



Product Brochure

SmartCheck

Measure your cyber risk

 **Huntsman**[®]

▶ SmartCheck

Our SmartCheck application rapidly provides automated risk assessment by monitoring 12 Safeguards across the cyber-attack sequence that prevent and limit ransomware, other malware and cyber attacks. It can be deployed to interrogate and protect your systems, staff and third-party suppliers across your organisation, on-site and in remote or third-party locations.

Why organisations choose our SmartCheck application **TO FORTIFY THEIR CYBER RISK MANAGEMENT**



AUTOMATED RISK ASSESSMENT & EXEC-LEVEL VISIBILITY

Connects to your security controls, to automatically generate an informative cyber risk report in minutes.



12 SAFEGUARDS ALIGNED WITH NCSC GUIDANCE

Gathers and assesses information from a set of security controls, to assess your cyber resilience and inform your risk management activities.



RELIABLE EVIDENCE-BASED RISK REPORTING IN MINUTES

Automated assessment of your mitigating controls, risk management steps, and measurement for ongoing baseline monitoring and improvements.

▶ Key Features

| A quick look at the SmartCheck key features

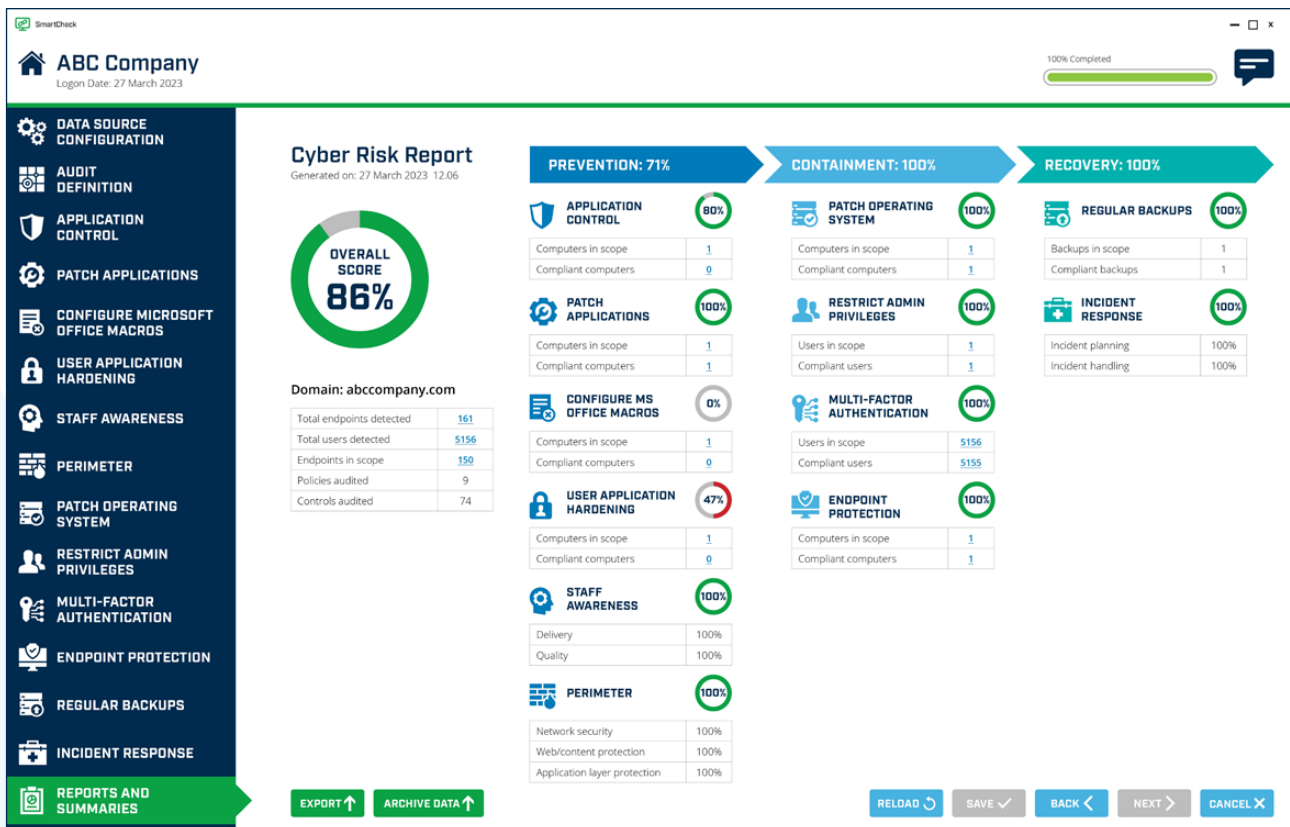
Visibility	
On-demand operation	✓
Measurement by control and in a consolidated view	✓
Visibility of the performance level of each technical control	✓
Accurate, evidence-based ransomware readiness assessment	✓
Live dashboards and data export available	✓
Aligned to NCSC & NIST ransomware mitigation guidance	✓
Reporting Capabilities	
Automates security effectiveness reports	✓
Executive security summary reports	✓
"To-do" list highlighting potential vulnerabilities for remediation	✓
Cyber risk level determination	✓
Status report of prevention, containment and recovery defences	✓
Installation	
Light weight	✓
Agentless	✓
Up and running in minutes	✓

