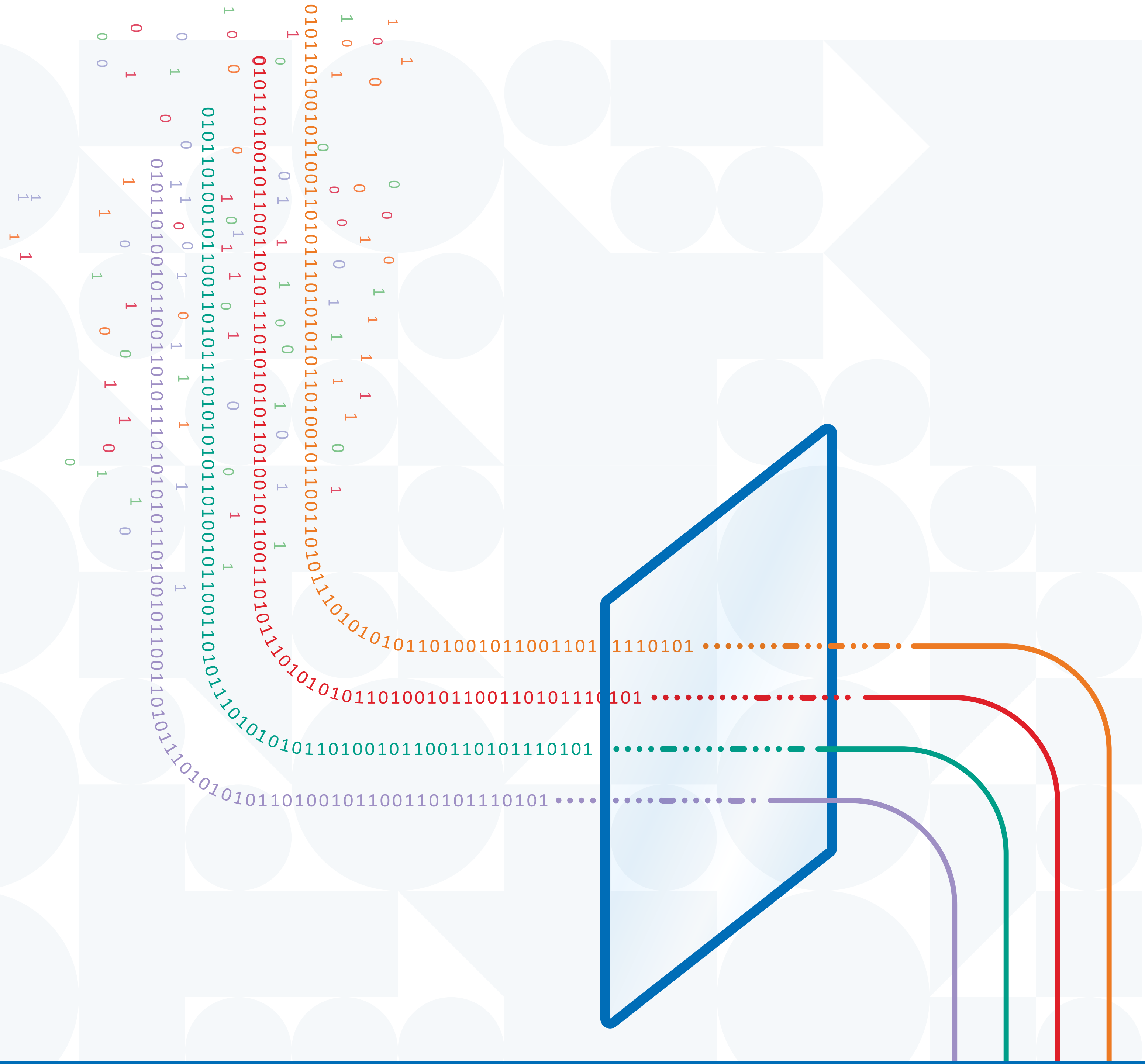
Mitigation strategies for edge devices: Practitioner guidance



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Communications Security Establishment
Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité

National Cyber Security Centre
a part of GCHQ

National Cyber Security Centre
PART OF THE GCSB

NISC
内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

JPCERT CC®

General Intelligence and Security Service
Ministry of the Interior and Kingdom Relations

National Cyber and Information Security Agency
NÚKIB

Disclaimer: *The information in this guide is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favouring by the authoring agencies.*

Table of contents

Audience

This guide is designed for **operational staff**, **cybersecurity staff** and **procurement staff**.

- **Operational staff** refers to practitioners responsible for the availability and maintenance of edge devices in an organisation's network.
  - *Roles include:* Network Engineers, System Administrators, IT System/Network Architects, IT Managers
- **Cybersecurity staff** refers to practitioners responsible for security aspects of edge devices in an organisation's network. These practitioners perform activities such as incident response, threat detection and vulnerability management.
  - *Roles include:* Security Operations Centre (SOC) Analysts, Cybersecurity Engineers, Incident Response Team members, Vulnerability Analysts, Security Managers
- **Procurement staff** refers to practitioners engaged in selection and purchasing of edge hardware and software, ensuring security controls are part of the procurement process.
  - *Roles include:* IT Purchasing Managers, Procurement Officers, Vendor Relationship Managers

Introduction: Living on the edge

Malicious actors are targeting 'edge devices' that act as intermediaries between the internet and internal enterprise networks. The rapid exploitation of newly discovered vulnerabilities is now standard tradecraft for many malicious actors. Both skilled and unskilled malicious actors conduct scanning and reconnaissance against internet-accessible networks to find unpatched software and exploit vulnerable devices.

