



Product Brochure

Essential 8 Scorecard

Continuous cyber risk
measurement & reporting

► Continuous cyber risk measurement & reporting

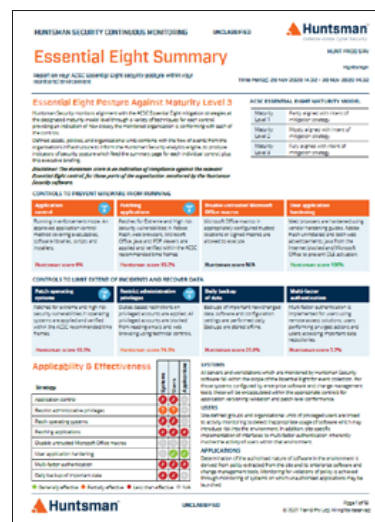
“If you can measure it,
you can manage it.”

The Essential 8 Scorecard measures the effectiveness of your organisation's security controls against the Essential Eight Framework; eight key cyber security strategies said to be the most effective protection against various cyber threats.



Essential 8 Scorecard
Continuous Cyber Risk Measurement

“The Essential 8 Scorecard provides measurement, and enables management, of cyber risk.”



“ The Essential 8 Scorecard delivers a continuous view of your cyber posture against the Essential Eight security controls ”

► What the Essential 8 Scorecard delivers

The Essential 8 Scorecard provides measurement, and enables management, of cyber risk. It delivers:

- Determination of your environment's maturity level against the Essential Eight Framework
- Essential Eight policy coverage across your environment
- Continuous monitoring of the environment against the Essential Eight Framework
- Real-time alerting of Essential Eight non-compliance
- A live dashboard displaying compliance and risks against each of the eight controls
- Automatically generated and distributed reports – Operational Controls Report and Executive Summary Report
- Trend reporting – to track and monitor performance over time

The Essential 8 Scorecard provides an objective, robust enterprise wide view of cyber risk, answering three fundamental questions:

- 1** **WHAT** is the quantitative measure of my organisation's exposure to cyber risk?
- 2** **WHY** is the performance as it is?
- 3** **HOW** can I reduce the risk?

► Essential 8 Scorecard – how it works

The Essential 8 Scorecard delivers a continuous view of your cyber posture against the Essential Eight security controls. It automatically gathers data from ongoing security operations, through direct connections and configuration interfaces; determining coverage, identifying weak points, policy failures and vulnerabilities against each of the controls.

► The Eight Key Security & Risk Controls and why they are important

The table below is sourced from the Australian Cyber Security Centre (ACSC). It explains each of the eight controls and why they are important.

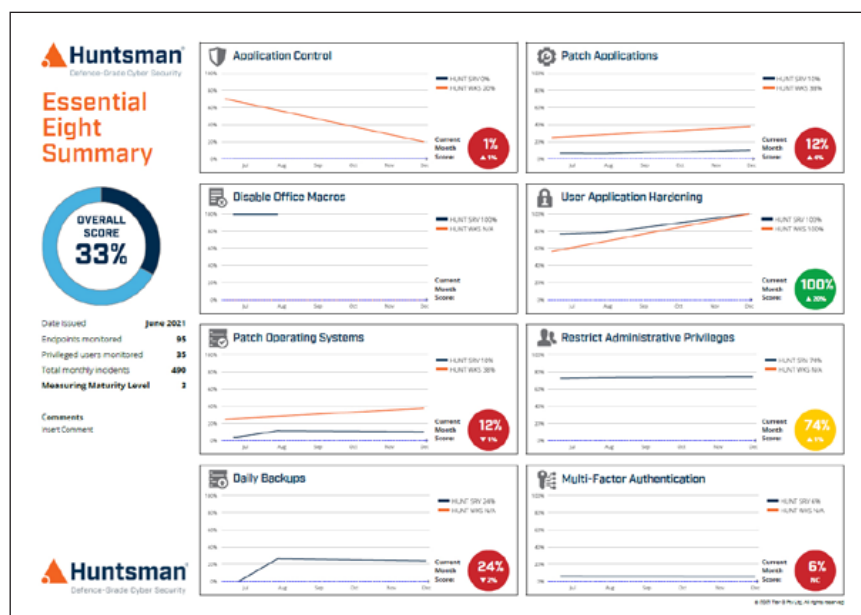
Mitigation strategies to prevent malware delivery and execution	
	<p>Application control to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.</p> <p>Why: All non-approved applications (including malicious code) are prevented from executing.</p>
	<p>Configure Microsoft Office macro settings to block macros from the internet and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.</p> <p>Why: Microsoft Office macros can be used to deliver and execute malicious code or systems.</p>
	<p>Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' security vulnerabilities within 48 hours. Use the latest version of applications.</p> <p>Why: Security vulnerabilities in applications can be used to execute malicious code on systems.</p>
	<p>User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet.. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.</p> <p>Why: Flash, ads and Java are popular ways to deliver and execute malicious code on systems.</p>
Mitigation strategies to limit the extent of cyber security incidents	
	<p>Restrict administrative privileges to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.</p> <p>Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.</p>
	<p>Multi-factor authentication including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.</p> <p>Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.</p>
	<p>Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' security vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.</p> <p>Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.</p>
Mitigation strategies to recover data and system availability	
	<p>Regular backups of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.</p> <p>Why: To ensure information can be accessed again following a cyber security incident (e.g. a ransomware incident).</p>

► How the Essential 8 Scorecard supports all your stakeholders

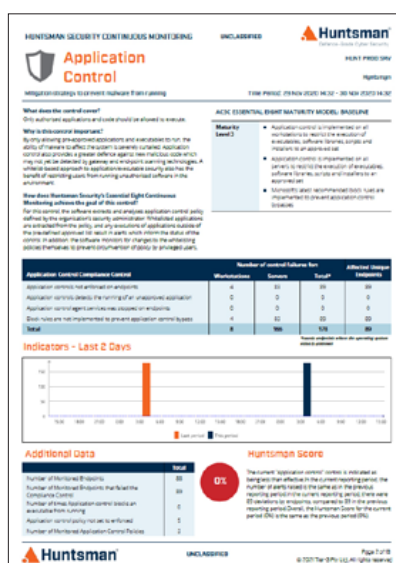
Whether you are a CIO, Risk Manager, Information Security Manager or a Security Analyst, the Essential 8 Scorecard can help develop your organisation's cyber resilience:

CIO & Risk Managers

Provides automated reports that give objective metrics of latest cyber posture, maturity level against the Essential Eight Framework as well as trend reports showing performance over time.



Essential 8 Scorecard – Trend Report



Essential 8 Scorecard – Application Control Report

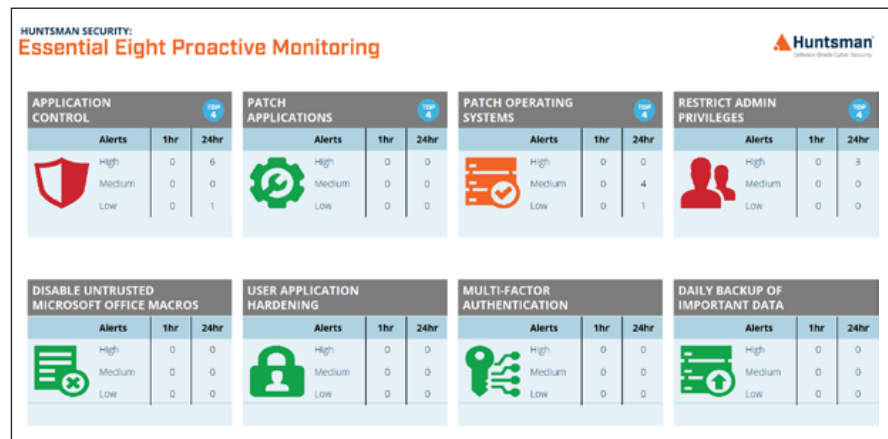
Information Security Managers

In addition to the reports provided to management, Information Security Managers will receive reports detailing the performance metrics for each of the Essential Eight mitigation strategies.

“ Whether you are a CIO, Risk Manager, Information Security Manager or a Security Analyst the Essential 8 Scorecard can help develop your organisation’s cyber resilience ”

Security Analysts

The cyber ops team is provided with an operational dashboard showing real-time performance of the Essential Eight controls. In addition to the real-time dashboards showing compliance to the controls, security analysts will receive alerts when non-compliance occurs. This will allow prioritisation of tasks with the greatest risk exposure.



Essential 8 Scorecard – Operational Dashboard

► How the Essential 8 Scorecard fits into your operation

The Essential 8 Scorecard provides a real-time solution that measures your security KPIs against the risk mitigation strategies of the Essential Eight. By passively gathering data from existing operational and system data sources, the Essential 8 Scorecard automatically highlights weak controls, policy failures and vulnerabilities within the environment.

► The importance of objective, quantitative measurement

The functionality of the Essential 8 Scorecard is formed on the ACSC Essential Eight Security controls, a framework developed to support the resilience of Australian government departments. The framework, combined with the scorecard technology, delivers an objective, quantitative measure of cyber risk to benchmark and track your organisation’s cyber risk.

► Cyber Risk Management

The Essential 8 Scorecard provides a continuous view of cyber risk:

- Determines your environment's maturity level against the Essential Eight Framework
- Live dashboard displaying compliance against each of the eight controls
- Real-time alerting of non-compliance
- Automatically generated and distributed reports – Operational & Management
- Trend reporting – to track and monitor performance over time

Product Features	Essential 8 Scorecard
Visibility	
Continuous Monitoring	✓
Live Dashboard	✓
Covers multiple Domains	✓
Policy coverage foot print	✓
Reporting Capabilities	
Automatically generate and distribute reports	✓
Weekly Control reports	✓
Monthly Executive Summary	✓
Trend reporting	✓
Provides basis for annual reporting obligations	✓
ACSC Maturity level determination (0-3)	✓
Benchmarks against ACSC Maturity Level 3	✓
Alerts when non-compliance occurs	✓
Installation	
Agentless install	✓
Integration with non-standard data sources	✓
Multi-tenancy supported	✓
Upgrades to maintain compliance with ACSC recommendations for Essential Eight	✓
Product Support	
Phone/Email	✓
Onsite	✓

Talk to Huntsman Security about measuring your cyber risk

For a more detailed discussion on measuring cyber risk, please contact the appropriate office listed below.

▶ About Huntsman Security

Since 1999, Huntsman Security has been on the cutting-edge of cyber security software development, serving some of the most sensitive and secure intelligence, defence and criminal justice environments in the world.



HUNTSMAN | TIER-3 PTY LTD

ASIA PACIFIC

t: +61 2 9419 3200

e: info@huntsmansecurity.com

Level 2,
11 Help Street
Chatswood NSW 2067

EMEA

t: +44 845 222 2010

e: ukinfo@huntsmansecurity.com

7-10 Adam Street,
Strand
London WC2N 6AA

NORTH ASIA

t: +81 3 5953 8430

e: info@huntsmansecurity.com

GINZA EAST SQUARE 4F
3-12-7 Kyobashi Chuoku, Tokyo
Japan 104-003



huntsmansecurity.com



linkedin.com/company/tier-3-pty-ltd



twitter.com/Tier3huntsman