▶ On-demand ransomware readiness rating

| Reporting, at any point in time

At any time, your team can run SmartCheck to:

- Verify your key cyber security controls and security posture, revealing the state of your ransomware readiness
- Know how well you are protected across multiple attack vectors, and give you a clear picture of the effectiveness of your prevention, containment and recovery strategies
- Check on the progress of security improvements, report on ongoing security operations, and stay responsive to changing security risks - as often as you need



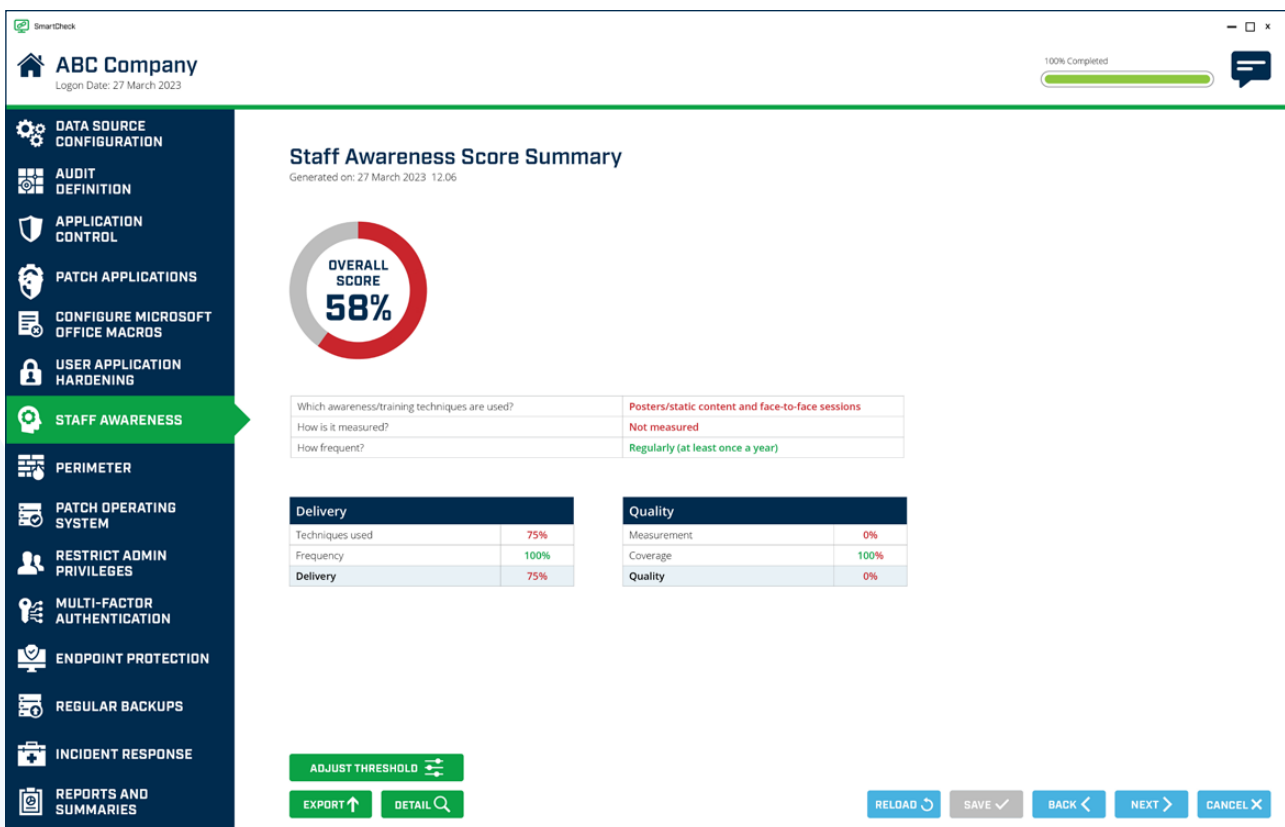
Cyber Risk Report

Automated reporting on staff and system readiness

Visibility across the organisation

SmartCheck provides:

- A discrete performance score for the effectiveness of each safeguard. It automatically provides clear visibility of risks needing mitigation to improve your cyber posture.
- A rapid assessment of the approach, frequency and coverage of your staff cyber-awareness program
- Recalculated maturity levels of each safeguard to reflect a changed risk situation and inform cyber risk management efforts
- Automatically aggregated performance scores to provide a summary cyber risk readiness rating for the enterprise