Throughout this publication, there are references to 'edge devices'. For the purpose of this guide, the term 'edge device' collectively includes internet-facing network hardware and appliances.

Purpose

This guide is the practitioner's expansion to ASD's Mitigation strategies for edge devices: Executive guidance and provides a list of principle mitigation strategies for edge devices to improve security and resilience against cyberthreats. These strategies are vendor agnostic and apply to some of the most common types of edge devices and appliances across enterprise networks and large organisations.

So what?

The Australian Signals Directorate (ASD)'s Australian Cyber Security Centre (ACSC) has noted a concerning increase in the number of incidents involving edge device compromises. Edge devices are internet exposed, typically difficult to monitor and able to access other assets on the network, providing an appealing ingress point and target to malicious actors.

> In a recent research project by ASD, conducted across the Australian environment, over a two-month period, **17.9 million** devices were visible to the public internet.
> **212,000** of these devices were identified as an edge device.[1]

As organisations apply Zero Trust Architecture (ZTA), the principles within this guidance should still be applied to edge devices across enterprise networks. Zero trust principles reduce dependency on boundary controls, however it will never eliminate the need for a secure edge across enterprise networks.

[1] 'Analytical Paper: Enterprise Edge Device Environment – Australian Government and Critical Infrastructure Networks', Research on Operational, Critical and Emerging Technology, ACSC (Limited distribution)

Overview of edge devices

What are edge devices?

Edge devices are critical network components that serve as security boundaries between internal enterprise networks and the internet. These devices perform essential functions such as managing data traffic, enforcing security policies, and enabling seamless communication across network boundaries. Positioned at the network's periphery—often referred to as "the edge"—these devices connect an internal, private network and a public, untrusted network like the internet.

The principles in this publication are scoped to include three of the most implemented edge devices: enterprise routers, firewalls, and VPN concentrators.

Enterprise routers

Routers at the network edge direct incoming and outgoing traffic between the internal network and untrusted external sources, primarily, the internet. They ensure that data is efficiently routed to its destination while applying basic security rules to control access.

Firewalls

Edge firewalls serve as the first line of defence, inspecting and filtering traffic to and from the internal network and the outside world. They enforce security policies by blocking or allowing traffic based on predefined rules, preventing unauthorised access and interdicting identified malicious activity.

VPN concentrators

VPN concentrators at the edge provide secure remote access to the internal network by creating encrypted tunnels for users connecting over the internet. They authenticate users and encrypt data, ensuring that sensitive information stays secure during transmission.

Risks and threats

Why secure the edge?

Any organisation that has a connection to the internet or external networks deploys at least one edge device which makes it crucial to address their security. Edge devices continue to suffer exploitation through vulnerabilities that can be readily mitigated. These devices are directly accessible from the external threat surface, whether part of a traditional network perimeter or within a mature zero trust environment. Organisations must take proactive steps to strengthen their security posture.

Impact

If edge devices are not adequately secure, the consequences can be damaging. Malicious actors compromise edge devices to get initial access and use this access to move laterally into an organisation's internal network environments. This access allows malicious actors to achieve other aims including disrupting systems and critical services, deploying malware, enabling persistence and stealing personal data or other sensitive information.

These malicious actions can lead to monetary loss, reputational damage, legal implications and other significant detriments to an organisation.

One recent example of how vulnerabilities in edge devices can be exploited is the Cutting Edge campaign, which targeted critical sectors and used zero-day vulnerabilities in VPN appliances to devastating effect.

The Cutting Edge campaign case study is included below and is mapped to MITRE ATT&CK techniques used by malicious actors.

Case study – Cutting Edge

Between December 2023 and February 2024, malicious actors behind the Cutting Edge campaign exploited zero-day vulnerabilities in Ivanti Connect Secure VPN appliances (previously Pulse Secure) by utilising defence evasion, living-off-the-land (LOTL) techniques, and deployment of web shells and custom malware.

