the OS.

XSL script processing is described in the MITRE ATT&CK® framework under ID **T1220**. Attackers may bypass application control and achieve execution of code by embedding scripts within XSL files. These files contain code that performs formatting on XML files, which means that it can be a way to run code supplied by an attacker. Due to its legitimate functionality, attackers can use XSL to bypass application allowlisting and execute arbitrary code.

Wmic.exe is a command-line utility that comes pre-installed on all versions of Windows and is used to access Windows Management Instrumentation (WMI). An attacker can use the Wmic.exe to invoke the code from an XML file. According to MITRE's ID **T1220**, an attacker can also use WMI to perform code execution by using the /FORMAT switch. It's also worth noting that Wmic.exe is capable of running code from local or remote XSL files.


As you can see, fileless techniques are extremely challenging to detect if you rely on signature-based methods, sandboxing, application control or even machine learning protection methods.

Developed by cybersecurity practitioners, **Airlock Digital** addresses the technical and organisational challenges typically associated with allowlisting. Airlock delivers purpose-built workflows that enable rapid and scalable deployment while significantly reducing staffing resources required for day-to-day management. Airlock also provides rich file visibility across the organisation, by collecting and building a centralised database of files seen within the environment. This data can be interrogated at any time and is further enhanced by CrowdStrike Falcon endpoint detection and response (EDR) telemetry.



[CROWDSTRIKE STORE DEMO](#)

1. Source: [CrowdStrike 2023 Global Threat Report](#)

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	CrowdStrike Store Partners
 <p data-bbox="73 649 266 735">Application Control</p>		<p data-bbox="730 217 1315 368">CrowdStrike uses a unique approach to application control as part of its endpoint protection solution. This approach combines multiple methods such as machine learning, custom rules, memory protection and file integrity monitoring. By using these complementary methods, CrowdStrike provides a powerful and integrated approach that delivers unrivaled endpoint protection against fileless attacks and other cyber threats:</p> <ul data-bbox="730 396 1315 1182" style="list-style-type: none"> <li data-bbox="730 396 1315 554">▪ CrowdStrike Falcon® Prevent (NGAV): CrowdStrike combines human and machine intelligence to uncover new threats and enable high-fidelity detections. Machine learning is implemented across the process lifecycle in the CrowdStrike Falcon platform. In this demonstration we dive into how machine learning is used and how it can benefit your organisation's security. DEMO <li data-bbox="730 582 1315 739">▪ CrowdStrike Falcon Prevent (Custom Rules): Customers can leverage custom indicators of attack (IOAs) to add their own customised rules to audit or protect against the testing methodology for this mitigation strategy. Used alongside global CrowdStrike preventions, these organisational indicators have unlimited potential to help organisations identify events defined by specific applications and behaviors. DEMO <li data-bbox="730 768 1315 896">▪ CrowdStrike Falcon Prevent (Memory Protection): Because malware-free or fileless attacks can be carried out entirely in memory, detection can be challenging. But with new cutting-edge Advanced Memory Scanning capabilities, organisations can quickly automate high-performance scanning to detect the most advanced attacks. DEMO <li data-bbox="730 925 1315 1025">▪ CrowdStrike Falcon® Insight XDR (Scheduled Searches): Falcon Insight XDR can be used to automate queries, send notifications and download event data as evidence to support the testing methodology. DEMO <li data-bbox="730 1053 1315 1182">▪ CrowdStrike Falcon® FileVantage: CrowdStrike's file integrity monitoring solution streamlines your security operations. It provides real-time insight for file, folder and registry changes, while offering valuable contextual data around detections, adding further evidence and visibility. DEMO 	

01

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

Technology Partners

ML2-PA-01 - A vulnerability scanner is run and reviewed at least weekly to scan the organisation's office productivity suites, web browsers, email clients, PDF software and security products.

ML2-PA-02 - A vulnerability scanner is run and reviewed at least fortnightly to scan the organisation's other applications.

ML2-PA-03 - The organisation has an effective process for patching office productivity suites, web browsers, email clients, PDF software and security products within two weeks.

ML2-PA-04 - Office productivity suites, web browsers, email clients, PDF software and security products do not have security vulnerabilities older than two weeks.

ML2-PA-05 - Other applications that have a vulnerability are patched or mitigated within one month.

Microsoft's Patch Tuesday is dreaded by every security team. With dozens of new patches inundating your team every month, how do you know which to prioritise? How do you know if you have visibility or risk across applications?

SecOps staff for both government agencies and organisations are often pressed for time. With the plethora of critical and highly scored vulnerabilities for applications, a common issue arises where not all highly scored vulnerabilities are addressed in a timely manner. This leaves organisations with gaps or flaws within their systems that threat actors use to exploit organisations for nefarious gain.

Historically, SecOps has relied on vendors to provide some prioritisation information around this large body of vulnerabilities — but that is no longer enough. With the limited amount of time typically allocated for patching and updating systems, critical vulnerabilities are not being remediated — a situation that can be potentially very damaging.

CrowdStrike combines the power of its world-class machine learning and unparalleled intelligence to arm every customer with the insight they need to prioritise patches and take action across workloads and applications within your ecosystem.

CrowdStrike Falcon® Spotlight offers organisations continuous and real-time assessment of vulnerability exposure on their endpoints. Falcon Spotlight's native integration into the Falcon platform enables customers to operationalise vulnerability assessment within a complete endpoint protection framework. Falcon Spotlight adds preparation and readiness to the unparalleled prevention, detection and response provided by the Falcon platform, resulting in a stronger security posture.