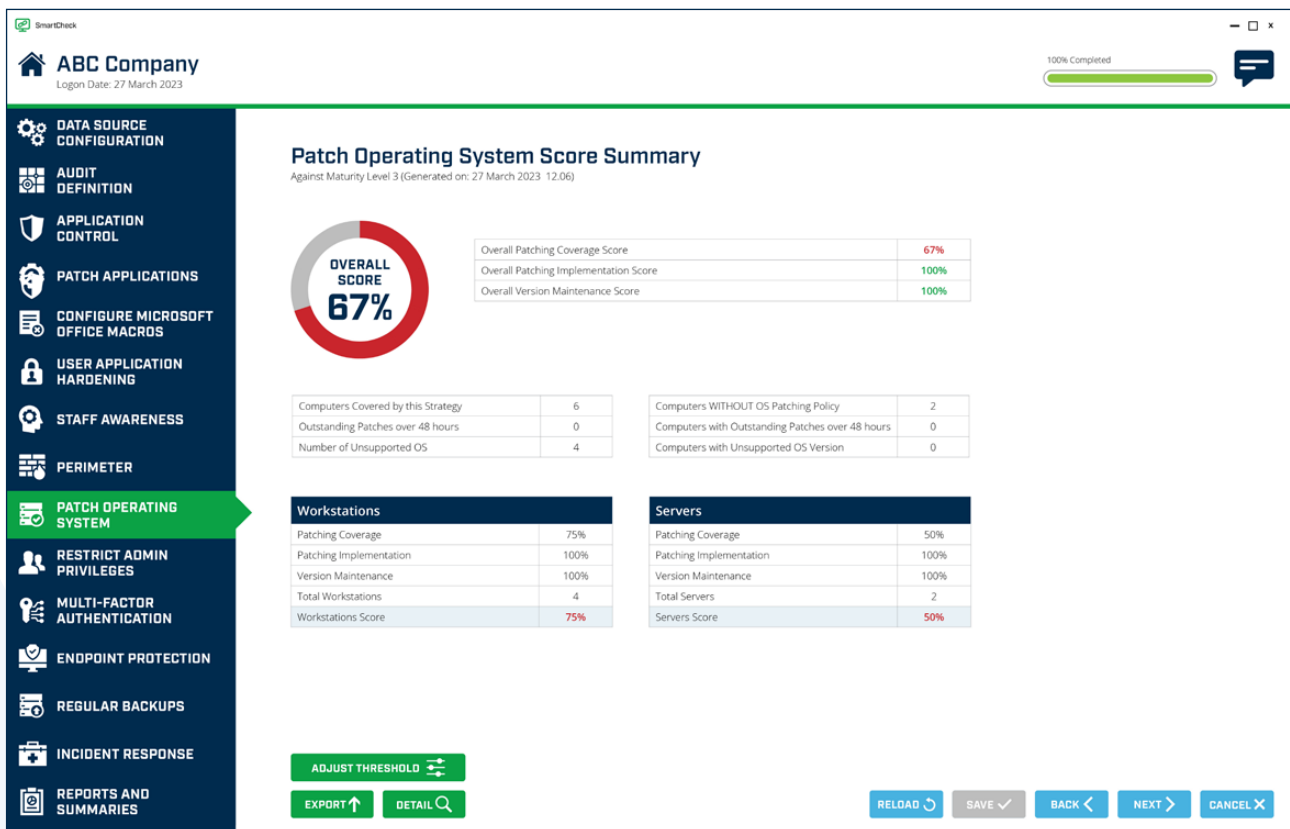
Staff Awareness Score Summary

▶ Reliable evidence-based assessment

■ Built-in, with full transparency

SmartCheck provides:

- Visibility and oversight of your key ransomware safeguards based on their configuration, coverage and operational telemetry – to highlight vulnerabilities or settings that require adjustment or mitigation
- Quick and quantitative assessments to identify and prioritise gaps requiring mitigation efforts to maintain your cyber resilience



Selected Computers

Risk management for cyber risk in minutes

Automated to avoid time-intensive manual reviews

SmartCheck enables you to:

- Quantitatively baseline your cyber security safeguards to quickly create a “to-do” list of vulnerabilities for attention
- Guide the quality improvement of your ransomware risk management by improving security control performance in all phases of the cyber-attack sequence
- Quantify risks, to confirm the relative effectiveness of your security controls and understand the state of your cyber resilience