Malicious actors achieved initial access by:

- exploiting CVE-2023-46805 and CVE-2024-21887 in Ivanti Connect Secure VPN appliances to enable authentication bypass and command injection. A server-side request forgery (SSRF) vulnerability, CVE-2024-21893 was later found and used to bypass mitigations for the first two vulnerabilities by chaining with CVE-2024-21887 [T1554]

Malicious actors established their presence by:

- 'trojanising' legitimate files in Ivanti Connect Secure appliances with malicious code [T1554]
- stealing the running configuration and cache data from Ivanti Connect Secure VPNs [T1005]
- leveraging exploits to download remote files to Ivanti Connect Secure VPN [T1105]
- using malicious plugins to maintain persistence on compromised Ivanti Secure Connect VPNs to enable deployment of backdoors [T1055]

Malicious actors stole credentials by:

- modifying JavaScript file on the Web SSL VPN component of Ivanti Connect Secure devices to keylog credentials [T1056.001]
- modifying JavaScript loaded by the Ivanti Connect Secure login page to capture credentials entered [T1056.003]

Malicious actors achieved lateral movement by:

- using previously stolen valid account credentials to access internal networks [T1078]
- using previously compromised credentials for remote service techniques (a mixture of SSH, SMB and RDP)

Malicious actors utilised multiple techniques to avoid detection, including:

- disabling logging and changing the `compcheckresult.cgi` component to edit the Ivanti Connect Secure built-in Integrity Checker exclusion list [T1562.001]
- changing timestamps of files on compromised Ivanti Connect Secure VPNs [T1070.006]

A deeper analysis of this case study exists at: Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

Frameworks and controls

Organisations should prioritise implementing the recommendations developed by their national cybersecurity authorities when developing an action plan for securing their edge devices.

The following documents have been sourced for the mitigations within this guide:

Australian Signals Directorate (ASD)

Information Security Manual (ISM) and Essential Eight Maturity Model (E8MM)

ASD's ISM provides a comprehensive set of guidelines for protecting IT and OT systems from cyberthreats. It includes standards for system hardening, networking and device procurement. The ISM aligns with the E8MM, which outlines strategies to protect against cybersecurity threats; each strategy has different maturity levels designed to support organisations in achieving progressively higher security standards.

United States Cybersecurity and Infrastructure Security Agency (CISA)

Cross-Sector Cybersecurity Performance Goals (CPGs)

CISA's CPGs, which align with the NIST CSF, offer a prioritised list of security outcomes, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. These goals are tailored to address sector-specific risks, providing organisations with concrete, outcome-focused objectives to improve their resilience against cyberthreats.

Canadian Centre for Cyber Security (CCCS)

Cross-Sector Cyber Security Readiness Goals (CRG) Toolkit

CCCS's CRGs offer a practical framework to protect organisations from common cyberthreats. Designed to align with CISA's Cybersecurity Performance Goals (CPGs) and National Institute of Standards and Technology's (NIST) Cyber Security Framework (CSF), these baseline controls emphasise foundational practices like secure configurations, incident response, and access management to guide organisations in managing and reducing cybersecurity risks.

New Zealand National Cyber Security Centre (NCSC–NZ)

New Zealand Information Security Manual (NZISM) and Cyber Security Framework (CSF)

The NZISM and NCSC-NZ CSF provide a comprehensive set of controls and standards to secure information systems across New Zealand's government and critical infrastructure sectors. Covering aspects such as system hardening, network management, and incident response, the NZISM and CSF support organisations in implementing robust cybersecurity measures aligned with national security requirements.

United Kingdom National Cyber Security Centre (NCSC–UK)

Cyber Assessment Framework (CAF)

The NCSC's CAF provides a systematic and comprehensive approach to assessing the extent to which organisations are affected by cyberrisks based on the organisation's essential functions and supports organisations in building their cyberresilience against these risks. Focusing on key principles such as governance, asset management, and system resilience, the CAF supports organisations in aligning their practices with the UK's National Cyber Security Strategy, helping them mitigate risks to essential services.

Japanese Ministry of Economy, Trade and Industry (METI-JP)

Cybersecurity Management Guidelines

METI and Information-technology Promotion Agency (IPA) provide the Cybersecurity Management Guidelines for business executives to promote cybersecurity measures under the leadership of management. From the perspective of protecting companies from cyberattacks, the guidelines outline "three principles" that executives need to recognize, as well as "ten important items" that they should instruct the responsible executives (such as the CISO) to implement information security measures.

Summarised list of mitigation strategies

Know the edge

Endeavour to understand where the periphery of the network is, and audit which devices sit across that edge. Identify devices that have reached EOL and remove/ replace them.

Procure secure-by-design devices

Prioritise procuring edge devices from manufacturers that follow secure-by-design principles during product development; explicitly demand product security as part of the procurement process. Track deliveries and maintain assurance that malicious actors have not tampered with edge devices.

Apply hardening guidance, updates and patches

Review and implement specific vendor hardening guidance. Ensure prompt application of patches and updates to edge devices to protect against known vulnerabilities.

Implement strong authentication

Implement robust identity and access management practices to prevent unauthorised access with weak credentials or poor access controls. Implement phishing-resistant MFA across edge devices to protect against exploitation.

Disable unneeded features and ports

Regularly audit and disable unused features and ports on edge devices to minimise the attack surface.

Secure management interfaces

Limit exposure by ensuring management interfaces are not directly internet accessible

Centralise monitoring for threat detection

Ensure centralised visibility and log access to detect and investigate security incidents. Event logs should also be backed up and data redundancy practices should be implemented.

