# Measuring Your Cyber Security Posture

The Huntsman Security Scorecard continuously measures your cyber security posture across a range of key security performance indicators. The eight controls identified are as a result of analysis of organisations that have succumbed to cyber attacks and malware.

The Security Scorecard focuses on the eight controls that have been found to have the highest impact on preventing a cyber attack and improving your ability to recover from one.

Measuring control effectiveness is a key element of any risk management process.

**“ You cannot manage what you cannot measure ”**

**Between October 2015 -December 2017 the UK NCSC recorded 34 significant cyber attacks.**

**The cyber threat to UK business, 2017-18, NCSC & NCA**

**Australia’s Notifiable Data Breaches (NDB) Scheme received 242 notifications in its first 3 months.**

**OAIC Notifiable Data Breaches Quarterly Statistics Report 1 April – 30 June 2018**

**Many of these cyber threats could have been prevented, or at least the impact reduced, by adopting basic cyber security measures.**

## The 8 essential controls

| | | |
|---|---|---|
| Top 4 | • Application white listing<br>• Patching applications<br>• Patch operating systems<br>• Restrict administrative privileges | **These 4 controls alone have been assessed to reduce the likelihood of suffering a cyber attack by up to 85%** |
| + | • Daily back up of data<br>• Multifactor authentication | These controls plus the Top 4 are key recommendations from the **NCSC** and the **ACSC** for protection against the most common cyber attacks |
| ++ | • Disable untrusted Microsoft Office macros<br>• User application hardening | Implementing these controls helps keep your business safe from users falling victim to cyber attacks targeting endpoints |

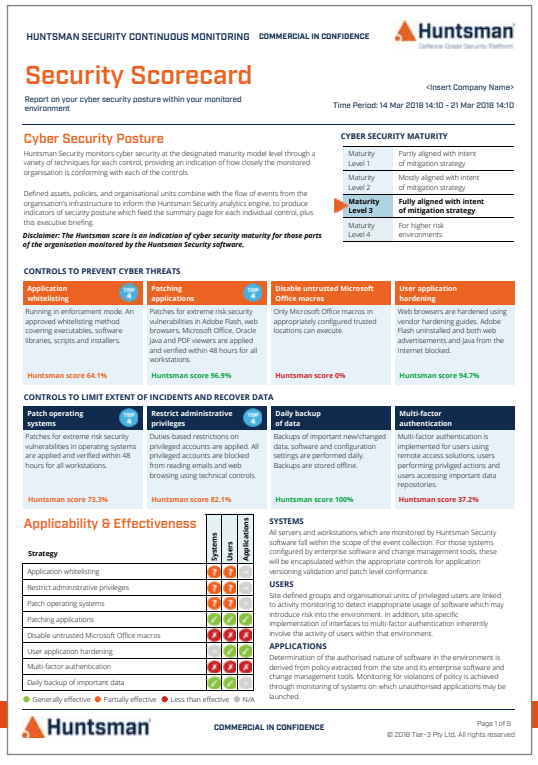
## Security Posture at a glance

To help mitigate cyber security risks the Security Scorecard is a powerful toolset that provides:

- Executive Summary Report and detailed control reports
- Clear Visibility of current security posture
- Guidance on where vulnerabilities exist

The Security Scorecard gives you a measure of the efficiency and effectiveness of your security controls and reveals the direction your cyber security posture is moving.

**For more information:**
https://www.huntsmansecurity.com/products/security-scorecard/



HUNTSMAN SECURITY CONTINUOUS MONITORING COMMERCIAL IN CONFIDENCE

Huntsman

Security Scorecard

Report on your cyber security posture within your monitored environment

<Insert Company Name>

Time Period: 14 Mar 2018 14:10 - 21 Mar 2018 14:10

Cyber Security Posture

Huntsman Security monitors cyber security at the designated maturity model level through a variety of techniques for each control, providing an indication of how closely the monitored organisation is conforming with each of the controls.

Defined assets, policies, and organisational units combine with the flow of events from the organisation's infrastructure to inform the Huntsman Security analytics engine, to produce indicators of security posture which feed the summary page for each individual control, plus this executive briefing.

*Disclaimer: The Huntsman score is an indication of cyber security maturity for those parts of the organisation monitored by the Huntsman Security software.*

CYBER SECURITY MATURITY

| | |
|---|---|
| Maturity Level 1 | Partly aligned with intent of mitigation strategy |
| Maturity Level 2 | Mostly aligned with intent of mitigation strategy |
| Maturity Level 3 | Fully aligned with intent of mitigation strategy |
| Maturity Level 4 | For higher risk environments |

CONTROLS TO PREVENT CYBER THREATS

| Application whitelisting | Patching applications | Disable untrusted Microsoft Office macros | User application hardening |
|---|---|---|---|
| Running in enforcement mode. An approved whitelisting method covering executables, software libraries, scripts and installers. | Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Oracle Java and PDF viewers are applied and verified within 48 hours for all workstations. | Only Microsoft Office macros in appropriately configured trusted locations can execute. | Web browsers are hardened using vendor hardening guides. Adobe Flash uninstalled and both web advertisements and java from the Internet blocked. |
| Huntsman score 64.1% | Huntsman score 96.9% | Huntsman score 0% | Huntsman score 94.7% |

