Product Brochure

Essential 8 Auditor

Automated Cyber Risk Auditing

Huntsman®
Defence-Grade Cyber Security

Automated Cyber Risk Auditing

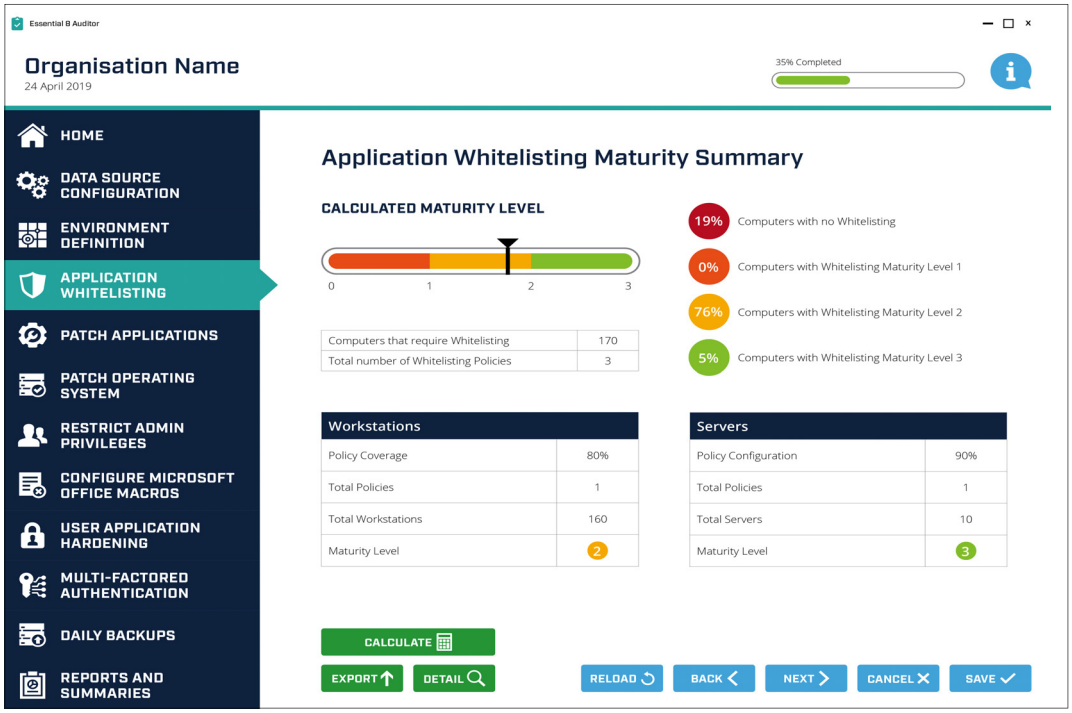
Objective measurement of cyber maturity

The Essential 8 Auditor provides an immediate view of an organisation's security controls' effectiveness against the Essential 8 Framework; eight key cyber security strategies found to mitigate 85% of cyber threats.

Essential 8 Auditor
Executes a Cyber Risk Audit

> "The Essential 8 Auditor delivers an immediate view of your cyber posture"

Huntsman



Essential 8 Auditor – Application Whitelisting Summary

What the Essential 8 Auditor delivers

The Essential 8 Auditor quickly and objectively answers the question "what is my organisation's cyber posture?"

- An immediate audit of risk and compliance to Essential 8 security controls
- Determination of your environment's maturity level against the Essential 8 Framework
- Compliance against Essential 8 maturity level 3
- Essential 8 policy coverage across your environment
- The basis for compliance reporting & annual attestations

Essential 8 Auditor – how it works

The Essential 8 Auditor delivers an immediate view of your cyber posture against the Essential 8 security controls. It automatically gathers data from ongoing security operations and through direct connections to systems and configuration interfaces to determine coverage, identify weak points, policy failures and vulnerabilities against each of the controls.

Ease of installation

The Essential 8 Auditor is self-installed agentless software making it quick and simple to deploy, when convenient to you.

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 JAve 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 'key to the kingdom'. Adversaries use these accounts to gain full access to information nd systems.

Multi-factor authentication including for VPNs, RDP, SSH and other remove acces, 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).

> "The functionality of the Essential 8 Auditor was created to measure compliance to the ACSC Essential Eight security controls"

Uses for the Essential 8 Auditor

The Essential 8 Auditing tool can be used for a number of different purposes:

- Internally, to determine an objective measure of cyber risk exposure
- Internally, forms the baseline for Annual Compliance reporting and Cyber Risk Attestations
- Auditing tool for Security Consultants, Auditors and Risk & Compliance Managers

The importance of objective, quantitative measurement

The functionality of the Essential 8 Auditor was created to measure compliance to the ACSC Essential Eight security controls, a framework developed to support the resilience of Australian government departments. The framework, combined with the Essential 8 Auditor technology delivers an objective, quantitative measure of cyber risk to benchmark an organisation's cyber risk.

Moving from Cyber Risk Measurement to include Management

The Essential 8 Auditor provides a simple, immediate view of an organisation's cyber security posture. If you want to move to continuous measurement and management then the Essential 8 Scorecard could be the solution for you. Continuous monitoring of the environment enables additional deliverables:

- Real-time alerting of non-compliance and risk
- A live dashboard displaying compliance 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

Huntsman®

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.

Talk to Huntsman Security about measuring your cyber risk

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

Huntsman®

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