Mitigation strategies for edge devices

The following list of principle mitigation strategies is primarily focused on addressing the common issues with edge devices that are leading to successful exploitation against enterprise networks. The strategies are not prioritised in any sequential level of importance.

The strategies compliment relevant Cyber Security Framework (CSF) controls where possible. Partnered nations are welcome to employ these mitigations or map these controls to a different equivalent CSF if compatible.

Know the edge

Before edge devices can be secured, organisations need to know where they are across a network periphery and what role they play. ASD's operational experience indicates entities often have limited understanding and visibility of their network edge and existing services.

Organisations should be aware that edge devices:

- can perform relatively minor roles, not widely understood within the information and communications technology (ICT) environment
- have been frequently discovered existing outside enterprise asset management consoles for assorted reasons
- may be offering more services to the internet than is known or necessary.

For example:
Converged firewall appliances leaving a VPN interface exposed to the internet when not being used.
Edge devices leaving management or administrative interfaces open to internal networks and the internet.

Knowing where edge devices exist is the first step to securing them.

Entities enrolled in ASD's Cyber Hygiene Improvement Program (CHIPs) can use CHIPs reports to inform this work. Organisations not enrolled in this program should consider developing their attack surface monitoring capabilities to enhance visibility of what their network edge looks like from the internet.

Procure secure-by-design devices

Managing cyber supply chain security risks in edge devices starts with procuring devices from vendors that prioritise security at every stage of the product lifecycle. By selecting vendors with a demonstrated commitment to security, organisations can minimise the risk of introducing vulnerable or compromised hardware and software into their networks.

Evaluate vendors

IT equipment is chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, using memory-safe programming languages (where possible), and other secure programming practices, and maintaining the security of their products.

Key framework controls, publications and standards: *ISM-1857; NIST CSF; NIST SP 800-53, Rev. 5; NIST SP 800-161r1upd1*

Procurement teams should apply caution when selecting edge device vendors. This includes reviewing a vendor's history of patch releases and response times to newly discovered vulnerabilities.

They should assess the vendor's transparency in disclosing security vulnerabilities and their history of addressing them.

Ideally, vendors should show commitment to producing edge device hardening guidance and have adopted secure-by-design and secure-by-default product configurations.

Selecting labelled or certified products, such as products with the JC-STAR label in Japan, or CC certified products in Canada helps organisations to procure products with appropriate security measures in place.

Manage vendor risk

The CISO oversees cyber supply chain risk management activities for their organisation.

Key framework controls, publications and standards: *ISM-0731; NZISM-3.2.14.C.01; NIST SP 800-161r1upd1*

A key part of supply chain security is understanding the geographic, geopolitical, and supply chain risks that might be associated with certain vendors. Evaluate whether each vendor's manufacturing processes, geographic location, and supply chain dependencies introduce unacceptable risk to an organisation. Consider whether alternate suppliers or secondary sources would reduce reliance on a single vendor in case of unforeseen vulnerabilities or disruptions in the supply chain.

Secure delivery

Applications, IT equipment, OT equipment and services are delivered in a manner that maintains their integrity.

Key framework controls, publications and standards: *ISM-1790; NZISM-12.7.18.C.02; NZISM-12.1.35.C.01; NZISM-12.1.34.C.02; NIST CSF; NIST SP 800-53, Rev. 5; NIST SP 800-161r1upd1*

Securing the delivery of edge devices from the point of manufacture to their final deployment is crucial for supporting the integrity of the network. Devices that are tampered with during shipping or handling may introduce significant vulnerabilities into an organisation's network infrastructure. To mitigate these risks, procurement staff should ensure appropriate integrity-checking mechanisms throughout the supply chain.

Track the supply chain

Implementing a supply chain visibility system can help track devices from point of production to their final delivery point. Partnering with suppliers who provide real-time tracking and transparent reporting on the status of device shipments can help keep confidence in the integrity of delivered devices.

Assess authenticity and integrity

Network devices are flashed with trusted firmware before they are used for the first time.

Key framework controls, publications and standards: *ISM-1800; NZISM-12.4.6.C.01; NIST SP 800-161r1upd1; CISA CPG 2.Q*

Organisations should thoroughly inspect both the hardware and software of edge devices for any signs of tampering or manipulation when they receive them. This may include verifying that tamper-evident packaging is intact.

Introduction of malicious firmware resulting from a cyber supply chain interdiction attack, a compromised vendor development environment or other cyber supply chain risks can be reduced by flashing network devices with trusted firmware, obtained from vendors via trusted means, before edge devices are used for the first time.

Check for default credentials prior to deployment

Default accounts or credentials for network devices, including for any pre-configured accounts, are changed.

Key framework controls, publications and standards: *ISM-1304; NZISM-14.1.10.C.02; CISA CPG 2.A; CCCS CRG-2.0*

Selecting vendor products that require credential creation rather than providing default credentials is preferred. Default credentials provided by device manufacturers are often widely known and are a prime target for malicious actors. Always change these during the initial setup on a new device, and audit for default credentials across existing edge devices to make the change at once.

Apply hardening guidance, updates and patches

Keeping edge devices hardened and up to date with the latest security patches is crucial in maintaining the security of networks.

