Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Mitigation strategies for edge devices: executive guidance

Content Complexity
MODERATE ● ● ○

The Australian Signals Directorate (ASD) has observed malicious actors targeting internet-facing 'edge' devices that act as security intermediaries between internal networks and the internet. The term 'edge devices' includes systems such as firewalls, routers, virtual private network (VPN) gateways, internet of things (IoT) devices, internet-facing servers, and internet-facing operational technology systems. Edge devices are essentially internet connected doors into enterprise networks, where data flows in and out. The primary functions of edge devices can include managing data traffic, enforcing security policies and ensuring seamless communication across network boundaries. Failing to secure these network perimeters is equivalent to leaving doors open, inviting malicious actors to access sensitive data, disrupt operations and initiate further exploits.

Malicious actors employ a range of techniques to gain access through network edge devices. The rapid exploitation of newly released vulnerabilities is now standard tradecraft. Both skilled and unskilled malicious actors conduct reconnaissance against internet-accessible networks to identify and exploit vulnerable devices.

Where multi-factor authentication (MFA) is not enabled, malicious actors use stolen credentials, or exploit weak or default credentials, to gain access to corporate networks through edge devices. The use of valid credentials allows malicious actors to maintain stealth, which, combined with other living off the land techniques creates challenges for defenders to detect malicious activity.

Introduction

This publication provides a high-level summary of ASD's existing guidance to manage and secure edge devices effectively. It is intended for executives in large organisations and critical infrastructure providers that are responsible for the deployment, operation, security, and maintenance of enterprise networks.

Summary of edge device mitigation strategies

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

Credential management	Change default credentials and use strong authentication methods, such as phishing-resistant MFA, for access to edge devices.
Threat modelling	Identify threats to edge devices and the greatest risks they present to the enterprise network.
Vulnerability management	Ensure edge devices are scanned and managed as part of an organisation's vulnerability management process.
Patching and updates	Ensure all edge devices are up to date with the latest security patches, especially when exploitable vulnerabilities are discovered. Enable automatic updates where supported.
Port and service management	Disable unnecessary ports and services on edge devices. Administration and management interfaces should not be internet accessible.
Asset management	Document the edge device architecture. This includes recording assets in your configuration management database or equivalent.
Event logging and forwarding	Enable detailed event logging on edge devices and forward event logs to a centralised logging facility.
Threat and anomaly detection	Monitor event logs and other telemetry, such as flow telemetry, for signs of suspicious or anomalous activity.
Access control	Employ strict access control and restrict administrator access to edge devices to only those who require it, and only from authorised management devices.
Network segmentation and segregation	Edge devices should be deployed into their unique network segments to minimise the risk of lateral movement if an edge device is compromised. For further information see ASD's Network Segmentation and Segregation publication.
Hardening	Harden the devices as per vendor or industry specific practices and stay up to date on vendor better practices as they will evolve over time. For managed service arrangements, ensure contractual terms with managed service providers require vendors to apply hardening and mitigation tactics. For example, using unique, unpredictable, securely stored credentials per customer.
Penetration testing	Conduct a penetration test against an organisation's network implementation and remediate identified findings.
Secure-by-Design procurement	Prefer manufacturers of edge devices that have followed Secure-by-Design principles and practices during their design, development, and operational support.

Supporting resources

ASD has released several publications to date that detail better practice guidance to assist with securing, hardening and operating devices securely, including edge devices.

Gateway hardening

The Gateway Security Guidance Package aims to help organisations designing, procuring, operating, maintaining, or disposing 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. The package helps organisations address cyber security challenges and make informed, risk-based decisions to enhance gateway security. While primarily intended for Australian Government entities, the package is applicable to any organisation and emphasises aligning gateway security with existing risk management frameworks.

Edge devices facilitate access to an organisation's services via the internet. Securing edge devices reduces the risk of compromise and subsequent lateral movement, thereby maintaining the integrity of the broader network, including in hybrid and cloud environments.

The Information Security Manual

ASD's Information Security Manual (ISM) is a cyber security framework which contains best practices to protect an organisation's information technology (IT) and operational technology systems, applications, and data from cyber threats. The ISM includes several chapters relevant to edge device hardening and security, especially those capable of running third-party software. These are:

- system hardening
- system management
- networking
- procurement
- gateways.

Where applicable, the controls in the ISM are also mapped to the Essential Eight Maturity Model, helping ensure that edge devices meet security standards at different maturity levels.

Edge devices in smart cities

Smart cities are places designed to provide enhanced services to citizens using a collection of smart IT enabled systems and devices that capture, communicate and analyse data. In these infrastructures, edge devices act as critical components that connect and manage systems by collecting and transmitting data. ASD has released an *Introduction to Securing Smart Places* and a joint-sealed publication, *Cybersecurity Best Practices for Smart Cities*.

These publications collate resources on hardening several edge devices, including:

- remote access VPN solutions
- IoT devices
- web servers
- remote or internet-facing industrial control systems.

Secure-by-design principles, robust authentication methods (like MFA) and moving towards a zero trust architecture are important to protect edge devices from unauthorised access. Strong cyber supply chain management and regular patching are also vital to mitigate vulnerabilities and ensure the safe operation of edge devices within interconnected smart city networks.

Event logging and threat detection

Edge devices are a vector for malicious actors to compromise your enterprise network. Once they have established a foothold, malicious actors can use living off the land techniques, which involve leveraging built-in tools and system processes to achieve their objectives. This makes it very difficult for network defenders to detect their activity amidst legitimate network activity. As such, it is crucial to have effective event logging and network telemetry to enable visibility and threat detection.

ASD has released guidance on *Best Practices for Event Logging and Threat Detection* to help organisations effectively monitor for threats and intrusions. Where compromises occur, or are suspected to have occurred, effective logging from edge devices will help you conduct forensics to determine the nature and extent of such an intrusion.

Procuring edge devices

The co-sealed *Choosing Secure and Verifiable Technologies* publication informs organisations and manufacturers of secure-by-design considerations for digital products and services. Choosing technologies that are secure-by-design is a worthwhile investment. These technologies are crucial for edge devices to reduce their operating costs over time. This approach is important for edge devices, as securing these devices from the outset can prevent costly data breaches. Robust security of edge devices helps to ensure the confidentiality, integrity and availability of the network and organisational information.

Legacy edge devices

All edge devices eventually become legacy when their firmware or operating systems are no longer supported by vendors. ASD's publication *Managing the Risk of Legacy IT* assists executives of any organisation to understand, assess and manage the risks associated with legacy edge devices.

Edge devices that have reached end-of-life (EOL), especially those no longer supported by vendors, can be more vulnerable to cyber threats. It is crucial to upgrade to supported versions or replace edge devices that have reached EOL to ensure that they remain secure and capable of handling cyber threats.

Further information

The Information Security Manual is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the Strategies to Mitigate Cyber Security Incidents, along with its Essential Eight, complements this framework.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).