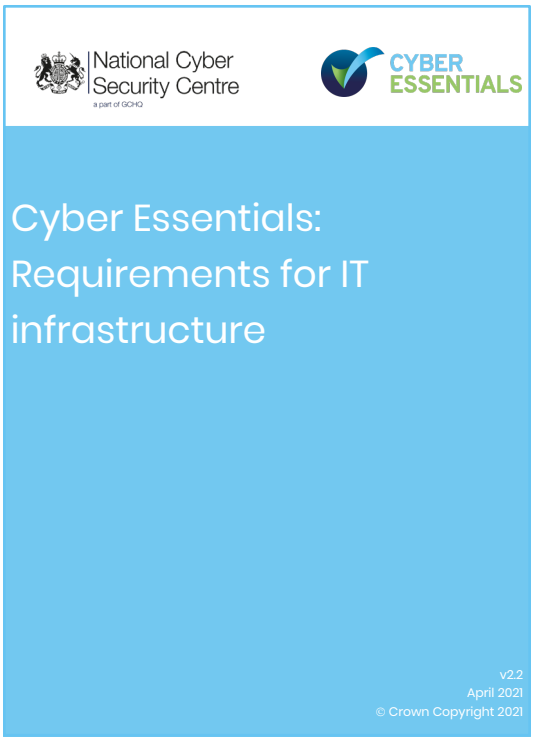

NCSC Cyber Essentials Plus

Alignment with Forescout

The Cyber Essentials certification scheme from the National Cyber Security Center (NCSC) helps you to guard your organisation against cyberattack. It's a simple but effective government-backed scheme that will help you protect your organisation, whatever its size, against a whole range of the most common cyberattacks. Cyber Essentials Plus uses the same framework, guidance and protections but requires a hands-on technical verification rather than a self-assessment.[1]

How Forescout helps

The Forescout® Platform continuously automates cyber security across your environment. Key capabilities that align with Cyber Essentials Plus include:

- Real-time discovery of all IP-connected devices
- Continuous assessment of security risk posture by device classification
- Complete and context-rich asset inventory across the entire enterprise
- Automated software updates, patch management and incident response

Key Components and Scope of Cyber Essentials Plus

COMPONENT	OBJECTIVE	APPLIES TO:
Firewalls	Ensure that only safe and necessary network services can be accessed from the Internet. Boundary firewalls should be supported by network controls (ACLs) and host-based firewall solutions.	▸ Boundary firewalls ▸ Desktops ▸ Laptops ▸ Servers
Secure Configuration	Ensure that computers and network devices are properly configured to reduce the level of inherent vulnerabilities and provide only the services required to fulfil their role.	▸ Application servers ▸ Infrastructure services ▸ Desktops, laptops ▸ Network infrastructure ▸ Mobiles and tablets
User Access Control	Ensure user accounts are assigned to authorised individuals only and provide access to only those applications, computers and networks actually required for the user to perform their role.	▸ Application servers ▸ Infrastructure services ▸ Desktops, laptops ▸ Network infrastructure ▸ Mobiles and tablets
Malware Protection	Restrict execution of known malware and untrusted software, to prevent harmful code from causing damage or accessing sensitive data.	▸ Desktops ▸ Laptops ▸ Mobile phones ▸ Tablets
Security Update Management	Ensure that devices and software are not vulnerable to known security issues for which fixes are available.	▸ Application servers ▸ Infrastructure services ▸ Desktops, laptops ▸ Network infrastructure ▸ Mobiles and tablets

COMPONENT	FORESCOUT PLATFORM	
	FUNCTIONALITY	**BUSINESS VALUE**
Firewalls	▸ Assess all devices to ensure a suitable host-based firewall is installed and functioning. ▸ Check and report on all running services and installed software for desktop, laptop and servers. ▸ Assess boundary firewalls for use of default credentials and settings (such as SNMP, Telnet, SSH). ▸ Monitor and visualise all traffic flow across the enterprise to provide assurance for firewall rule set. ▸ Alert (or block) traffic flows to and from the internet that violate expected behaviour. ▸ Integrate with NGFW's to allocate devices to specific firewall trust zones or rule sets.	▸ Ensure all connected devices have suitable host-based firewall installed and functioning. ▸ Gain complete visibility into all network traffic flows between all connected devices; and those to the internet.
Secure Configuration	▸ Assess all devices against a security baseline for their unique device classification. ▸ Assess devices for known vulnerabilities, natively or through integration with vulnerability assessment tools. ▸ Check and report on all running services and installed software for desktop, laptop and servers. ▸ Assess IoT, IoMT, IT and cloud devices for use of default or out-of-the box credentials. ▸ Assess network infrastructure for use of default credentials and settings (such as SNMP, Telnet, SSH). ▸ Integrate with mobile device management (MDM) solutions to discover and assess mobile phones and tablets.	Ensure all connected devices are uniquely assessed for their individual security requirements to remove any default or weak configuration and remediate misconfiguration and risk.
User Access Control	▸ Check and report on users' accounts in use on all desktop, laptop and servers. ▸ Leverage Activity Directory Group Membership to control access to resources or align control policies. ▸ Integrate with privilege access management solutions to monitor and control escalated access. ▸ Leverage user or device credentials to provide least privilege network access control policies. ▸ Overlay username or group membership to Network Traffic Flow Visualisation Matrix.	Align user to device context to gain a better understanding of the devices on your network and the users that are currently using them. Use this combined context to monitor traffic flows and communication patterns between users, the device they use and the applications, servers and services they interact with.
Malware Protection	▸ Assess all devices to ensure a suitable anti-malware (AV/EDR/EPP) solution is installed and functioning. ▸ Assess all devices to ensure the AV/EDR/EPP signatures are up to date. ▸ If available ensure a suitable vulnerability assessment tool is installed and has assess the device recently. ▸ Integrate with mobile device management solutions to discover and assess mobile phones and tablets. ▸ Quarantine or restrict high-risk or known compromised devices detected by the AV/EDR/EPP/VA tools.	▸ Ensure all connected devices have suitable security tools installed, functioning and up to date to minimise the risk of infection from malware. ▸ Automate Incident response to detected threats and prevent lateral spread of infections.
Security Update Management	▸ Assess all devices to ensure they are running a suitable and supported operating system. ▸ Check for critical patches and hotfixes to all operating systems ▸ Assess all devices to ensure suitable security tools are installed and patched correctly. ▸ Check and report on all running services and installed software for desktop, laptop and servers. ▸ Assess software and services for vulnerabilities and patch as required. ▸ Integrate with patch management tools or initiate remediation through control policies.	Orchestrate 3rd-party patch management tools and/or automate patch management and the deployment of suitable hotfixes, and/or agents to remove vulnerabilities and minimise risk posture.

1 https://www.ncsc.gov.uk/cyberessentials/overview
https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-2.pdf

Forescout Technologies, Inc.
Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591
Learn more at Forescout.com