Review and implement specific vendor hardening guidance

IT equipment is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.

Key framework controls, publications and standards: *ISM-1858; NZISM-22.2.14.C.05; NIST National Checklist Program*

Specific edge devices and appliances have varying levels of maturity regarding inherent baseline security. When they are deployed with default settings, it can lead to malicious actors gaining access.

Many devices have settings that enable them to be configured in an approved secure state to minimise this security risk. Vendors often produce hardening guidance to assist users in hardening the configuration of edge devices, so they are more secure.

Before deploying edge devices, check for and apply vendor hardening guidance and/or CIS baseline hardening guidance (CIS Center for Internet Security).

Identify any compromised edge devices

Before applying updates or patches, organisations must assess whether their edge devices have already been compromised, particularly when vulnerabilities are known to be actively exploited.

Applying a patch will not remedy a device that has already been compromised, as the patch only addresses the vulnerability itself, not the presence of an adversary on the system.

Before and after patching, or in cases where an organisation has been using end-of-life (EOL) devices or has delayed patching for vulnerabilities that have been actively exploited, it is advisable for security staff to perform a thorough examination of these devices for Indicators of Compromise (IoCs).

Applying mitigations or patches to a compromised device could inadvertently remove security controls that were temporarily implemented, leaving the device vulnerable again. In these instances, organisations should consider which action to take, depending on the severity of the compromise and the resources available to investigate. Risks should be weighed between applying the latest updates or identifying and evicting any adversaries that may have already gained access.

If compromise is detected, seek support from vendors and cybersecurity authorities for more guidance. Australian organisations should report cybercrimes, security incidents and abuse through ReportCyber. Your report helps to disrupt crime operations and makes Australia more secure

Maintain current patch versions

Operational staff and cybersecurity staff should not wait for security issues to be advertised before updating edge devices. Maintaining edge devices on the latest versions of supported vendor releases is important because:

- Vendors do not always advertise that updates contain important security fixes – especially if vulnerabilities are discovered and fixed by the vendor's own team.
- Vendors prioritise advice, mitigation and patches against their most current supported versions of software – if an organisation is on the latest release of a supported version, it will likely get a patch and relevant guidance sooner.
- If the organisation is not on a current release, it may be more difficult to apply the patch. This may require applying an intermediate patch, or other processes due to a device's software being out of date for a greater period. This may increase the outage window for the edge device whilst updating.

Stay informed with vendor security advisories

Most edge device manufacturers release security advisories that detail vulnerabilities and corresponding patches. It is important for operational staff and cybersecurity staff to remain informed about these advisories through vendor communication channels such as:

- vendor security bulletins – subscribe to manufacturer notifications
- Really Simple Syndication (RSS) feeds – RSS feeds should be setup to notify IT staff the moment new patches are available
- email alerts – subscribe to email alerts to receive announcements when new patches are advertised

When a vulnerability is known and a patch has not yet been deployed, vendors typically recommend other mitigations while developing the patch. Organisations should implement these mitigations while waiting for the patch to become available.

Consider automatic updates

Where available, organisations should consider setting up automatic updates of edge devices. The risk of compromise if systems are not swiftly patched is significant. ASD has observed that patches can be missed, which can leave an edge device vulnerable for weeks, months and even years. Implementing automatic updates ensures patches are applied promptly, reducing the window of exposure between vulnerability disclosure and patches being applied. It also eliminates the scenario where a patch is forgotten.

However, automatic patching does create potential availability risks, including having no opportunity to test the impact of updates on operations. Therefore, operational staff should consider the benefits and risks of enabling automatic firmware and software updates before doing so.

Operational, cybersecurity or procurement staff should ask their vendor to understand the mechanisms the vendor has already implemented, such as configuration backups, automatic rollback and restore points.

In cases where automatic updates are not supported, or not used, operational staff and cybersecurity staff will need to:

- ensure they receive, review and respond to vendor security advisories
- regularly check for vendor updates
- schedule maintenance windows for applying critical patches as needed

Real world example
The Fortinet FortiOS vulnerability (CVE-2018-13379) exemplifies the risks of delayed patching. Even two years after the patch was issued, many devices remained vulnerable. Renewed malicious actor interest in the vulnerability lead to significant compromises in both government and commercial sectors.[2]

Scan for unmitigated vulnerabilities

A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.
Key framework controls, publications and standards: *ISM-1701; NIST SP 800-161r1upd1, CCCS CRG-1.1*

To ensure that patches or updates are being applied to edge devices, it is critical that an organisation regularly identifies all assets within their environment using an automated method of asset discovery, such as an asset discovery tool or a vulnerability scanner with equivalent functionality.

Following asset discovery, identified edge devices can be scanned for missing patches or updates using a vulnerability scanner with an up to date vulnerability database. Ideally, vulnerability scanning should be conducted in an automated manner and take place at least daily for internet-facing network devices.

