Managed Defender Endpoint Detection and Response (EDR)

We deliver endpoint security to continuously monitor, detect, investigate, and respond to advanced threats

The rapidly evolving threat landscape, characterised by sophisticated ransomware attacks and the increasing complexity of hybrid work environments, has overwhelmed traditional security measures. Cybercriminals leverage advanced technologies like cloud computing, AI, and machine learning to launch increasingly sophisticated attacks that often go undetected for extended periods, enabling attackers to cause significant damage.

Due to resource constraints and a lack of expertise, many organisations struggle to effectively detect and respond to cyberattacks quickly.

Powered by Microsoft, Telstra Managed Defender Endpoint Detection and Response (EDR) addresses these challenges by providing advanced threat detection, response, and remediation capabilities, helping organisations to stay ahead of cyber threats and minimise business disruption.

Managed Defender Endpoint Detection and Response (EDR) Capabilities

Core Defender Vulnerability Management

Discovery,assessment, prioritisation, and remediation of endpoint vulnerabilities and misconfigurations.

Attack Surface Reduction (ASR)

The first line of defence in the stack. This includes network protection and web protection, which regulate access to malicious IP addresses, domains, and URL.

Next-Generation Protection

Catch and block all types of emerging threats using Microsoft Defender Antivirus. It provides a behavior-based, heuristic, and real-time antivirus protection.

Endpoint Detection and Response (EDR)

Detect, investigate, and respond to advanced threats that may have made it past the ASR and Next Gen protection. It provides Advanced Hunting to proactively find breaches and create custom detections.

Automated Investigation and Remediation (AIR)

Automatic investigation and remediation capabilities that help reduce the volume of alerts in minutes at scale.

Key Service Features

24x7x365 Security Monitoring & Response
Proactively detects and prioritises security incidents, enabling swift remediation with actionable alerts.

Multi-Source Threat Intelligence
Enhances threat detection with data enrichment from Microsoft Defender Threat Intelligence (MDTI) and Telstra's unique threat telemetry.

Resource Optimisation
Eliminates the need for internal security teams, streamlining operations and reducing costs.

Enhanced Risk Management and Compliance
Telstra Managed Defender EDR improves security posture and manages risk through continuous monitoring, threat detection, and incident response, ensuring compliance with regulations.

Automated Security Operations
Bridge skill and technology gaps with Telstra's security operations expertise whilst leveraging an automated and streamlined incident lifecycle capability for reduced mean-time-to-respond (MTTR).

Key Service Benefits

Reduce Risk
Enhance detection and response capabilities to mitigate risks.

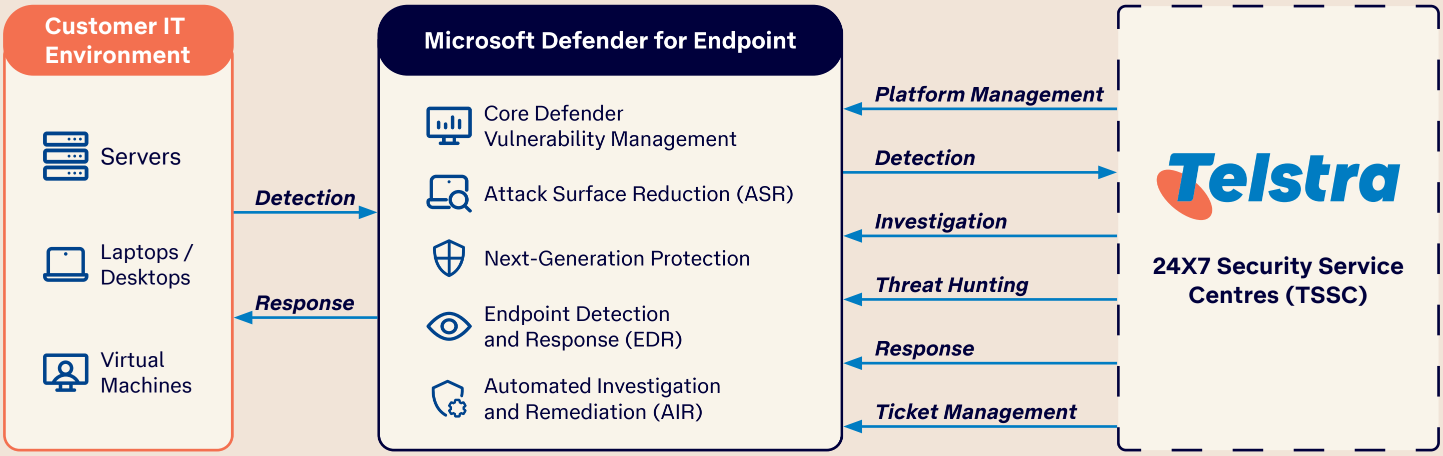
Improved Operational Efficiency
Free up security teams for strategic initiatives, leverage specialised expertise, and ensure optimised security operations.