CONTROLS TO LIMIT EXTENT OF INCIDENTS AND RECOVER DATA

| Patch operating systems | Restrict administrative privileges | Daily backup of data | Multi-factor authentication |
|---|---|---|---|
| Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all workstations. | Duties-based restrictions on privileged accounts are applied. All privileged accounts are blocked from reading emails and web browsing using technical controls. | Backups of important new/changed data, software and configuration settings are performed daily. Backups are stored offline. | Multi-factor authentication is implemented for users using remote access solutions, users performing privileged actions and users accessing important data repositories. |
| Huntsman score 73.3% | Huntsman score 82.1% | Huntsman score 100% | Huntsman score 37.2% |

Applicability & Effectiveness

| Strategy | Systems | Users | Applications |
|---|---|---|---|
| Application whitelisting | ● | ● | ○ |
| Restrict administrative privileges | ● | ● | ○ |
| Patch operating systems | ● | ● | ○ |
| Patching applications | ✓ | ✓ | ✓ |
| Disable untrusted Microsoft Office macros | ✗ | ✗ | ✗ |
| User application hardening | ○ | ✓ | ✓ |
| Multi-factor authentication | ✗ | ✗ | ✗ |
| Daily backup of important data | ✓ | ✓ | ○ |

● Generally effective ● Partially effective ● Less than effective ○ N/A

SYSTEMS

All servers and workstations which are monitored by Huntsman Security software fall within the scope of the event collection. For those systems configured by enterprise software and change management tools, these will be encapsulated within the appropriate controls for application versioning validation and patch level conformance.

USERS

Site-defined groups and organisational units of privileged users are linked to activity monitoring to detect inappropriate usage of software which may introduce risk into the environment. In addition, site-specific implementation of interfaces to multi-factor authentication inherently involve the activity of users within that environment.

APPLICATIONS

Determination of the authorised nature of software in the environment is derived from policy extracted from the site and its enterprise software and change management tools. Monitoring for violations of policy is achieved through monitoring of systems on which unauthorised applications may be launched.

Huntsman COMMERCIAL IN CONFIDENCE

Page 1 of 9



Huntsman®
Defence-Grade Cyber Security

## The 8 essential controls

Each of the controls is reported in detail on a weekly basis and is automatically compared to the previous week so you can see if your security posture is going in the right direction. The controls fit into two categories:

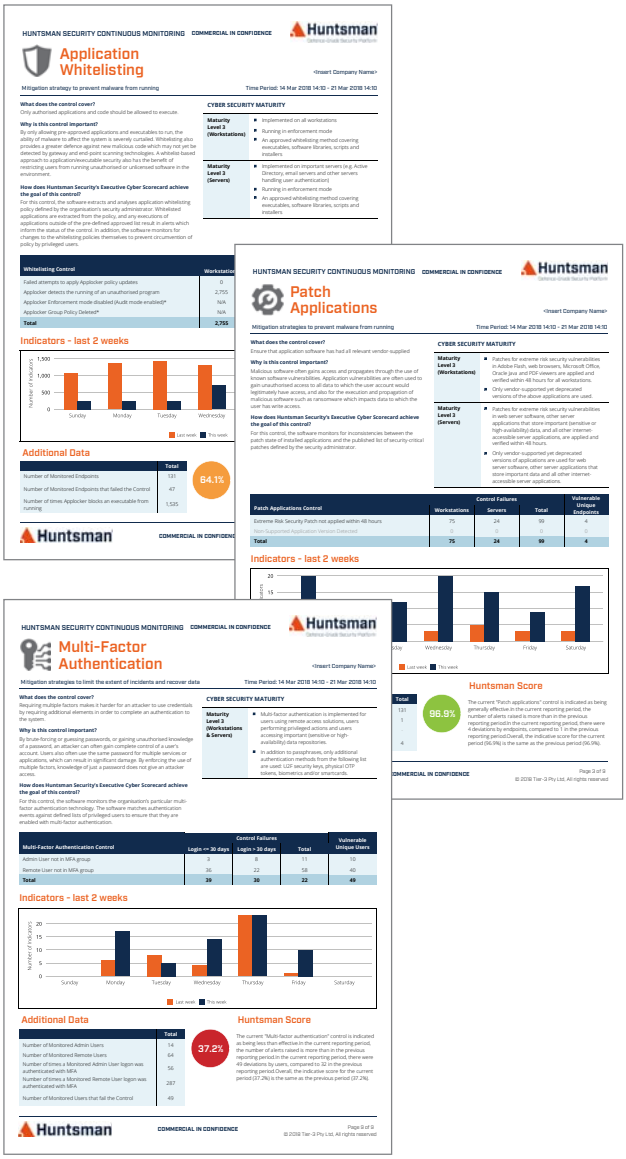
### Controls to mitigate against cyber threats:

- Application Whitelisting – running in enforcement mode.
- Patching Applications – for extreme risk security vulnerabilities in Adobe Flash, web browsers etc.
- Disable untrusted Microsoft Office Macros
- User Application Hardening

### Controls to limit the extent of incidents and recover data:

- Patch operating systems – patch for extreme risk security vulnerabilities with 48 hours.
- Restrict administrative privileges – duties-based restrictions on privileged accounts.
- Daily back-up of data
- Multi-factor authentication – for users performing privileged actions, accessing important data, remote access etc.

**Implementation of these eight controls improves cyber resilience, minimises the likelihood of an attack being successful and increases your ability to recover from one in real terms.**





## Status Dashboard

Monitoring of your environment including on-premise, cloud and hybrid.

Pre-defined alerts, dashboards, queries and reports.