Mitigation strategies for edge devices: Executive guidance

Malicious actors are increasingly targeting internet-facing edge devices to gain unauthorised access to networks; therefore, it is vital that organisations prioritise securing edge devices in their environments. Edge devices are critical network components that serve as security boundaries between internal enterprise networks and the internet. The most commonly observed edge devices implemented across enterprise networks include enterprise routers, firewalls, and VPN concentrators. 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.

Failing to secure edge devices is like leaving a door open from the internet to internal networks, potentially allowing malicious actors to gain access to networks – from there, they can access sensitive data and disrupt operations.

If organisations have not applied zero trust principles in their environments, malicious actors can use a range of techniques to gain access through network edge devices. This typically occurs through identifying and exploiting newly released vulnerabilities for edge devices, which have a poor track record for product security. Both skilled and unskilled malicious actors conduct reconnaissance against internet-accessible endpoints and services to identify and exploit vulnerable devices.

Some examples of malicious actors exploiting edge devices include:

- PRC state-sponsored actors compromise and maintain persistent access to U.S. critical infrastructure (ASD)
- People's Republic of China-Linked Cyber Actors Hide in Router Firmware (CISA)

Scope

This publication offers a high-level summary of existing guidance for securing edge devices from the cybersecurity authorities of the following partnered countries: Australia, Canada, Czech Republic, Japan, Netherlands, New Zealand, South Korea, the United Kingdom, and the United States. It consolidates key practices for effectively managing and securing edge devices. This guidance is intended for executives within large organisations and critical infrastructure sectors responsible for the deployment, security, and maintenance of enterprise networks.

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.*

Summary of mitigation strategies

The following table outlines key strategies for securing edge devices, aimed at enhancing network security and reducing vulnerabilities.

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 end-of-life (EOL) and remove/replace them.

Procure secure-by-design devices

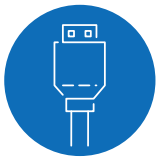
Prioritise procuring edge devices from manufacturers that follow secure-by-design principles during product development. Explicitly demand product security as part of the procurement process; for more guidance consider Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem. 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 multi-factor authentication (MFA) across edge devices to protect against exploitation.

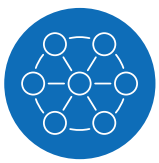


Disable unneeded features and ports

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.

Frameworks and controls

The authoring organisations provide the following publications for organisations to use that contain the best practice guidance on securing, hardening, and managing edge devices effectively. All organisations are encouraged to review and follow these policies, procedures, and publications to improve the security of their edge devices. Organisations should prioritise implementing the recommendations developed by their national cybersecurity authorities when developing a plan of action and implementation for securing their edge devices.

The following publications have been sourced to build 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.

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.

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.

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.

Procuring edge devices that are secure by design

Before procuring any edge device, organisations must evaluate the manufacturer - including its country of origin, and its product - to ensure all security concerns have been considered and addressed. Choosing technologies that have been developed following secure-by-design practices will assist organisations in building a resilient enterprise network that maintains confidentiality, integrity and availability and mitigates costly events.

The authoring organisations recommend the following publications for guidance when procuring edge devices:

Choosing Secure and Verifiable Technologies: Secure-by-Design Foundations (ASD)

Secure-by-Design Foundations (ASD)

Cyber supply chain: An approach to assessing risk (CCCS)

Supply chain security guidance (NCSC–UK)

Secure-by-Design (CISA)

Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (CISA and Federal Bureau of Investigation [FBI])

Additionally, selecting labelled or certified products, such as products with the JC-STAR label in Japan, will help organisations to procure products with appropriate security measures in place.

Furthermore, the authoring agencies encourage all edge device manufacturers to make their products secure by design. Manufacturers can review CISA's Secure by Design Alert: Security Design Improvements for SOHO Device Manufacturers for guidance on how to implement secure features by default in their products and join CISA's Secure by Design Pledge. This pledge outlines specific goals for manufacturers to meet to make their products more secure, including goals to reduce the presence of vulnerabilities in their products and transparently report on vulnerabilities.

Network segmentation and segregation

Network segmentation and segregation are critical to safeguarding an organisation's environment by limiting potential pathways for unauthorised access and lateral movement within their networks. By isolating sensitive systems, this approach strengthens defences against cyberthreats, minimises the impact of breaches, and ensures resilient operations across interconnected systems.

The authoring organisations recommend the following publications for guidance on network segmentation and segregation:

Implementing Network Segmentation and Segregation (ASD)

A zero trust approach to security architecture (CCCS)

Baseline security requirements for network security zones (version 2.0) - ITSP.80.022 (CCCS)

Preventing Lateral Movement (NCSC–UK)

Cross-Sector CPGs; Securing Network Infrastructure Devices; Zero Trust Maturity Model; Layering Network Security Through Segmentation Infographic (CISA)

Reducing the risk of network compromises (NSA)

Gateway hardening

Gateway hardening aims to help organisations design, procure, operate, maintain, or dispose of gateway services. A gateway is a boundary system that separates different security domains and allows an organisation to enforce its security policy for data transfers between the different security domains. Partnered cybersecurity authorities strive to assist organisations in addressing cybersecurity challenges and making informed risk-based decisions to enhance gateway security.