[2] On 3 April 2021, ASD released an alert reminding organisations that APT groups had been observed exploiting CVE-2018-13379. Later, in September 2021, ASD received a report of a successful exploitation of CVE-2018-13379 against an Australian entity. Despite being vulnerable for more than 2 years, the victim's device had not been patched. ASD Cyber Threat Report 2022-2023 | Cyber.gov.au

Manage end-of-life devices

Edge devices that have reached their EOL are particularly vulnerable since vendors no longer provide security updates or patches. Organisations should not use EOL edge devices.

Maintain an inventory of edge devices and their respective support timelines. Periodically review which edge devices have an upcoming EOL date and plan to remove/replace them before EOL occurs.

Actively scan networks for undocumented edge devices, these may also have reached EOL. If replacing an EOL device is not immediately possible:

1. Identify the risk in the context of the system and make an informed decision
2. Look for compensating controls that may reduce risk
3. Identify a plan /schedule for replacement

However, due to the risk of leaving a vulnerable device accessible to public networks as edge devices are, we strongly recommend replacing EOL edge devices immediately.

Relying on unmitigated EOL devices significantly increases the risk of compromise. Further guidance on these risks can be explored in Managing the Risks of Legacy IT: Executive Guidance.

Implement strong authentication

One of the most common vectors to compromise edge devices is exploiting default credentials, weak authentication, or poor identity and access management practices, particularly for edge devices that routinely support user login, such as VPN concentrators.

Whether a malicious actor obtains credentials by password spraying, credential stuffing, using malware such as info stealer or other techniques, weak authentication opens the door to unauthorised access, which can compromise the entire network.

Understand central authentication risks and benefits

Central authentication systems, such as Active Directory, increase an organisation's attack surface when edge device authentication is linked to the primary corporate identity store or when one Identity Provider (IDP) is used across multiple security zones. Edge devices are considered high risk due to being public-facing and internet accessible. Therefore, it is critical to segregate edge devices from an organisation's corporate AD forest or an equivalent authentication, authorisation and accounting (AAA) solution.

For example, by combining a Golden Ticket [T1558.001] with SID History, malicious actors can forge a ticket-granting tickets (TGT) to access other domains in the same forest — or even other forests, if inter-forest trusts exist. For more information visit ASD's Detecting and mitigating Active Directory compromises publication.

ASD has observed advanced persistent threats (APTs) such as APT40 and Volt Typhoon exploiting edge device authentication. These malicious actors have used lateral movement and credential dumping by exploiting centralised authentication systems where edge devices use, or are linked to the primary corporate identity store. One specific observation of this scenario is a service account on an edge device that can perform Lightweight directory access protocol (LDAP) directory lookups against the corporate directory.

Although these risks are prevalent, central authentication systems also offer a range of security advantages, including fine-grained access control, device management plane isolation, and robust hardening of centralised authentication services. These measures can limit lateral movement risks and provide benefits like individual accountability, synchronised account revocation, efficient credential management, logging and anomaly detection.

To effectively manage these risks, organisations should consider both the vulnerabilities and the security strengths of centralised authentication, and tailor their approach accordingly.

Alternative AAA solutions beyond Active Directory may offer similar benefits while addressing specific vulnerabilities. For a detailed approach to secure centralised AAA configurations, refer to NSA's Network Infrastructure Security Guide.

Secure local credentials

Edge devices that use local accounts should be managed through a Privileged Access Management (PAM) system or secrets manager. Depending on the scenario, these solutions can rotate credentials after each use, reducing the risk of long-term credential exposure.

Fortify authentication with multi-factor authentication (MFA)

Multi-factor authentication used for authenticating users of systems is phishing-resistant.

Key framework controls, publications and standards: *ISM-1682; CISA CPG 2.H, CCCS CRG-2.7*

Where edge devices need to have internet exposed login interfaces, such as in a VPN gateway scenario, enabling phishing-resistant multi-factor authentication (MFA) is a key control across various security frameworks and best practices. Implementing phishing-resistant MFA, where possible, provides strong protection against credential stuffing, brute force techniques and makes other password reuse exploits impractical.

Use appropriate single-factor authentication if MFA is not supported

When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.

Key framework controls, publications and standards: *ISM-0417; CISA CPG 2.B*

If phishing-resistant MFA is not supported by a device, single-factor authentication should be achieved using the latest password or passphrase complexity and length advice from local cybersecurity authorities.

For Australian organisations, passphrases used for single-factor authentication should be at least 4 random words with a total minimum length of 15 characters (unless more stringent requirements apply for an organisation). In cases where systems do not support passphrases, and as an absolute last resort, the strongest password length and password complexity supported by a system should be implemented.

Credentials should never be reused.

Apply strong protections for password storage

Credentials stored on systems are protected by a password manager; a hardware security module; or by salting, hashing and stretching them before storage within a database.

Key framework controls, publications and standards: *ISM-1402; CCCS CRG-2.10*

When storing credentials on edge devices, it is crucial to use secure hashing algorithms to protect against credential theft. To ensure password storage algorithms are less vulnerable to brute force attacks, avoid algorithms that:

- use older, less secure algorithms like MD5
- use a single or small number of hash function iterations
- use legacy methods which store passwords with custom encodings and not cryptographic hash functions.