The screenshot shows the SmartCheck interface for ABC Company. The left sidebar contains a navigation menu with icons and labels for various security controls. The main content area displays the 'Multi-Factor Authentication Score Detail Result' for a maturity level of 3, generated on 27 March 2023 at 12:06. A progress bar at the top right indicates '100% Completed'. The dashboard includes several tables summarizing account security metrics.

Navigation Menu:

- DATA SOURCE CONFIGURATION
- AUDIT DEFINITION
- APPLICATION CONTROL
- PATCH APPLICATIONS
- CONFIGURE MICROSOFT OFFICE MACROS
- USER APPLICATION HARDENING
- STAFF AWARENESS
- PERIMETER
- PATCH OPERATING SYSTEM
- RESTRICT ADMIN PRIVILEGES
- MULTI-FACTOR AUTHENTICATION**
- ENDPOINT PROTECTION
- REGULAR BACKUPS
- INCIDENT RESPONSE
- REPORTS AND SUMMARIES

Multi-Factor Authentication Score Detail Result
 Against Maturity Level 3 (Generated on: 27 March 2023 12:06)

Total Number of Accounts with MFA	439
Authentication Factors Used : Passwords with six or more characters, Universal 2nd Factor Security Keys	Compliant

Total Number of Privilege User Accounts	27	Non-Compliant* Privilege User Accounts	7
Total Number of Privilege Service Accounts	9	Non-Compliant* Privilege Service Accounts	4
Total Number of Privilege Accounts	36	Non-Compliant* Privilege Accounts	11