Falcon Spotlight: [DEMO](#)

Falcon Spotlight (Automate Workflows): [DEMO](#)

CrowdStrike's adversary-focused approach to its **cloud-native application protection platform** (CNAPP) provides both agent-based and agentless solutions delivered from the Falcon platform to extend vulnerability assessment to DevOps. CrowdStrike enhances your vulnerability management program by focusing on integrating security into the CI/CD pipeline.

Customers can build automated workflows using CrowdStrike Falcon® Fusion integrated security orchestration automation and response (SOAR) to trigger incident ticket creation in ServiceNow IT Service Management (ITSM). Security and DevSecOps teams can leverage detections and incidents from the Falcon platform to help streamline incident management and accelerate response capabilities. You can also orchestrate remediation of vulnerabilities by creating ServiceNow tickets directly from Falcon Spotlight, and easily configure the workflow to attach auto-generated reports, enabling you to track the remediation progress of your security team to improve efficiency and monitoring.

This ServiceNow ITSM plugin leverages Falcon Fusion to allow you to receive Falcon-generated alerts via ServiceNow ITSM.



[CROWDSTRIKE STORE](#)

Build automated workflows using Falcon Fusion to trigger issue creation in Jira. Security and DevSecOps teams can leverage detections and incidents from the Falcon platform to help streamline incident management and accelerate response capabilities. You can also orchestrate remediation of vulnerabilities by creating Jira issues directly from Falcon Spotlight, enabling you to track the remediation progress of your security team to improve efficiency and monitoring.



[CROWDSTRIKE STORE](#)



Patch Applications

02

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

Technology Partners



Patch Applications

02

As part of the functionality of [CrowdStrike Falcon® Cloud Security](#), customers have the ability to create verified image policies to ensure that only approved images are allowed to progress through the CI/CD pipeline and run in their hosts or Kubernetes clusters.

- Falcon CNAPP: [DEMO](#)

[CrowdStrike Falcon Fusion](#) is the extensible response framework built on the CrowdStrike Falcon platform that enables the security orchestration, automation and response (SOAR) of complex workflows. These workflows can be used to simplify tasks, accelerate response and save valuable time for security teams when handling incidents and, in this case, vulnerabilities workflows. Falcon Fusion is included in the Falcon platform and available to all customers.

- Falcon Fusion: [DEMO](#)
- Falcon Plugins and Add-Ons: [CROWDSTRIKE STORE](#)

Why just focus on the inside out? Resilient cybersecurity posture can only be achieved with a full understanding of your internal and external attack surface. As the attack surface expands, so does the “community” of adversaries and cybercriminals exploiting externally exposed assets to break into organisations around the globe. Gartner identified attack surface expansion as the number one trend in its most recent Top Security and Risk Management Trends for 2022,² turning external attack surface management (EASM) into a critical tool in the cybersecurity arsenal.

[CrowdStrike Falcon® Surface](#) provides a uniquely differentiated EASM offering, delivering an adversary-driven EASM capability that minimises risk from unknown, externally exposed assets. With Falcon Surface, security teams can close security gaps by employing an outside-in view of the enterprise attack surface. This empowers teams to prioritise and manage all exposed internet-facing assets that are centralised or remote across on-premises environments, subsidiary, cloud and third-party vendors — all with a zero-touch approach.

2. Gartner Press Release, [Gartner Identifies Top Security and Risk Management Trends for 2022](#), March 7, 2022. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

JumpCloud empowers your security operations, IT and DevOps teams to secure and manage your devices, all from a single platform. By integrating with the CrowdStrike Falcon platform's Real Time Response (RTR) commands to deploy the JumpCloud agent, you can easily secure, update and manage the host's operating system. With group-based patching and policies, you can quickly gain visibility and close security gaps.






[CROWDSTRIKE STORE](#)

Kenna.VM integrates with Falcon Spotlight to allow security teams to focus their limited resources on remediating the vulnerabilities that matter the most. Kenna layers CrowdStrike's rich endpoint data with robust threat and vulnerability intel and advanced data science to identify and prioritise the vulnerabilities that pose a real risk to the organisation. With Kenna.VM and CrowdStrike data, security teams are able to get a clearer accurate picture of risk within their environment, along with the actionable insight to make effective and efficient remediation decisions.



[CROWDSTRIKE STORE](#)

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	Technology Partners
 <p>Patch Applications</p>		<p>Falcon Surface automatically prioritises risks by leveraging CrowdStrike's adversary intelligence to guide precise actions based on the most critical risks, including natively integrating context of industry-specific risks, CVE scores for vulnerabilities on exposed assets, geolocation, attack history and asset type.</p> <ul style="list-style-type: none"> ▪ Falcon Surface (EASM): DEMO 	<p>Improve security posture with NopSec Unified VRM® as it continually ingests Falcon Spotlight vulnerabilities and enriches the data with aggregated threat intelligence and context from over 30 different sources to prioritise and accelerate vulnerability remediation. Unified VRM consolidates and prioritises risks, putting an end to vulnerability fatigue. Integration with industry-standard ticketing and patching systems dramatically reduces the time necessary to fix critical vulnerabilities.</p>  <p>CROWDSTRIKE STORE</p> <hr/> <p>Vulcan Cyber gives you the tools to effectively manage the vulnerability and risk lifecycle for your cyber assets, including application, cloud and infrastructure. By integrating with your tools, including the Falcon platform, you can better analyse and prioritise your vulnerability and risk data to orchestrate remediation. Playbooks automate communication and collaboration between teams responsible for mitigation and execute remediation actions when appropriate.</p>  <p>CROWDSTRIKE STORE</p>

02

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

Technology Partners

ML2-OM-01 - Microsoft Office macros in Microsoft Office files are unable to make Win32 API calls.