Faster Threat Correlation
Accelerate investigations with faster correlation of threats across endpoints, enriched with threat intelligence.

Enhanced Compliance
Meet compliance requirements through improved security controls and monitoring.

Reduce Costs
Provide a cost-effective alternative to building, maintaining, or expanding an in-house SOC by eliminating associated costs such as additional staffing, staff retention, staff upskilling and infrastructure.

Delivering Endpoint Security 24X7 through Telstra Security Service Centres



Customer IT Environment

Servers

Laptops / Desktops

Virtual Machines

Detection

Response

Microsoft Defender for Endpoint

Core Defender Vulnerability Management

Attack Surface Reduction (ASR)

Next-Generation Protection

Endpoint Detection and Response (EDR)

Automated Investigation and Remediation (AIR)

Platform Management

Detection

Investigation

Threat Hunting

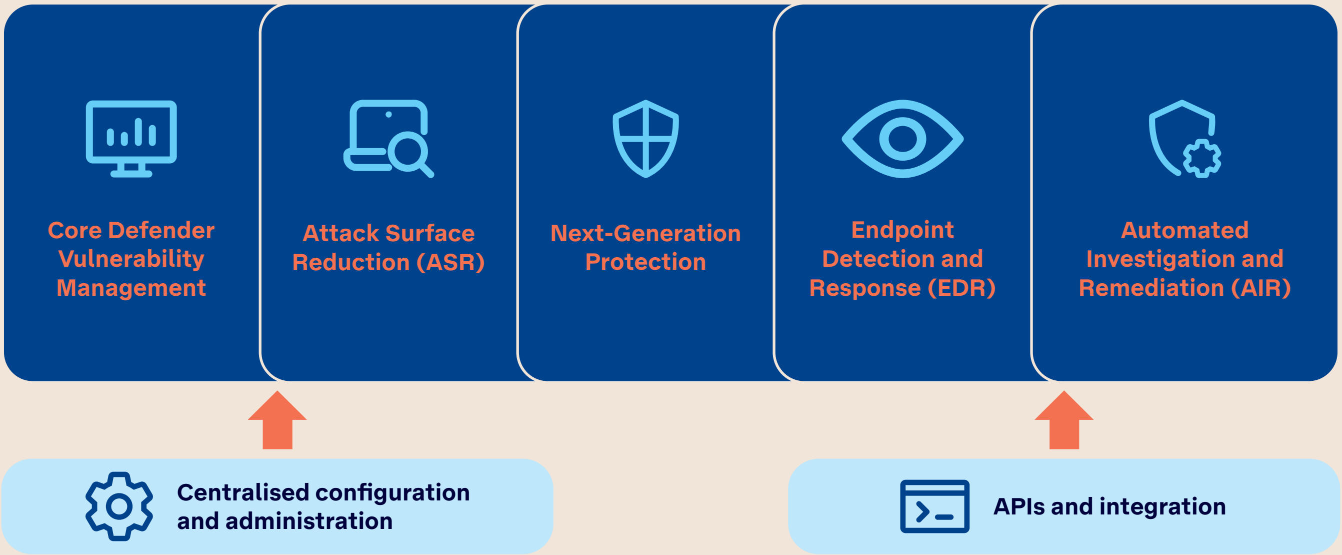
Response

Ticket Management

Telstra

24X7 Security Service Centres (TSSC)

How does Telstra Managed Defender Endpoint Detection and Response (EDR) work?