Disable unneeded features and ports

Many available features on modern edge devices are optional, enabled by default, and at times, not used by organisations. Conducting an audit and disable any features that are not being used will reduce the attack surface of the device.

Some commonly exposed services are:

- **VPN interfaces:** Many security related edge devices have a VPN feature and offer a VPN service by default. If a VPN feature is not being used, disable the service and block the service from the internet.
- **Application Programming Interfaces (APIs):** Many edge devices have APIs which are enabled by default. If these are not being used and if it is possible to disable the API, then do so.
- **Simple Network Management Protocol (SNMP):** If SNMP is needed for monitoring, configure SNMPv3, allow it from only approved endpoints and disable other versions of the protocol. SNMPv3 supports encryption and stronger authentication to protect against exploits against older versions.
- **Device administration interfaces:** Many edge devices may have interfaces for device administration open by default. These interfaces should be placed behind appropriate access controls during device configuration. These interfaces, especially web implementations, should be blocked from the internet.
- **Internet Protocol version:** Organisations exclusively using Internet Protocol version 4 (IPv4) should disable IPv6. This will assist in minimising the attack surface of networks and ensure that IPv6 cannot be exploited by malicious actors.

Close unused ports

Unused physical ports on network devices are disabled.

Key framework controls, publications and standards: *ISM-0534; NZISM-22.3.11.C.01; CISA CPG 2.B; NIST SP 800-53, Rev. 5, CCCS CRG-2.17*

Edge devices often come with multiple open ports that support assorted services, which an organisation may not need for their environment. Reducing the number of open ports minimises the device's exposure to potential threats.

Regularly audit the open ports on edge devices to ensure only necessary services are enabled. Disable any ports or services that are not actively in use.

Secure management interfaces

Securing management interfaces and services on edge devices is crucial for minimising the attack surface that malicious actors can exploit.

Apply access control lists

Network access controls are implemented on networks to prevent the connection of unauthorised network devices and other IT equipment.

Key framework controls, publications and standards: *ISM-0520; NZISM-18.1.13.C.01; CISA CPG 2.B; NIST CSF; NIST SP 800-53, Rev. 5*

Implementing network access control lists (ACL) on edge devices helps restrict who can communicate with specific ports and services. ACLs provide strict control over which IP addresses or networks can access the management interfaces of edge devices.

Use dedicated management interfaces

Whenever possible, edge devices should be equipped to use dedicated management interfaces that are segregated from the primary data interfaces. Isolating management traffic from regular network traffic (also referred to as separating the control plane from the data plane) reduces the exposure of sensitive management functions and ensures only authorised operational staff and cybersecurity staff can access these critical interfaces.

Do not expose management interfaces to the internet

Networked management interfaces for IT equipment are not directly exposed to the internet.

Key framework controls, publications and standards: *ISM-1863; CCCS CRG-2.21, CISA Binding Operational Directive (BOD) 23-02: Implementation Guidance for Mitigating the Risk from Internet-Exposed Management Interfaces*

Management interfaces can include services such as telnet, Simple Network Management Protocol (SNMP), Secure Shell (SSH), web-based administration interfaces (on standard and non-standard ports) and application programming interface (API) endpoints in existing web interfaces.

A vendor's security configuration advice should explain these various management interfaces and the recommended configuration options for each of them.

Management interfaces are not designed to be exposed to the internet. This is borne out by how often critical vulnerabilities arise in management interfaces, compared to interfaces built to be internet facing.

It is imperative that these management interfaces are not exposed to the internet.

Real world example
Threat group BackdoorDiplomacy exploited CVE-2020-5902, an F5 BIG-IP vulnerability, to drop a Linux backdoor into an exposed management interface. This is an example of exploiting a public facing application [T1190].

An attack surface is also expanded by aggregating management interfaces into a single management network. This attack surface can be reduced by implementing private virtual LANs (VLANs) to prevent lateral movement of a malicious actor. This management traffic should be terminated on a firewall with appropriately configured ACLs.

Consider network segmentation

Network segmentation is a key practice in securing networks. By dividing a network into smaller, isolated segments, organisations can control the flow of traffic, restrict access to sensitive data and limit the potential for lateral movement during compromise.

Segmentation with sufficient filtering rules can reduce the attack surface, help contain breaches, increase the chances of detecting malicious activity and make it harder for malicious actors to escalate privileges and move laterally.

Edge devices are sometimes used to create this segmentation, such as a layer 4 firewall. In other situations, edge devices might perform a layer 7 function, such as an email security gateway. Converged edge devices, such as modern firewalls, may perform both functions, particularly in smaller environments. For example, a single converged security edge device may act as a layer 4 gateway for most network traffic, but also a layer 7 gateway for VPN and email services.

Due to the wide set of deployment scenarios edge devices are used for, and the wide variety of edge device types and features, it is difficult to give succinct advice for each instance.