ML2-OM-02 - Allowed execution of a Microsoft Office macro within a Microsoft Office file is logged.

ML2-OM-03 - Blocked execution of a Microsoft Office macro within a Microsoft Office file is logged..

While adversaries continue to innovate their tactics to remain under the radar, tried-and-true techniques such as phishing remain popular among targeted and eCrime operators alike. In the [CrowdStrike 2022 Falcon OverWatch Threat Hunting Report](#), CrowdStrike Intelligence assessed that adversaries began making the shift to using other methods in response to Microsoft's announcement that it would begin disabling internet-enabled macros in Office documents by default.

Script-based threats such as BokBot and other fileless attacks are on the rise because they can avoid detection from traditional file-inspection-based detection capabilities by leveraging trusted applications that are part of the operating system, and also productivity applications like Office, to interpret and execute malicious script content.

[Falcon Prevent](#) customers are protected from script-based attacks using the Falcon platform's Script-Based Execution Monitoring feature. The Script Control feature implements a set of components that provides expanded visibility into a scripting language.

ScriptControl provides AMSI-based and AMSI-emulation-based introspection of the PowerShell engine. ScriptControl allows the Falcon sensor to block malicious operations that attempt to hide by translating high-level operations into multiple lower-level requests, such as:

- Contents of executed script files
- Typed strings on a PowerShell prompt
- Dynamically executed strings through the Invoke-Expression cmdlet
- Commands supplied as a command-line parameter, such as -EncodedCommand

This enables the prevention of malicious VBA macros in Microsoft Office products as well as malicious VBScript, JScript and Excel 4.0 macros.

- Falcon Prevent (Script Control): [BLOG](#)

Mimecast and CrowdStrike protect organisations at both the secure email gateway and on endpoint devices. Joint customers can enhance threat protection through the integration of these industry-leading platforms. The integration shares intelligence derived from malware detected at the Mimecast Secure Email Gateway with the CrowdStrike Falcon platform.



[CROWDSTRIKE STORE](#)

Proofpoint and CrowdStrike have partnered to transform your security program and protect your organisation from the ever-changing threat landscape. Together, they improve your security efficacy and enhance your visibility and context around threats. The orchestration and response capabilities make your security team more productive.



[CROWDSTRIKE STORE](#)



Configure
Microsoft
Office
Settings

03

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

Technology Partners



User Application Hardening

ML2-AH-01 - Microsoft Office files cannot create child processes

ML2-AH-02 - Microsoft Office files cannot create executable content.

ML2-AH-03 - Microsoft Office files cannot inject code into other processes.

ML2-AH-04 - Microsoft Office files do not execute OLE packages.

ML2-AH-05 - Microsoft Office security settings are unable to be modified by a standard user account.

ML2-AH-06 - PDF software cannot create child processes.

ML2-AH-07 - PDF software security settings are unable to be modified by a standard user account.

ML2-AH-08 - The Microsoft guidance for hardening Microsoft Edge is implemented.

ML2-AH-09 - The Google guidance for hardening Google Chrome is implemented.

ML2-AH-10 - The ACSC guidance for hardening Microsoft Office is implemented. OR The Microsoft guidance for hardening Microsoft Office is implemented.

ML2-AH-11 - Vendor guidance for hardening PDF software is implemented.

ML2-AH-12 - PowerShell scripts that have been blocked are logged.

Rather than simply relying on static signatures and heuristics, security solutions need to do more to detect and protect against today's targeted attacks. They need to identify behaviors that indicate malicious activity. By identifying malicious or suspicious behaviors, security solutions can protect against attacks that have never been seen, including sophisticated fileless attacks.

And because each organisation has unique circumstances and environments to monitor and protect, tailored security can be needed for specific or very localised risks such as limiting use of infrequently used applications or detecting suspicious activity that isn't fundamentally malicious.

Falcon Prevent uses the detailed event data collected by the Falcon agent to develop baseline rules or indicators that identify and prevent attacks that would otherwise leverage bad behaviors. CrowdStrike tunes and expands those built-in indicators to offer immediate protection against the latest attacks.

In addition to the included global IOAs, customers can create custom IOA rules in the Falcon platform. Because advanced tactics can be narrowly directed, tailored rules (e.g., preventing Office from executing files) give customers the ability to create specific behavioral detections based on what they know about their environment, applications, specific tools and expected behaviors.

The **CrowdStrike Falcon® Zero Trust Assessment (ZTA)** expands Zero Trust beyond authentication to enable detection, alerting and enforcement of conditional access based on device health and compliance checks to mitigate risks. With expanded support for macOS and Linux, Falcon ZTA provides visibility into all endpoints running across all operating platforms in an organisation. Falcon ZTA monitors over 120 different unique endpoint settings, including sensor health, applied CrowdStrike policies and native operating system (OS) security settings; these settings are a few of those recommended by the guidelines set forth by Microsoft and the Center for Internet Security. Customers also receive actionable reports on findings via the Falcon console and APIs to ensure that the highest degree of device security is enforced.