Total Number of Remote User Accounts	0	Non-Compliant* Remote User Accounts	0
Total Number of Remote Service Accounts	0	Non-Compliant* Remote Service Accounts	0
Total Number of Remote Accounts	0	Non-Compliant* Remote Accounts	0

Total Number of Privilege and Remote Accounts	36	Non-Compliant* Privilege and Remote Accounts	11
---	----	--	----

*Non-Compliance against Maturity Level 3 is when a Privilege or Remote User is not covered by MFA using: passwords with six or more characters, Universal 2nd Factor security keys, physical on-time password tokens, biometrics or smartcards.

Privilege Users Accounts with MFA	20	Privilege Users Accounts without MFA	7
Privilege Service Accounts with MFA	5	Privilege Service Accounts without MFA	4
Privilege Accounts with MFA	25	Privilege Accounts without MFA	11

Remote Users Accounts with MFA	0	Remote Users Accounts without MFA	0
Remote Service Accounts with MFA	0	Remote Service Accounts without MFA	0
Remote Accounts with MFA	0	Remote Accounts without MFA	0

Buttons at the bottom: EXPORT ↑, EXPORT RAW DATA ↑, BACK <

Score Summary



Explore the features >



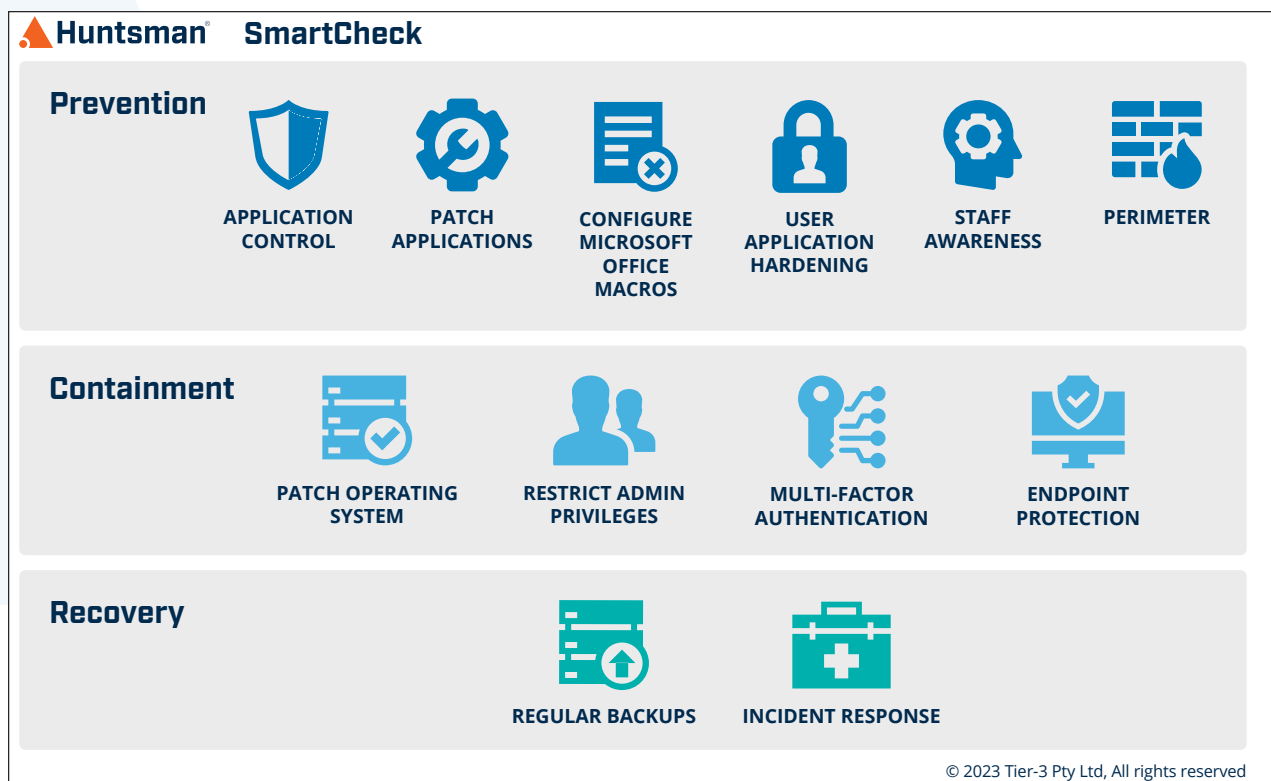
Request a demo >

▶ How SmartCheck works

No single cyber security control can protect against every situation. The concept of defence-in-depth anticipates multiple independent security controls operating in concert to protect you across the attack sequence. Cyber-risk readiness or resistance is best achieved when the effectiveness of these security controls is maintained across each of the prevention, containment and recovery phases.

With its comprehensive Attack Surface Management (ASM) capabilities, SmartCheck automatically verifies your IT assets, measures vulnerabilities and reports any areas of changing cyber risk.

Accurate, reliable and quick measurement to maintain the effectiveness of the 12 Safeguards ensures the risk of a successful ransomware or other malware attack is kept to a minimum. Beyond your annual audit, SmartCheck for can be used on-demand to quickly provide comprehensive cyber readiness reports as and when required.



| Do you have visibility of your ransomware readiness?







Visibility of the effectiveness of your key security controls is an essential element in managing organisational ransomware risk.

▶ 12 Safeguards aligned with UK NCSC & US NIST guidance





| For Prevention, Containment and Recovery

Accurate, reliable and quick measurement to maintain the effectiveness of the 12 Safeguards ensures the risk of a successful ransomware attack is kept to a minimum.



Prevention

