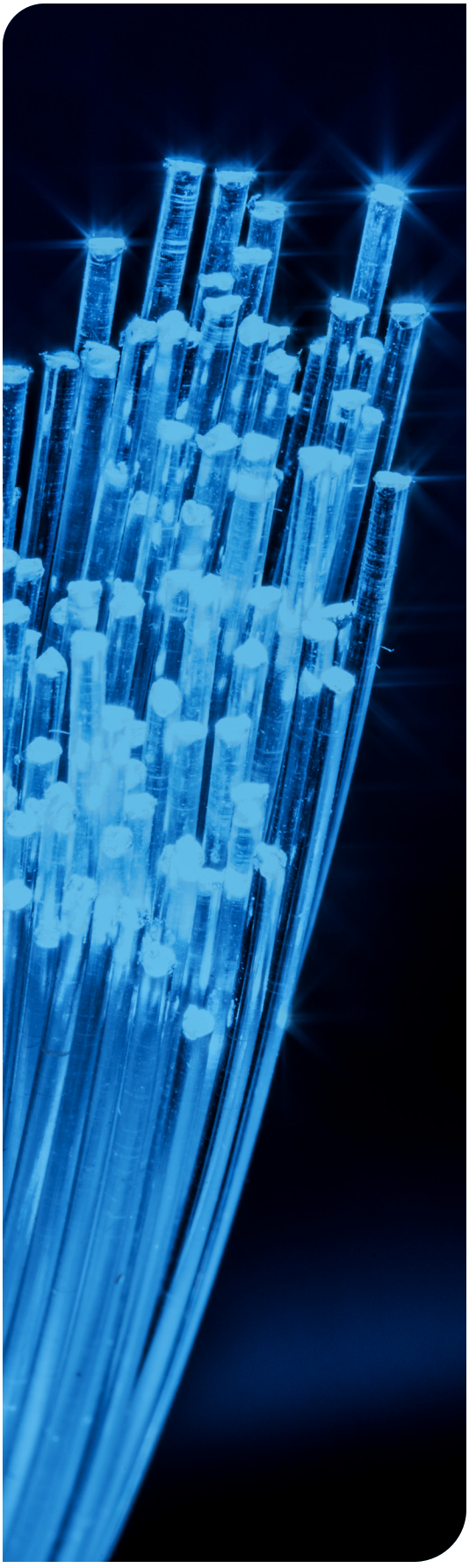

UK Telecoms Security Regulations

Alignment with Forescout

IT and telecom networks play a major role in the stability and prosperity of a nation. Guaranteeing their functioning is essential. For this reason, the UK government – alongside the National Cyber Security Centre (NCSC) and Ofcom – is developing new regulations and code-of-practice proposals that would require telecoms providers to take measures to protect their networks and services from cyber threats and ensure their resilience during major incidents. The current draft includes requirements and technical guidance regarding risk and compliance analysis, traffic and incident monitoring, and log retention reporting.

How Forescout helps

The Forescout® Platform extends scarce resources with continuous, automated asset management, risk compliance, network segmentation, network access control. security orchestration, and threat detection and response across all connected assets – cloud, IT, IoT, IoMT and OT/ICS – going above and beyond baseline security recommendations to provide a strong foundation for zero trust and other security frameworks. Following are excerpts from the draft TSR (regulations 6, 9 and 12) along with key areas within those regulations where Forescout can help address the requirements and how.

Draft regulation summary*	Main areas where Forescout can help**
Regulation 3 ▸ Understand the risks of security compromises to network architecture, record those risks, and act to reduce them. ▸ Securely maintain networks serving the UK by ensuring that network providers can identify security risks and, where necessary, operate the network without reliance on persons, equipment or stored data located outside the UK.	▸ Segmentation ("Security Zone") (2.4) ▸ Maintain records and automation ▸ Prevent exposure to the internet (2.10) ▸ Ensure that admin access is authorised (2.21) ▸ Verify that secure protocols are used (2.21) ▸ Protect management platforms by ensuring only outbound network traffic is permitted (2.23) ▸ Map the virtualised network (2.58) ▸ Access full details of hosts (2.59) ▸ Access the logical flow (protocols, equipment, trust domains, etc.) (2.60) ▸ Secure automation and orchestration (2.64) ▸ Assess criticality and sensitivity of network equipment and systems (2.80) ▸ Assets management and network monitoring (2.78)

Specifics:

The Forescout Platform continuously discovers, classifies and monitors all assets on the private network (in the cloud, on-premises, virtualised or bare metal). This includes IT/IoT and OT devices. Leveraging 30+ techniques, the Forescout Platform can provide extensive host details such as OS version, brand and model, function, installed patches and software, Active Directory membership and more. All contextual information is accessible via a set of dashboards for asset visibility, compliance and risk, device health and more.