Falcon Insight (ZTA): [DEMO](#)

Falcon Insight (ZTA Integrations): [BLOG](#)

Developed by cybersecurity practitioners, Airlock Digital addresses the technical and organisational challenges typically associated with allowlisting. Airlock delivers purpose-built workflows that enable rapid and scalable deployment while significantly reducing staffing resources required for day-to-day management. Airlock also provides rich file visibility across the organisation, by collecting and building a centralised database of files seen within the environment. This data can be interrogated at any time and is further enhanced by CrowdStrike Falcon EDR telemetry.



[CROWDSTRIKE STORE DEMO](#)

Talon Cyber Security secures SaaS and web-based applications with TalonWork, its Secure Enterprise Browser. By integration with CrowdStrike Falcon® Intelligence, you gain a hardened Chromium-based browser that provides deep visibility and control to defend against malware and prevent data loss from unmanaged endpoints. Seamlessly reduce cyber risk and simplify meeting audit and compliance requirements by easily verifying any endpoint's security posture before granting users access to corporate systems. With an intuitive cloud-based management console, it's easy for central administrators to configure TalonWork features, set policies, manage browser extensions, audit activities, demonstrate compliance, and detect, investigate and resolve security incidents.



[CROWDSTRIKE STORE](#)

04

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

Technology Partners



Restrict Administrative Privileges

ML2-RA-01 - A process for disabling known privileged accounts exists and is enforced. Users are made aware of this requirement when being provisioned with a privileged account.

ML2-RA-02 - There are no privileged accounts that have an Active Directory expiry date that is greater than 12 months or do not have an expiry date.

ML2-RA-03 - A process for disabling privileged accounts that have not been used for 45 days exists and is enforced by the entity. Evidence exists for the usage of the 45 days inactive disabling process, including support tickets or administrative logs that show accounts were disabled.

ML2-RA-04 - There are no enabled privileged accounts that have a lastlogondate that is greater than 45 days.

ML2-RA-05 - Where a privileged environment is virtualised, the virtualised image is not located in an unprivileged environment. This includes virtual machines on a standard unprivileged SOE.

ML2-RA-06 - Servers are configured to not allow remote access traffic or connections from systems that are not jump servers.

ML2-RA-07 - The Microsoft Local Administrator Password Solution (LAPS) or a similar solution is implemented on Windows workstations and servers.

ML2-RA-08 - Services account passwords are generated to be long, unique and unpredictable. Service account passwords are stored in a secure location, such as a password manager or a Privileged Access Management solution.

ML2-RA-09 - Passwords should be changed at least once every 12 months.

ML2-RA-10 - Successful and failed logins of privileged accounts are logged.

ML2-RA-11 - Changes made to privileged accounts and groups within Active Directory are logged.

Access brokers are threat actors who acquire access to organisations and provide or sell this access to other actors, including ransomware operators. As outlined in the [CrowdStrike 2023 Global Threat Report](#), the popularity of their services increased in 2022, with more than 2,500 advertisements for access identified — a 112% increase compared to 2021.

Why would an attacker hack into a system when they can simply use stolen credentials to masquerade as an approved user and log in to the target organisation?

Once inside, attackers increasingly target Microsoft Active Directory (AD) because it holds the proverbial keys to the kingdom, providing broad access to the systems, applications, resources and data that adversaries exploit in their attacks. When an attacker controls the keys, they can control the organisation.

The problem for security teams and CISOs is they often lack visibility into the risk presented by AD and identity threats. With thousands of identities and configurations to manage, understanding the level of risk and enforcing AD hygiene can be difficult. But because the ability to detect and stop identity-based attacks is critical to stopping breaches, understanding the risk that your AD creates is the best place to start.

[CrowdStrike Falcon® Identity Threat Detection](#) (ITD) represents the first level of detection for AD security. Falcon ITD provides visibility for identity-based attacks and anomalies, comparing live traffic against behavior baselines and rules to detect attacks and lateral movement. It provides real-time AD security alerts on rogue users and sideways credential movement within the network or cloud.

Combine best-in-class solutions for identity management and endpoint security to strengthen and simplify secure remote access for trusted users and devices. Okta and CrowdStrike have a deeply integrated joint solution that centralises visibility and supplies critical user and device context to access requests. You get the data-driven insights you need to support reliable, automated access decisions, so your teams can support remote team productivity while keeping the enterprise safe.





[CROWDSTRIKE STORE](#)

The CyberArk PAM as a Service solution leverages leading automation technologies to protect your business as it grows. The Conditional Access integration allows clients to leverage the Falcon ZTA risk score when determining what level of privileged access can be granted to a user. If the Falcon ZTA score exceeds a certain threshold, the user can be blocked or their access can be limited until the issues on the endpoint have been resolved.



