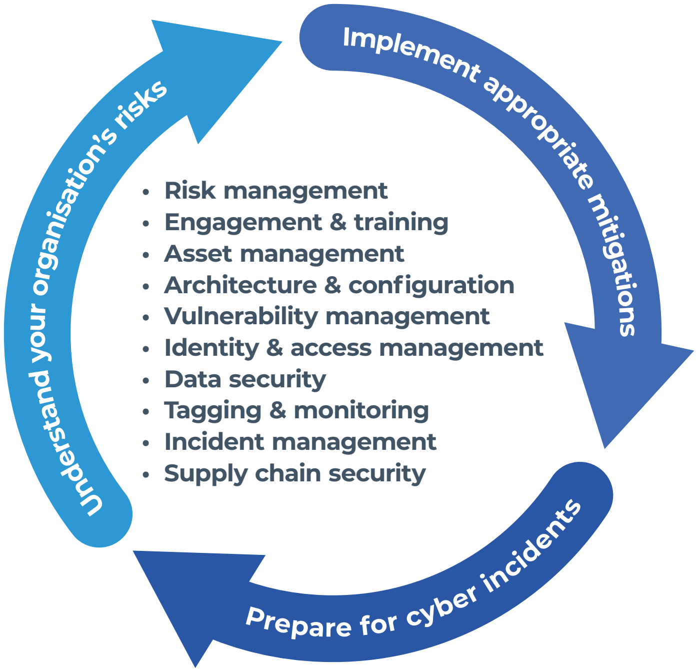
NCSC Top 10 Steps to Cyber Security

Compliance with Forescout

In 2022, the United Kingdom's National Cyber Security Centre (NCSC) updated their 10 Steps to Cyber Security to help medium to large organisations better understand and mitigate their cyber risk. The guidance addresses topics such as the widespread adoption of cloud services, the shift to mobile working and increasing threats such as ransomware and supply chain security. Compliance with the 10 Steps is designed to ensure that technology, systems and information are protected against the majority of cyberattacks.[1]

How Forescout helps

Digital transformation has led to explosive growth in IT, IoT, IoMT and OT/ICS assets connecting to organizational networks, all of which improve efficiency but also expand the cyberattack surface.



Understand your organisation's risks

Implement appropriate mitigations

Prepare for cyber incidents

- Risk management
- Engagement & training
- Asset management
- Architecture & configuration
- Vulnerability management
- Identity & access management
- Data security
- Tagging & monitoring
- Incident management
- Supply chain security

Either natively or by coordinating automated actions among security tools, the Forescout Continuum Platform supports many of the 10 Steps. It extends scarce IT and InfoSec resources with continuous, automated asset management, risk compliance, network segmentation, network access control and security orchestration across all connected assets, going above and beyond baseline security recommendations to provide a strong foundation for zero trust.

Overarching principles

Understand your organisation's risks

The Forescout Continuum Platform continuously identifies and mitigates risk across all connected assets in your digital terrain. For every connected device, it calculates a prioritized score based on configuration, function and behaviour. Factors include number and severity of vulnerabilities, open ports, internet exposure and operational criticality. By correlating risk scores with traffic flows between devices Forescout Continuum also assesses the blast radius to critical assets.

Implement appropriate mitigations

Once you have a good understanding of your risks, you can create control policies based on what risks need to be mitigated and what risks you're willing to accept. Forescout Continuum continuously identifies and mitigates risk across your digital terrain with automated remediation, network access control, segmentation and CMDB updates. It orchestrates policy-based actions among your security tools while also ensuring they are deployed, configured and working correctly.

Prepare for cyber incidents

Visibility is the foundation of cybersecurity – you can't protect what you can't see. Forescout Continuum automates the discovery, assessment and governance of all connected assets in your environment to minimize the attack surface and breach impact. By continuously monitoring every asset on your network and sharing collective insights among security products, Forescout enforces policies to drive the right automated actions and be prepared.

[1] 10 Steps to Cyber Security - NCSC.GOV.UK

SECURITY ACTION	FORESCOUT CONTINUUM PLATFORM CAPABILITIES
Risk management Take a risk-based approach to securing your data and systems.	▸ Continuously share in-depth device, user and network context for all managed and unmanaged assets ▸ Automate policy-based controls among security products to enforce network access, improve device compliance, implement network segmentation, remediate noncompliant devices, accelerate incidence response and contain threats
Engagement & training Collaboratively build security that works for people in your organisation.	▸ Train users on the Forescout Continuum Platform to optimize performance and outcomes, in alignment with the organisation’s engagement and training practices, as well as culture. ▸ Identify non-Forescout training gaps based on observed network behaviour our platform monitors
Asset management Know what data and systems you manage, and what business need they support.	▸ Continuously discover all IT, OT, IoT and IoMT devices upon connect, including what type of device is connecting, who is using it and where and how it is connecting ▸ Auto-classify and assess security posture of managed and unmanaged devices against security policies and external mandates ▸ Continuously sync all device information in your CMDB with rich context (function, relationships, criticality, dependencies) to serve as a single source of truth to manage asset lifecycles and optimize performance
Architecture & configuration Design, build, maintain and manage systems security.	▸ Align with the widely adopted NIST Cybersecurity Framework, designed to help organisations identify, protect, detect, respond and recover from threats ▸ Set the stage for zero trust security by automating enforcement of least-privilege access policies based on user, device, connection, posture and compliance for all cyber assets — with or without 802.1X, and without infrastructure upgrades or changes
Vulnerability management Keep your systems protected throughout their lifecycle.	▸ Automate information sharing and workflows with VM solutions to streamline threat detection and remediation ▸ Trigger real-time vulnerability scans and initiate patching and security updates ▸ Continuously monitor last vulnerability scan date for all endpoints and OS versions to ensure scans are being performed and all patches are applied within required timeframes
Identity & access management Control who and what can access your systems and data.	▸ Enforce network access control policies based on user, device and security posture ▸ Enforce segmentation policies that restrict access to sensitive resources when violations are detected yet allow critical operations to function ▸ Accelerate design, planning and deployment of context-aware segmentation across your terrain, facilitating policy design with interactive maps that visualize assets and traffic flows ▸ Simulate segmentation policies and monitor traffic flows to avoid business disruption
Data security Protect data where it is vulnerable.	▸ Automate policy-based control actions (network access, device compliance, segmentation, remediation, incident response) to help ensure only authorized systems and users are accessing systems and data ▸ Continuously monitor networks to help ensure only authorized communications occur between systems and users despite dynamic changes to enforcement points ▸ Help ensure only authenticated, compliant, verified hosts are on the network
Logging & monitoring Design your systems to be able to detect and investigate incidents.	▸ Help ensure central logging is functioning and scans log files to identify vulnerable and violated hosts ▸ Use 20 techniques to continuously monitor, detect both internal risks and external threats before they lead to incidents including rogue devices, misconfigurations, anomalous behavior, unwanted connectivity, open ports, etc. ▸ Leverage deep integration with leading IT and OT network switches, routers, wireless, access points, firewalls, VPN concentrators, and data center and cloud solution providers ▸ Use an advanced threat detection engine to analyze asset and communication data, cut through the noise and identify the most serious threats that require action ▸ Monitor communications, including DNS traffic outbound to the internet, and alert when anomalous or errant DNS requests are generated ▸ Continuously monitor networks to help ensure only authorized communications occur between systems and users
Incident management Plan your response to cyber incidents in advance.	▸ Share device and network information and automate workflows across security tools to enable and accelerate context-aware incident response
Supply chain security Collaborate with your suppliers and partners.	▸ Forescout’s Vedere Labs does groundbreaking research on supply chain cybersecurity (Project Memoria, Access:7, OT:ICEFALL) using the Forescout Device Cloud, one of the world’s largest cyber asset repositories of anonymized data, to discover supply chain vulnerabilities, heed CVEs and help customers match their asset inventories with vendor advisories

FORESCOUT®

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