FORESCOUT

FCA Network Security Basics

How Forescout helps

Automated cybersecurity across your digital terrain

For more than 20 years, Fortune 100 organizations and government agencies have trusted Forescout to provide automated cybersecurity at scale.

The **Financial Conduct Authority (FCA)** in the United Kingdom provides guidance designed to help organisations better protect themselves against the risk encountered in the constant evolving cyberspace. Among the best practices and tools, the FCA recommends a number of basics requirements for network security.

Beyond the basics, the FCA acknowledges that "tackling external threats requires effective cyber security policies, standards, procedures and controls." One of the main challenges is identifying what you need to protect by keeping track of your assets and information.

Continuously know what is on your network and control access

The Forescout Continuum Platform extends scarce resources with continuous, automated asset management, risk compliance, network segmentation, network access control and security orchestration across all IP-connected assets – cloud, IT, IoT, IoMT and OT/ICS – going above and beyond baseline security recommendations to provide a strong foundation for zero trust.

- Control Access ✓
- Secure Wireless Access ✓
- Monitor Your Networks ✓
- Segregate Your Networks ✓
- Use Firewalls ✓
- Run Regular Vulnerability Scans ✓
- Prevent Malicious Content ✓

FCA GUIDANCE	HOW FORESCOUT HELPS
Control access Control who can access your network – and what they can do in it.	▸ Discover any IP-connected asset—IT, IoT, IoMT and OT asset—connected to the network with no agent and continuously. Any unmanaged, non-compliant or non-corporate device is automatically identified. ▸ Automate remediation controls in line with the organisation's security framework policies. ▸ Access controls enforcement can be based on device properties and user directory membership. ▸ Guest users, rogue and non-compliant devices can be automatically quarantined or granted limited access.
Secure wireless access Secure your wireless access points, only allowing known devices to connect to your Wi-Fi services.	▸ Manage WLAN devices deployed in a network. ▸ Restrict or block wireless clients from connecting to the organizational network. ▸ Integrate with many 3rd party wireless controllers and access points.
Monitor your networks Use network detection and prevention tools and make sure they are correctly installed by someone qualified.	▸ Centrally manage security policies by security teams and push corrective actions across your digital terrain. ▸ Visualise security posture and quickly identify potential threats on your network via a customisable dashboard. ▸ Automatically map assets and traffic flows to logical taxonomy of users, applications, service, and assets, leveraging a traffic matrix to facilitate policy design and prevent violations.
Segregate your networks Identify, group together and then isolate systems that are critical to your business – and apply the appropriate network security controls to them.	▸ Simulate planned segmentation policies to assess their impact before deployment. ▸ Segregate devices and systems based on their functions and other properties. ▸ Restrict non-corporate devices to a specific area of the network.
Use firewalls Use firewalls to create a buffer zone between the Internet – and any other networks you don't trust – and your business's internal networks.	▸ Effectively verify which devices have access to the internet. ▸ Virtual firewall capabilities and 3rd party next-generation firewall integrations. ▸ Ensure that devices with privileged account users logged in are not accessing the internet or using email or web services.
Run regular scans to check vulnerability Regularly run automatic scanning tools on your networked devices. Use the findings to resolve or manage any vulnerability identified.	▸ Get effective, extensive vulnerability assessments from Forescout via integration with 3rd party VA tools. ▸ Continuously monitor the last vulnerability scan date for all IP-connected endpoints based on events instead of schedules, ensuring scans are being performed and looking for missing patches/updates for security vulnerabilities as required.
Prevent malicious content Use malware-checking and scanning services to evaluate where files come from. They will also check incoming and outgoing data from external sources (the 'perimeter'), such as mobile devices, as well as your own internal protection.	▸ Manage and orchestrate antivirus software. ▸ Detect IoCs (Indicators of Compromise) via 3rd party systems. ▸ Quarantine compromised endpoints and trigger IoC scans on all other systems at risk. ▸ Receive regular releases of policy templates for newly discovered malware from Forescout research team (Vedere Labs) findings.

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