[CROWDSTRIKE STORE](#)

05

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	Technology Partners
 <p data-bbox="73 661 311 793">Restrict Administrative Privileges</p> <p data-bbox="28 1120 270 1292">05</p>		<p data-bbox="875 247 1103 268">Falcon ITD enables you to:</p> <ul data-bbox="875 311 1431 636" style="list-style-type: none"> <li data-bbox="875 311 1431 361">■ See all organisational service accounts, privileged users and user credentials and attributes <li data-bbox="875 379 1431 429">■ Add the context of “who” to network attack discovery and investigation, with behavioral analysis for each credential <li data-bbox="875 448 1431 546">■ Track every authentication transaction, and alert when the risk is elevated (e.g., accessing new systems or being granted additional privileges), or if the traffic is abnormal (varies from normal patterns of the user behavior) <li data-bbox="875 565 1431 636">■ Expand understanding for both architecture and security teams by combining context of authentication-level events with recommended best practices for network security <p data-bbox="875 682 1431 753">Seeing user authentication activity everywhere, from local legacy apps to your cloud environment stack, is the first step toward effectively managing AD security for identity and access.</p> <p data-bbox="875 772 1431 925">CrowdStrike offers a complimentary Active Directory Risk Review to help security teams achieve visibility, understand risk and gain insights into the proactive steps that stop identity-based attacks before they happen. The risk review is powered by the CrowdStrike Falcon® Identity Threat Protection (ITP) module, native to the Falcon sensor.</p> <p data-bbox="875 943 1031 965">Falcon ITP: DEMO</p> <p data-bbox="875 983 1205 1005">Falcon ITP (Lateral Movement): DEMO</p> <p data-bbox="875 1023 1431 1282">Identity theft and overly permissive accounts are also major challenges faced by organisations in public and hybrid cloud environments. As demonstrated with the Sunburst attack, the adversary is looking to take advantage of the human error and misconfigurations that can be common with cloud deployments. Leveraging CrowdStrike’s wealth of cloud experience, CrowdStrike Falcon® Cloud Security provides cloud security posture management (CSPM) to help organisations identify those security issues and indicators of misconfiguration (IOMs) and IOAs.</p> <p data-bbox="875 1300 1354 1322">Falcon Cloud Security (Secure Identity Services): DEMO</p> <p data-bbox="875 1340 1195 1362">Falcon Cloud Security (CIEM): DEMO</p>	<p data-bbox="1483 247 1818 665">The AI-powered ForgeRock Identity Platform is both comprehensive and simple to use. It is the only platform that includes full-suite identity and access management (IAM) and identity governance and administration (IGA) capabilities; can be implemented across an organisation for all identities (workforce, consumers, things); and offers feature parity across all delivery options, including on-premises, any cloud environment, multi-cloud, hybrid and as a service. Choose the best authentication method for your users and applications based on endpoint intelligence from CrowdStrike.</p> <div data-bbox="1483 743 1644 825">  <p data-bbox="1483 796 1644 825">ForgeRock</p> </div> <p data-bbox="1483 896 1702 918">CROWDSTRIKE STORE</p>

Mitigation Strategy

Maturity Level Two Test Descriptions

ML2-PO-01 - A vulnerability scanner is run and reviewed at least weekly to scan the organisation's operating systems.

ML2-PO-02 - The organisation has an effective process for patching operating systems within two weeks.

ML2-PO-03 - Operating systems that have a vulnerability are patched or mitigated within two weeks.



Patch Operating Systems

06

CrowdStrike Alignment

Microsoft's Patch Tuesday is dreaded by every security team. With dozens of new patches inundating your team every month, how do you know which to prioritise? How do you know if you have visibility of every workload? And let's not forget that macOS and Linux carry their own vulnerabilities that need to be mitigated.

Driven by all of the new technologies being adopted and the move to the cloud, the number and types of assets an organisation has to manage increased nearly fourfold over the last 10 years.³ As a result, organisations are at risk to adversaries, who continually conduct reconnaissance to identify, target and exploit soft targets and vulnerabilities.

The proliferation of assets also creates an untenable situation for IT to minimise service disruption as asset configurations are changed and patches are applied. Gaining visibility and being able to manage both known and unknown assets are critical to maintaining proper security hygiene and a proactive security posture, but remain an unsolved challenge for nearly every organisation.

CrowdStrike Asset Graph dynamically monitors and tracks the complex interactions among assets, providing a single holistic view of the risks those assets pose, including vulnerabilities. CrowdStrike Asset Graph provides graph visualisations of the relationships among all assets such as devices, users, accounts, applications, cloud workloads and operations technology (OT), along with the rich context necessary for proper security hygiene and proactive security posture management to reduce risk in their organisations — without impacting IT.

Within CrowdStrike Asset Graph, a new relationship mapping tool provides a comprehensive visual map of how assets are connected to each other, including how many steps an internet-exposed device is from business-critical assets to trace and shutdown potential adversary paths before they can be used.

3. Source: <https://www.crowdstrike.com/blog/introducing-crowdstrike-asset-graph/>

Technology Partners

Customers can build automated workflows using Falcon Fusion to trigger incident ticket creation in ServiceNow ITSM. Security and DevSecOps teams can leverage detections and incidents from the Falcon platform to help streamline incident management and accelerate response capabilities. You can also orchestrate remediation of vulnerabilities by creating ServiceNow tickets directly from Falcon Spotlight, and easily configure the workflow to attach auto-generated reports, enabling you to track the remediation progress of your security team to improve efficiency and monitoring.



[CROWDSTRIKE STORE](#)

Build automated workflows using Falcon Fusion to trigger issue creation in Jira. Security and DevSecOps teams can leverage detections and incidents from the Falcon platform to help streamline incident management and accelerate response capabilities. You can also orchestrate remediation of vulnerabilities by creating Jira issues directly from Falcon Spotlight, enabling you to track the remediation progress of your security team to improve efficiency and monitoring.



[CROWDSTRIKE STORE](#)

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

Technology Partners



Patch Operating Systems

06

[CrowdStrike Falcon® Discover](#), the Falcon platform's IT hygiene module, is powered by CrowdStrike Asset Graph, feeding it information on assets where the Falcon agent is deployed. CrowdStrike Asset Graph can then provide high-level information about all assets in your environment such as operating systems, manufacturer and model, and whether the asset is managed, unmanaged, or unsupported by the Falcon sensor or even out of support with Microsoft.

CrowdStrike Asset Graph Top Insights for an asset provides visibility into critical vulnerabilities, recommended remediations and last patch installed date to quickly prioritise patching efforts. A single-click pivot from the asset view takes you to Falcon Spotlight for a more comprehensive view of the vulnerabilities and options to expand the search to understand how broad the risk is.

[Falcon Spotlight](#), as highlighted in the Patch Applications mitigation strategy, offers organisations continuous and real-time assessment of vulnerability exposure on their workloads. Its native integration into the Falcon platform enables customers to operationalise vulnerability assessment within a complete endpoint protection framework. Falcon Spotlight coverage for operating systems also adds response actions delivered via emergency patching within the Falcon Spotlight dashboard or available via API:

- Falcon Spotlight: [DEMO](#)
- Falcon Spotlight (Automate Workflows): [DEMO](#)
- Falcon Spotlight (Emergency Patching): [DEMO](#)

JumpCloud empowers your security operations, IT, and DevOps teams to secure and manage your devices, all from a single platform. By integrating with the CrowdStrike Falcon platform's Real Time Response (RTR) commands to deploy the JumpCloud agent, you can easily secure, update, and manage the host's operating system. With group-based patching and policies, you can quickly gain visibility and close security gaps.






[CROWDSTRIKE STORE](#)

Kenna.VM integrates with Falcon Spotlight to allow security teams to focus their limited resources on remediating the vulnerabilities that matter the most. Kenna layers CrowdStrike's rich endpoint data with robust threat and vulnerability intel and advanced data science to identify and prioritise the vulnerabilities that pose a real risk to the organisation. With Kenna.VM and CrowdStrike data, security teams are able to get a clearer accurate picture of risk within their environment, along with the actionable insight to make effective and efficient remediation decisions.



[CROWDSTRIKE STORE](#)

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	Technology Partners
 <p data-bbox="73 661 247 793">Patch Operating Systems</p>		<p data-bbox="803 261 1329 439">Falcon Fusion is an extensible framework built on the Falcon platform that allows the orchestration and automation of complex workflows. These workflows can be used to simplify tasks, accelerate response and save valuable time for security teams when handling incidents, and in this case vulnerabilities workflows. Falcon Fusion is included in the Falcon platform and available to all customers.</p> <ul data-bbox="803 465 1174 534" style="list-style-type: none"> <li data-bbox="803 465 1174 486">▪ Falcon Fusion (Built-in Workflows): DEMO <li data-bbox="803 512 1174 534">▪ Falcon Plugins and Add-Ons: STORE 	<p data-bbox="1389 261 1812 544">Improve security posture with NopSec Unified VRM® as it continually ingests Falcon Spotlight vulnerabilities and enriches the data with aggregated threat intelligence and context from over 30 different sources to prioritise and accelerate vulnerability remediation. Unified VRM consolidates and prioritises risks, putting an end to vulnerability fatigue. Integration with industry-standard ticketing and patching systems dramatically reduces the time necessary to fix critical vulnerabilities.</p> <div data-bbox="1389 591 1485 684">  </div> <p data-bbox="1389 729 1605 751">CROWDSTRIKE STORE</p> <hr data-bbox="1389 779 1843 782"/> <p data-bbox="1389 805 1804 1062">Vulcan Cyber gives you the tools to effectively manage the vulnerability and risk lifecycle for your cyber assets, including application, cloud and infrastructure. By integrating with your tools, including the Falcon platform, you can better analyse and prioritise your vulnerability and risk data to orchestrate remediation. Playbooks automate communication and collaboration between teams responsible for mitigation and execute remediation actions when appropriate.</p> <div data-bbox="1389 1125 1474 1196">  </div> <p data-bbox="1389 1243 1605 1265">CROWDSTRIKE STORE</p>

06



Multi-Factor Authentication

07

Mitigation Strategy

Maturity Level Two Test Descriptions

ML2-MF-01 - A privileged user who is performing administrative activities is required to respond to an MFA challenge at some point in the authentication lifecycle. This can be implemented when authenticating to a machine (such as a jump server) or when attempting to raise privileges. The organisation has a list of systems that have privileged users or support privileged functions.

ML2-MF-02 - The organisation requires that internet-facing services use multi-factor authentication that uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

ML2-MF-03 - The organisation requires that privileged users utilise multi-factor authentication that uses either: something users have and something users know, or something users have that is unlocked by something users know or are.

ML2-MF-04 - The organisation's internet-facing systems log successful MFA attempts.

ML2-MF-05 - Administrative access connections log successful MFA attempts.

ML2-MF-06 - The organisation's internet-facing systems log unsuccessful MFA attempts.

ML2-MF-07 - Administrative access connections log unsuccessful MFA attempts.