Core Defender Vulnerability Management

Attack Surface Reduction (ASR)

Next-Generation Protection

Endpoint Detection and Response (EDR)

Automated Investigation and Remediation (AIR)

Centralised configuration and administration

APIs and integration

Core Defender Vulnerability Management

Built-in vulnerability management capabilities use a modern risk-based approach to:

- Discover and assess vulnerabilities and misconfigurations on endpoints
- Prioritise critical vulnerabilities
- Automate remediation processes

Attack Surface Reduction (ASR)

The attack surface reduction (ASR) capabilities form the first line of defense by:

- Ensuring proper configuration settings
- Applying exploit mitigation techniques
- Resisting attacks and exploitation attempts

Next-Generation Protection

Telstra Managed Defender EDR further reinforces security by leveraging next-generation protection to:

- Detect and respond to all types of emerging threats
- Protect your network perimeter

Endpoint Detection and Response (EDR)

Endpoint detection and response capabilities are put in place to detect, investigate, and respond to advanced threats that may have made it past the first two security pillars.

Advanced hunting provides a query-based threat-hunting tool that lets you proactively find breaches and create custom detections.

Automated Investigation and Remediation (AIR)

Microsoft Defender for Endpoint combines advanced threat detection and response with automated investigation and remediation capabilities to quickly address threats and reduce alert fatigue.

Centralised Configuration and Administration, APIs and Integration

Integrate Microsoft Defender for Endpoint into your existing workflows and Microsoft solutions.

Centralised configuration and administration for streamlined management.

Our Approach to Safeguard Your Business

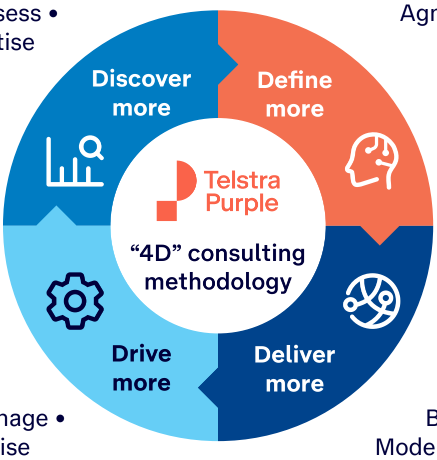
Our proven consulting methodology has helped global customers to safeguard their business and achieve their desired business outcomes.

Discover more

Strategise • Assess • Identify • Prioritise

Define more

Agree • Architect • Design • Plan



Transition • Manage • Review • Optimise

Drive more

Build • Migrate • Modernise • Innovate

Deliver more

What we'll do

Logical and pragmatic approach to solution adoption and deployment, helping your business to navigate the complexities of security.

End-to-end solutioning that grows as your business does. Understand your security needs and design tailored services, managed by our experts.

Provide clear visibility of your solution functions and any risks we might encounter along the way.

Contextually-mapped and strategically-built around your specific threat profile to enable swift identification and resolution.

Business is everywhere. Security should be too.

Your business needs to be secure.

Telstra International offers modular security solutions designed to help safeguard your data, people and business.

Our deep experience and expertise empower you to navigate the complexities of the digital business landscape and help develop a comprehensive cybersecurity strategy to address your critical business priorities and optimise your security posture to keep you ahead of cyber threats.

Why Telstra International?

Expertise and Experience

Our deep experience and knowledge of security frameworks such as NIST, GDPR and SOC 2 enable us to design and implement robust and effective solutions that align with your industry, compliance requirements, and risk management objectives.

ISO/IEC 27001 Certified

bsi ISO/IEC 27001 Information Security Management CERTIFIED IS 764456

Our technology, delivery and support processes are certified to the ISO 27001 Information Security Management standard.

Strong Alliance Ecosystem

We bring together the strengths of our partner alliances with global technology leaders in our ecosystem to support you.

Proven Consulting Methodology

Our Telstra Purple "4D" Consulting Methodology has helped many global customers to strengthen their security posture. We have been named a 'Major Player' in the IDC MarketScape Worldwide Cybersecurity Consulting Services 2024 Vendor Assessment.

Discover how Telstra Managed Defender Endpoint Detection and Response (EDR) can help you to secure your business 24X7X365

Contact your Telstra account representative for more details.

✉ telstraenquiry@team.telstra.com   telstrainternational.com

2024.12.04 110 7M