- Search for any IP-connected asset on the network and rapidly obtain its properties, compliance status and risk.
- Build security policies based on device location, function, OS type, brand, etc.
- Quickly detect threats and automate remediation actions using built-in features or by centrally orchestrating and leveraging 3rd-party security tools and existing network equipment (switches, routers, access points, etc.)
- Generate and export reports to demonstrate compliance.

To facilitate segmentation design, implementation and monitoring, the Forescout Platform provides intuitive mapping of traffic flows between zones with the ability to first simulate and then enforce zero trust or other segmentation policies to prevent lateral movement attacks and reduce the attack surface. The solution provides information about the exposed protocols and ports between source and destination, as well as frequency and time frame of the traffic flows. This enables you to:

- Quickly identity and deny any traffic flows such as outbound traffic to the internet.
- First simulate, then enforce new traffic flow policies for minimal disruption.

Draft regulation summary*	Main areas where Forescout can help**
Regulation 6 ▸ Use monitoring and analysis tools to identify and record access to the most sensitive parts of the network or service (defined as "security critical functions"). ▸ Securely retain logs relating to security critical function access for at least 13 months ▸ Have systems to ensure providers are alerted to and can address unauthorised changes to the most sensitive parts of the network or service.	▸ Monitoring and analysis (5.3) ▸ Normal and anomalous activity (5.8) ▸ Network-based monitoring (Internally) (5.9) ▸ Critically, sensitivity, exposure and vulnerability of interfaces and equipment (5.10) ▸ Host-based monitoring (4.12) ▸ Protection of monitoring data (5.15) ▸ Effective analysis - SOC (5.16) ▸ Contextual network information (5.17) ▸ Ticketing to build a chain of events (5.19) ▸ Proactive security monitoring (5.21) ▸ Threat hunting (5.26) ▸ Regular scanning (5.29) ▸ Retaining equipment logs for 13 months (5.30)

Specifics:

The Forescout Platform detects any anomalous activity and deviation from baselines. The contextual information is processed and displayed in a dashboard to quickly visualise non-compliant devices (unauthorised, outdated and/or vulnerable software, exposed ports, etc.). To reduce IT fatigue, the platform provides multifactor risk scoring, which lists devices according to their risk based on the device behaviour, function and configuration.

The platform provides agentless and/or agent-based monitoring for deeper host-based analysis and remediation. It also integrates with many third-party vulnerability assessment (VA) tools for an even more accurate threat landscape and can enforce regular VA scans.

Forescout's extended detection and response (XDR) solution intelligently correlates threat signals from across the entire enterprise to quickly generate high-fidelity, high-confidence detections for analyst investigation – reducing the number of alerts a typical security operations centre (SOC) receives per hour from 450 low-confidence alerts to one probable threat. It uses a blend of five threat detection techniques and consolidates point solutions (data lake, security analytics, SIEM, SOAR, UEBA, threat intel platform) with a unified console to accelerate investigation and response. It includes 30-day log storage in our cloud data lake (that offers rapid search and retrieval.

For even more stringent compliance and audit requirements, Forescout provides the option to view assets' threat, vulnerability and compliance history for up to 7-years.

Finally, the Forescout Platform integrates with ITSM solutions (e.g., ServiceNow), automating workflows by sharing information with the CMDB and by automatically creating security incident within the ITSM.

Draft regulation summary*	Main areas where Forescout can help**
Regulation 12 ▸ Standardise best practice, such as rapid patching aimed at – wherever possible – fixing any new vulnerabilities within 14 days of patches becoming available.	▸ Patching and updates (11.4)

Specifics:

Any system that is running outdated software or lacking from the latest patches can be quickly identified by the Forescout Platform and put back into compliance, else quarantined, blocked or any other actions aligned to the organisation's security and compliance policy.

* Source: https://www.gov.uk/government/consultations/proposal-for-new-telecoms-security-regulations-and-code-of-practice/telecoms-security-proposal-for-new-regulations-and-code-of-practice#overview

** See the corresponding sections found in the "Draft Telecommunications Security Code of Practice": https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1057446/Draft_telecoms_security_code_of_practice__accessible_.pdf

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

©2023 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at www.forescout.com/company/legal/intellectual-property-patents-trademarks. Other brands, products, or service names may be trademarks or service marks of their respective owners. Version 01_01