For more resources toward understanding secure architecture and design around the configuration of network segmentation, refer to the following guidance from ASD's ACSC:

- Guidelines for Networking
- Gateway Security Guidance Package: Gateway Security Principles
- Managing the Risks of Legacy IT: Practitioner Guidance

Centralise event logging for threat detection

Effective logging and monitoring are crucial for detecting potential threats on edge devices. Centralising log collection allows for more efficient analysis and threat detection and complicates the process for a malicious actor to remove logs that may lead to their detection.

Centralise logging in real time

Log events from edge devices should be sent in real time to a centralised system. Controls, which do not rely on the edge device, such as a separate firewall, should be used to restrict the access from the edge device to the log collection point so that only the data necessary for transferring logs is shipped.

Secure event log storage and integrity

A centralised event logging facility is implemented, and event logs are sent to the facility as soon as possible after they occur.

Key framework controls, publications and standards: *ISM-1405; NZISM-16.6.12.C.03; CISA CPG 2.U, CCCS CRG-2.16*

Logs must be secured in both transit and at rest, ensuring that they are protected from unauthorised access, modification, or deletion. Event logs should be stored in a centralised facility, such as a data lake or a SIEM system, to enable access and analysis by authorised users.

The log aggregator(s) and parser(s) should use input validation. The key control to be considered for edge device logging is that the edge devices should not have access that allows the modification or deletion of any logs. This safeguards against malicious actors tampering with evidence of exploitation.

For more comprehensive detail on event logging and threat detection, please see the co-sealed Best practices for event logging and threat detection.

Profile expected events

Having a baseline understanding of what normal activity looks like between the internet and an edge device, plus between the edge device and other internal systems, is critical.

Certain activity on an edge device should be considered high-risk and investigated as soon as possible. Examples may include unexpected:

- configuration changes
- reboots
- ACL modifications
- password changes
- tunnels/traffic forwarding
- outbound connections (Web, File Transfer Protocol)
- large data transfers to the internet
- serialisation errors

Certain interactions between an edge device and an internal network should also be investigated at once, including:

- where edge devices are configured with internal network credentials (for example, an AD account so the edge device can do LDAP searches), this account should alert if it accesses any hosts other than the one it is specifically configured to communicate with.
- network traffic directed at hosts that the edge device doesn't normally communicate with.

Additionally, generating event logs and alerts for network traffic that contravenes any rule in a firewall ruleset can help identify suspicious or malicious traffic entering networks due to a failure of, or configuration change to, firewalls.

Engage authorities for any compromises

When irregular and suspicious activity is discovered, security staff should proactively report to vendors and cybersecurity authorities (ASD for Australian organisations – Report and recover | Cyber.gov.au). ASD can help organisations understand malicious behaviour or catch zero-day vulnerabilities.

If an organisation has a Network Operations Centre (NOC) or a Security Operations Centre (SOC), identification of these activities should be prioritised as detection engineering scenarios. Threat modelling may assist teams in finding what should be analysed to identify tactics, techniques and procedures (TTPs) used.

Conclusion

Edge devices, which serve as critical points between internal networks and the internet, are increasingly targeted by malicious actors due to their key role in managing traffic and enforcing security policies. As organisations scale their digital infrastructure, the security of these devices must be a top priority. The strategies in this guide are a set of practices aimed to build resilience across edge devices and the networks they interact with.

Further guidance

ASD's resources

- Mitigation strategies for edge devices: executive guidance
- Identifying Cyber Supply Chain Risks
- Choosing secure and verifiable technologies
- Cyber Supply Chain Risk Management
- Gateway hardening package
- Secure your Wi-Fi and router
- Identifying and Mitigating Living Off the Land Techniques
- Cybersecurity Best Practices for Smart Cities
- Guidelines for System Hardening

- Managing the Risks of Legacy IT: Practitioner Guidance
- Best practices for event logging and threat detection
- Network hardening
- Implementing Network Segmentation and Segregation

United States CISA's resources

- Cybersecurity Performance Goals (CPGs)
- Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers
- Secure-by-Design
- Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem
- Securing Network Infrastructure Devices
- Zero Trust Maturity Model
- Layering Network Security Through Segmentation Infographic
- Trusted Internet Connections (TIC)
- Understanding Patches and Software Updates
- CISA Binding Operational Directive (BOD) 23-02: Implementation Guidance for Mitigating the Risk from Internet-Exposed Management Interfaces

NIST's resources

- Cybersecurity Framework (CSF)
- SP 800-53, Rev. 5
- SP 800-161r1upd1
- National Checklist Program

Canada's CCCS's resources

CCCS recommends wherever possible, organisations should endeavor to "Consolidate, monitor, and defend Internet gateways" as per CSE's Top 10 IT security actions:

- Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089)

Japan's METI's resources

Japan Cyber STAR (JC-STAR): "Labeling Scheme based on Japan Cyber-Security Technical Assessment Requirements" is a Japanese labeling scheme that confirms the conformance of IoT products to conformance requirements (security technical requirements) based on its own standards, while harmonising with domestic and international standards such as ETSI EN 303 645 and NISTIR 8425.

- Japan Cyber STAR (JC-STAR) | IPA, METI

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre