Product Brochure

Essential 8 Scorecard

Continuous Cyber Risk Measurement

Huntsman®
Defence-Grade Cyber Security

Continuous Cyber Risk Measurement

“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 8 Framework; eight key cyber security strategies found to mitigate 85% of cyber threats.

Essential 8 Scorecard
Continuous Cyber Risk Measurement

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

Huntsman

> The Essential 8 Scorecard delivers a continuous view of your cyber posture against the Essential 8 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 8 Framework
- Essential 8 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 8 security controls. It automatically gathers data from ongoing security operations and through direct connections and configuration interfaces to determine coverage, identify weak points, policy failures and vulnerabilities against each of the controls.

The Eight Key Security 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 delivery execution

Application whitelisting of approval/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. windows Script Host, PowerShell and HIA) and installers.

Why: All non-approved applications (including malicious code) are prevented from executing.

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 digitaly signed with a trusted certificate.

Why: Microsoft Office macros can be used to deliver and execute malicious code or systems.

Patch applications e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.

Why: Security vulnerabilities in applications can be used to execute malicious code on ssystems.

User application hardening. Configure web browsers to block Flash (ideally uninstall it), ads and Jave on the internet.. Disable unneeded features in Microsfy Office (e.g. OLE), web browsers and PDF viewers.

Why: Flash, ads and Java are popular ways to deliver and execute malicious code on systems.

Mitigation strategies to limit the extent of cyber security incidents

Restrict administrative privileges to operate systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.

Why: Admin accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.

Multi-factor authentication including for VPNs, RDP, SSH and other remove access, and for all users when they perform a privileged action or access an important (sensitive/high-availibility) data repository.

Why: Stronger user authentication makes it harder for adversaries to access sensitive information and systems.

Patch operating systems. Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.

Why: Security vulnerabilities in operating systems can be used to further the compromise of systems.

Mitigation strategies to recover data and system availabilty

Daily backups of important new/changd data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Why: To ensure information can be accessed again following a cyber security incident (e.g. a ransomware incident).

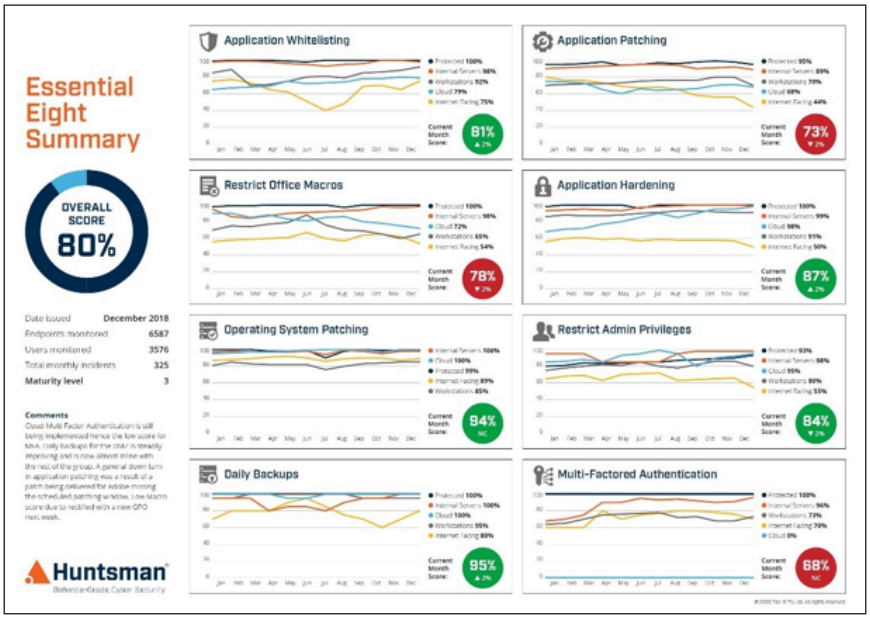
Huntsman®

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

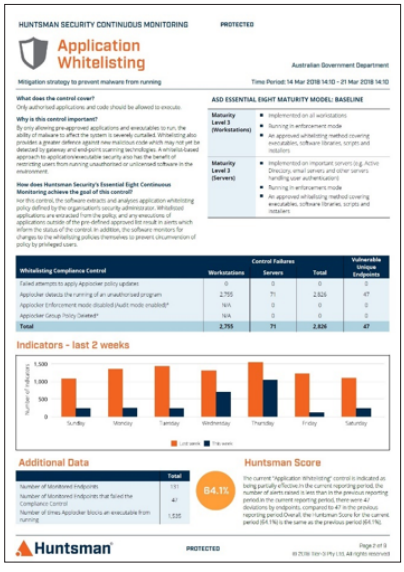
Provides automated reports that give objective metrics of latest cyber posture, maturity level against the Essential 8 Framework as well as trend reports showing performance over time.



Essential 8 Scorecard – Trend 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 8 mitigation strategies in relation to the Essential 8 Framework.



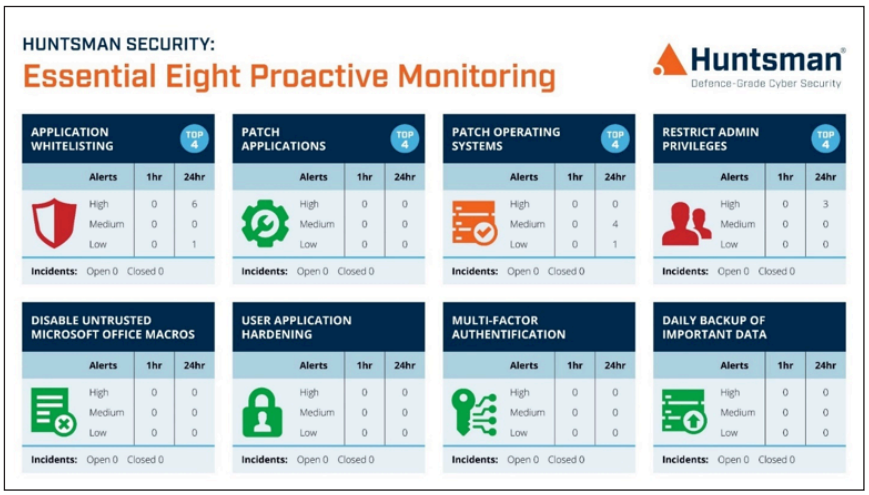
Essential 8 Scorecard – Application Whitelisting Report

Huntsman®

> “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 8 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 8. 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 8 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 versus Cyber Risk Auditing

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

- Determines your environment's maturity level against the Essential 8 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

If you'd prefer to have a simple, point-in-time snapshot of your organisation's cyber security posture, or if you are looking for an auditing tool, then the Essential 8 Auditor could be the solution for you. The table below shows the functionality of both products:

Product Features	Essential 8 Auditor	Essential 8 Scorecard
Visibility		
Continuous Monitoring		✓
Immediate Audit	✓	
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		
Self-Install	✓	
Agentless install	✓	✓
Integration with non-standard data sources		✓
Multi-tenancy supported		✓
Upgrades to maintain compliance with ACSC recommendations for Essential 8	✓	✓
Product Support		
Phone/Email	✓	✓
Onsite		✓

*Each individual domain measured separately.

Huntsman®

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

Huntsman Security is the trading name of Tier-3 Pty Ltd. The technology's heritage lies in delivering a key foundation stone of the cyber security risk management, monitoring and response capability in some of the most secure and sensitive environments within the intelligence, defence and criminal justice networks across the world, where Huntsman Security solutions are deployed and accredited to the highest security levels.

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**

Awajicho Ekimae Building 5F
1-2-7 Kanda Sudacho
Chiyodaku, Tokyo 101-0041

huntsmansecurity.com linkedin.com/company/tier-3-pty-ltd twitter.com/Tier3huntsman