	Application control. Only approved software should run on a computer system. This safeguard supports securing your systems by limiting what can run on devices across your organisation.
	Patch Applications. Applications must be regularly patched or updated to prevent intruders exploiting known vulnerabilities. This safeguard supports the identification of vulnerabilities and the application of relevant patches in a timely manner.
	Configure Microsoft Office Macros. Macro and document settings need correct configuration. This safeguard checks macros and settings to protect against malicious code.
	User Application Hardening. Effective security policies limit user access to active content and web code. This safeguard supports the implementation of application and browser controls.
	Staff awareness. Building an ongoing understanding by staff about cyber security threats, and mitigation strategies that minimise cyber-attacks, is vital. This safeguard is a checkpoint for ongoing staff awareness.
	Perimeter. Appropriately configured and regularly updated, perimeters / firewalls can limit access to, and use of, certain computer systems. This safeguard defends your network against unauthorised traffic.

Containment

	Patch Operating System. Fully patched operating systems are vital across every endpoint. This safeguard reduces the likelihood of malware or ransomware spreading across the network.
	Restrict admin privileges. Best-practice limits admin privileges, by allowing only those staff needing system access to do so, for specified purposes. This safeguard limits the number of users who can make significant changes to your systems.
	Multi-factor authentication. Requires multiple independent credentials to verify a user before they gain system access. This safeguard supports the management of user access (including remote users) to high sensitivity accounts and systems.
	Endpoint Protection. Anti-virus software is a vital part of any cyber security strategy. This safeguard supports the coverage of anti-virus software across every device within your organisation.

Recovery

	Regular backups. Securing data and system backups off-site, and testing recovery processes is crucial. This safeguard ensures important data, systems information and configurations are backed up and retained in a secure manner.
	Incident response. Validating that incident management plans exist, and are tested. This safeguard supports planning for a worst-case scenario and the use of your incident management playbook.

Want to find out more?

Request a demo of SmartCheck

Request a Demo

Or contact your local Huntsman Security office (listed below) to talk to one of our team today.

▶ 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