The authoring organisations recommend the following publications for guidance on gateway hardening:

Gateway Security Guidance Package (ASD)

Top 10 IT security actions to protect Internet connected networks and information (CCCS)

Trusted Internet Connections (TIC) (CISA)

Network Infrastructure Security Guidance, Hardening Network Devices (NSA)

Securing edge devices in smart infrastructure

Edge devices play a key role in modern smart infrastructure, where they serve as critical connection points that support data flow and communication across smart technologies.

The authoring organisations recommend the following publications for guidance toward securing edge devices in smart infrastructure:

Introduction to Securing Smart Places (ASD)

VPNs (CCCS)

Connected Communities (CCCS)

VPNs; Network Architectures (NCSC–UK)

Cybersecurity Best Practices for Smart Cities (CISA)

Event logging and threat detection

Once malicious actors have established a foothold within a network, they can use living-off-the-land (LOTL) techniques, which involve leveraging built-in tools and system processes to achieve their objectives. This makes it difficult for network defenders to differentiate malicious activity from legitimate activity. To defend against these techniques, it is crucial to have comprehensive event logging and network telemetry to enable visibility and detect threats.

Where compromises occur, or are suspected to have occurred, robust logging will help organisations effectively monitor for threats and intrusions.

The authoring organisations recommend the following publications for guidance on monitoring for threats and intrusions:

Best Practices for Event Logging and Threat Detection (ASD)

Introduction to logging for security purposes (NCSC–UK)

Cross-Sector CPGs (CISA)

Network security logging and monitoring (CCCS)

Legacy edge devices

Edge devices will eventually become legacy hardware, or End-of-Life (EOL), when software is no longer supported or updated by the manufacturer. Edge devices that have reached EOL, especially those no longer supported by manufacturers, can be more vulnerable to cyberthreats. It is crucial to upgrade software to supported versions or replace edge devices that have reached EOL to ensure that they remain secure against cyberthreats.

The authoring organisations recommend the following publications for guidance on understanding, assessing and managing the risks associated with legacy edge devices:

Managing the Risk of Legacy IT: Executive Guidance (ASD)

Obsolete products (CCCS)

Obsolete products (NCSC–UK)

Understanding Patches and Software Updates (CISA)

Further information and contacts

For additional guidance, resources, or specific inquiries related to securing edge devices and implementing cybersecurity best practices for edge devices, organisations are encouraged to contact their respective national cybersecurity authorities:

Australian Signals Directorate (ASD)

For inquiries, visit the ASD's website at www.cyber.gov.au or call the Australian Cyber Security Hotline at 1300 CYBER1 (1300 292 371).

Canadian Centre for Cyber Security (CCCS)

The CCCS supports Canadian organisations. Visit www.cyber.gc.ca for publications and guidance or contact CCCS via 1-833-CYBER-88 or email contact@cyber.gc.ca.

New Zealand National Cyber Security Centre (NCSC–NZ)

The NCSC–NZ assists New Zealand organisations. Visit www.ncsc.govt.nz for guidance and resources, or email them at info@ncsc.govt.nz

National Cyber Security Centre (NCSC–UK)

For UK-based organisations, the NCSC offers comprehensive resources at www.ncsc.gov.uk. The NCSC's contact page provides details for inquiries, or they can be reached by email at enquiries@ncsc.gov.uk.

Cybersecurity and Infrastructure Security Agency (CISA)

CISA provides support for U.S.-based organisations. Visit www.cisa.gov for resources or reach out via email at central@cisa.gov. Report suspicious or malicious cyberactivity to CISA via the agency's Incident Reporting Form or its 24/7 Operations Center (report@cisa.gov), or by calling **1-844-Say-CISA** (1-844-729-2472).

National Center of Incident readiness and Strategy for Cybersecurity (NISC)

For Japan-based organisations, should you have any question, please visit NISC Query form (JP) : https://www.kantei.go.jp/jp/forms/nisc_opinion.html

Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

To submit incident reports to JPCERT/CC, please send an email to info@jpcert.or.jp

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

This publication was developed by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) in collaboration with United States' Cybersecurity and Infrastructure Security Agency (CISA) & National Security Agency (NSA); the Canadian Centre for Cyber Security (CCCS); the National Cyber Security Centre UK (NCSC-UK); the National Cyber Security Centre New Zealand (NCSC-NZ); Japan's National Center of Incident Readiness and Strategy for Cybersecurity (NISC) & Computer Emergency Response Team (JPCERT); Republic of Korea's National Cyber Security Centre (NCSC) and National Intelligence Service (NIS); the General Intelligence and Security Service of the Netherlands (AIVD) and Dutch Military Intelligence & Security Service (MIVD); and the National Cyber and Information Security Agency (NUKIB) of the Czech Republic.