CrowdStrike Alignment

Access brokers have become a key component of the eCrime threat landscape, selling access to threat actors and facilitating a myriad of criminal activities. Many access brokers have established relationships with [big game hunting](#) (BGH) ransomware operators and affiliates of prolific [ransomware-as-a-service](#) (RaaS) programs.

Many intrusion scenarios, as highlighted in the [CrowdStrike 2022 Falcon OverWatch Threat Hunting Report](#), feature the exploitation of remote access services and the use of RDP and some form of valid account.

Multifactor authentication (MFA) has become a crucial method for controlling access to critical applications and resources, and a key control in deterring threat actors who purchase compromised credentials from access brokers.

One way to enforce identity verification is to trigger MFA every time a user tries to access a resource or application. This can create MFA fatigue, which not only may reduce user productivity but also potentially creates a risk scenario in which the user inadvertently allows access to a malicious sign-in attempt.

Customers using [Falcon identity protection solutions](#) gain a better user experience and improved security with risk-based MFA: The user's trust is evaluated in real time to determine whether to allow access to specific resources even before the authentication request hits the AD. With baselines and dynamic risks tied to every identity and its behavior, malicious activity — such as lateral movement, risky behavior, unusual endpoint usage, privilege escalation and malicious RDP login attempts — is detected and challenged in real time without requiring cumbersome log analytics or point solutions.

Prioritising security controls in these areas, such as implementing MFA, would help in many cases. When it comes to hunting for precursors of ransomware activity, identifying lateral movement between critical assets such as domain controllers and backup servers is also crucial.

CrowdStrike Store Partners

Combine best-in-class solutions for identity management and endpoint security to strengthen and simplify secure remote access for trusted users and devices. Okta and CrowdStrike have a deeply integrated joint solution that centralises visibility and supplies critical user and device context to access requests. You get the data-driven insights you need to support reliable, automated access decisions, so your teams can support remote team productivity while keeping the enterprise safe.



CROWDSTRIKE STORE

Beyond Identity eliminates the vulnerabilities of passwords and the inconvenience of traditional MFA. It ensures high confidence in identity claims by cryptographically binding a user identity to their devices. The solution leverages X.509 certificates and the TLS protocol without any certificate management required by customers.

The integration of Beyond Identity's advanced, passwordless MFA with CrowdStrike's leading endpoint protection stops the two most prevalent sources of ransomware and account takeover attacks: passwords and compromised endpoints.

The integration provides a critical and foundational layer for Zero Trust, enabling an extremely high-trust method of authenticating users (employees, contractors, and consultants) and ensuring they are only able to gain access from endpoint devices that meet security policy requirements and those that are given a clean bill of health by Beyond Identity and CrowdStrike.



CROWDSTRIKE STORE

Mitigation Strategy

Maturity Level Two Test Descriptions

CrowdStrike Alignment

CrowdStrike Store Partners



Multi-Factor Authentication

07

[Falcon identity protection solutions](#) automatically classify and assess the privileges of all identities — think of it as next-generation privileged access security — with visibility and security control of all accounts tied to AD, Azure AD and SSOs like Okta, Ping and Active Directory Federation Services (ADFS). With identity segmentation and visibility into behavior and risks for all users, organisations can restrict access to high-value resources and stop ransomware attacks from progressing, thus allowing organisations to adopt a broader identity protection strategy.

The identity attack surface can also be influenced by a single non-privileged account, so you shouldn't narrow security efforts to only privileged accounts. It is important to understand that traditional privileged access management (PAM) solutions provide visibility into only privileged accounts. In addition to requiring careful planning to deploy and configure a PAM solution, organisations should consider the probability that jump servers can be bypassed and password vaults can be compromised.

Think of PAM as an “operational” solution to “manage” privileged accounts. For example, PAM solutions do not prevent the misuse of valid credentials, they only manage the use of privileged accounts — however, a privileged account from PAM could still be used by a skilled adversary to go undetected within a customer environment.

[Falcon identity protection solutions](#) can complement your PAM solution by enabling holistic visibility, analytics and protection for your privileged identities and service accounts, and enforcement of risk-based MFA — improving the user experience for your administrators.

- Falcon ITP (Zero Trust): [DEMO](#)

CrowdStrike Falcon® Intelligence Recon, CrowdStrike's digital risk protection solution, goes beyond the dark web to include forums with restricted access on the deep web, breach data and messaging apps — all resources commonly used by access brokers to trade or advertise. Falcon Intelligence Recon provides customers with an increased level of situational awareness and helps uncover potential malicious activity before eCrime adversaries have the chance to exploit it.


- Falcon Intelligence Recon: [DEMO](#)


TruU replaces hackable passwords with continuously validated identity that adapts to how people work so they can be protected and productive.

TruU and CrowdStrike take the Falcon ZTA score from the endpoint and combine that into the TruU risk score using the TruU Risk Engine. The TruU risk score is compared against the score indicated by the policy threshold and if the score is within the bounds, the user is logged into the computer with TruU presence alone. If the score is higher than the threshold then another factor is required for access.




[CROWDSTRIKE STORE](#)

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	CrowdStrike Store Partners
 <p data-bbox="73 662 224 746">Regular Backups</p> <p data-bbox="27 1119 274 1293">08</p>	<p data-bbox="340 212 678 304">ML2-RB-01 - Privileged users (excluding backup administrator accounts) are unable to access backups that do not belong to them.</p> <p data-bbox="340 329 678 396">ML2-RB-02 - Privileged users (excluding backup administrator accounts) are unable to modify and delete backups.</p>	<p data-bbox="726 212 1319 496">ECrime adversaries remain highly capable, particularly if measured by the speed at which they can move through a victim's environment. An important Falcon OverWatch speed measurement is breakout time: the time an adversary takes to move laterally, from an initially compromised host to another host within the victim environment. According to the CrowdStrike 2022 Falcon OverWatch Threat Hunting Report, of the hands-on eCrime intrusion activity observed between July 2021 and June 2022 where breakout time could be derived, the average was just 1 hour 24 minutes. Moreover, the Falcon OverWatch team found that in 30% of those eCrime intrusions, the adversary was able to move laterally to additional hosts in under 30 minutes.</p> <p data-bbox="726 522 1319 596">Without a data backup, companies are often at a complete loss when a ransomware attack occurs. Backups are normally the quickest and most reliable way to recover.</p> <p data-bbox="726 622 1319 775">The LockBit ransomware family has constantly been adding new capabilities, including tampering with Microsoft Server Volume Shadow Copy Service (VSS) and System Restore by interacting with the legitimate Windows tools. Capabilities such as lateral movement or destruction of shadow copies are some of the most effective and pervasive tactics ransomware uses.</p> <p data-bbox="726 801 1319 953">The tampering and deletion of VSS shadow copies is a common tactic to prevent data recovery. Adversaries will often abuse legitimate Microsoft administrator tools to disable and remove VSS shadow copies. Common tools include Windows Management Instrumentation (WMI), BCDEdit (a command-line tool for managing Boot Configuration Data) and vssadmin.exe.</p> <p data-bbox="726 979 1319 1029">LockBit 2.0 utilises the following WMI command line for deleting shadow copies and disabling system recovery:</p> <pre data-bbox="755 1058 1267 1182">C:\Windows\System32\cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no</pre> <p data-bbox="726 1208 1319 1336">The use of preinstalled operating system tools, such as WMI, is not new. Still, adversaries have started abusing them as part of the initial access tactic to perform tasks without requiring a malicious executable file to be run or written to the disk on the compromised system.</p>	

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	CrowdStrike Store Partners
 <p data-bbox="73 664 222 749">Regular Backups</p>		<p data-bbox="730 211 1315 339">Falcon Prevent takes a layered approach to detecting and preventing ransomware developed by eCrime actors, by using behavior-based IOAs and advanced machine learning, among other capabilities. CrowdStrike is committed to continually improving the efficacy of its technologies against known and unknown threats and adversaries.</p> <p data-bbox="730 364 1315 544">CrowdStrike's enhanced IOA detections accurately distinguish malicious behavior from benign, resulting in high-confidence detections. This is especially important when ransomware shares similar capabilities with legitimate software, like backup solutions. Both can enumerate directories and write files that on the surface may seem inconsequential, but when correlated with other indicators on the endpoint, can identify a legitimate attack.</p> <p data-bbox="730 571 1315 751">The Falcon platform offers protection against ransomware incidents, which is increasingly valuable as the popularity of ransomware continues to rise. CrowdStrike's approach is to stop ransomware from infecting a system and encrypting its files. CrowdStrike believes a prevention approach is absolutely necessary because decryption is often impossible and no organisation wants to pay the ransom, leaving often-cumbersome restoration from backups as a last resort.</p> <p data-bbox="730 778 1315 929">Falcon Prevent protects shadow copies from being tampered with, adding another protection layer to mitigate ransomware attacks. Protecting shadow copies helps potentially compromised systems restore encrypted data with much less time and effort. Ultimately, this helps reduce operational costs associated with person-hours spent spinning up encrypted systems post-compromise.</p> <p data-bbox="730 956 1315 1136">The Falcon platform can prevent suspicious processes from tampering with shadow copies and performing actions such as changing file size to render the backup useless. For instance, should a LockBit 2.0 ransomware infection occur and attempt to use the legitimate Microsoft administrator tool (vssadmin.exe) to manipulate shadow copies, Falcon immediately detects this behavior and prevents the ransomware from deleting or tampering with them.</p>	

08

Mitigation Strategy	Maturity Level Two Test Descriptions	CrowdStrike Alignment	CrowdStrike Store Partners
 <p data-bbox="73 662 227 748">Regular Backups</p>		<p data-bbox="730 211 1315 415">By combining the Falcon Fusion integrated SOAR solution with Falcon RTR, which provides surgical remote remediation capabilities, responders are able to automate post-remediation actions including: running checks on the system to ensure it is clean, running custom scripts and executables, issuing automated notifications via collaboration channels like email, Slack or Microsoft Teams, and updating ticket status on IT management systems like ServiceNow and Jira.</p> <ul data-bbox="730 444 1315 672" style="list-style-type: none"> <li data-bbox="730 444 1315 544">■ Falcon Prevent (Falcon RTR): Falcon RTR is a tool that can provide as many unique solutions as there are threats. Because response to a cybersecurity incident can be as unique as the attack itself, there is no “one-click-fixes-all” solution. DEMO <li data-bbox="730 572 1315 672">■ Falcon Fusion: Falcon Fusion integrates with Falcon RTR to provide powerful incident response and remediation across the entire Falcon platform via a simple drag-and-drop experience that works at scale across a multi-platform technology stack. DEMO 	

08