Business Challenges

- Protect private data and preserve public trust
- Avoid data breaches, related fines and reputational fallout
- Improve overall network security
- Demonstrate GDPR compliance

Technical Challenges

- Keep targeted attacks from stealing data or forcing network downtime
- Discover connected devices and identify their level of compliance
- Prevent infected or non-compliant devices from spreading malware
- Measure effectiveness of security controls and demonstrate compliance with regulations
- Orchestrate unified, automated device remediation and threat response capabilities

Addressing the EU General Data Protection Regulation (GDPR)

Prepare for the new data privacy regulation by reducing your network risk profile

The GDPR requires all organizations that store or process the private information of EU residents to reduce their overall network risk profiles, improve compliance with standards and take appropriate measures to decrease chances of a data security breach.[1] The ForeScout platform can help your organization accomplish all three of these directives and avoid breach-related costs, disruptions and brand damage.

The Challenge

The European Union's General Data Protection Regulation (GDPR) is slated to take effect on May 25, 2018, and is widely described as the most sweeping change in data privacy regulation in 20 years. It affects all organizations that control or process private data of EU residents, including organizations without a physical presence in the EU. All organizations that provide goods or services to EU residents and collect data as part of the process are expected to comply.

The good news is that the new regulation seeks to "harmonize" data protection regulation throughout the 28 EU states by providing a consistent set of requirements. The bad news is that there are severe penalties associated with failure to comply: fines of up to four percent of global revenue or €20 million, whichever is higher.

The GDPR is short on details, but it does provide solid guidelines for organizations to demonstrate accountability when it comes to data security. In essence, the GDPR requires organizations to assess the level at which private data is at risk and determine which practices and technologies will effectively reduce those risks. From there, next steps are largely left to each organization.

The ForeScout platform is a key component of many organizations' GDPR readiness strategies because it is such an effective tool for strengthening data privacy and protection, reducing overall risk and demonstrating compliance.

Why ForeScout

Organizations need visibility into what is happening on the network. What devices are connected? When did they connect? Are they compliant with policies and regulations? Who has access to what data? To establish, maintain and demonstrate

compliance with GDPR requirements, organizations need to be able to readily answer these questions. Moreover, they need automated policies to enforce their security operational processes.

Whether it's helping organizations build and maintain a secure network, drive a vulnerability management program, implement strong access control measures, monitor and test networks, or sustain an effective information security policy, the ForeScout platform can play a vital role. A multifaceted cybersecurity solution, it can protect data and support compliance in the following ways:

See The ForeScout platform offers the unique ability to see devices the instant they connect to your network, without requiring software agents or previous device knowledge. It profiles and classifies devices, users, applications and operating systems while continuously monitoring managed devices, personally owned devices and other endpoints as well as ports and connections. Centrally administered, it can dynamically manage over one million endpoints from a single console.

Control The ForeScout platform delivers unparalleled network access control. Unlike systems that flag violations and send alerts to IT and security staff, ForeScout control capabilities enforce access control policies, endpoint compliance and mobile device security. Devices can be allowed or denied. They can also have network access limited based on their posture and your security policies. By assessing and remediating non-compliant devices as well as potentially malicious or high-risk endpoints, the ForeScout platform mitigates the threat of data breaches and malware attacks. In addition, by continuously monitoring devices on your network and controlling them in accordance with your security policies, the ForeScout platform dramatically streamlines your ability to demonstrate compliance with GDPR. In fact, it provides automatic identification of policy violations and documentation of adherence to GDPR and other industry mandates and regulations. It even enables one-click access to reports for auditors.

Orchestrate The ForeScout platform extends agentless visibility and control capabilities to more than 70 leading network, security, mobility and IT management products* via ForeScout Extended Modules. This ability to share real-time security intelligence across systems and enforce a unified network security policy reduces vulnerability windows by automating system-wide threat response. For example, integration with advanced threat detection solutions can automatically isolate an infected system to a secure VLAN or instantly drop the system's port, preventing it from spreading malware or exfiltrating data. Integration with a security information and event management (SIEM) system can enable detection of suspicious behavior by a device or user and trigger automatic policy-based enforcement or remediation. This level of orchestration is key to quickly identifying and mitigating a security breach, even while the network is under a distributed denial of service (DDoS) attack.

Automating Endpoint System Compliance

The ForeScout platform automatically discovers corporate-owned endpoints that do not have the required antivirus (AV) security software or that have out-of-date security software installed. It provides this intelligence to its centrally managed AV engine and can install or update the required AV software, thus bringing devices into compliance. In addition, ForeScout visibility capabilities discover, profile and classify devices with or without agents, automatically identifying and categorizing thousands of traditional, IoT and operational technology devices. This saves valuable time by providing IT teams with accurate, real-time inventories of network-connected devices to demonstrate compliance with GDPR, SOX, PCI DSS and other regulations.

When a guest's device is non-compliant with security policies (for example, missing security updates, lacking up-to-date AV software or exhibiting anomalous behavior),

WHAT GDPR INCLUDES

- Defines what data holders and processors must do to protect data
- Establishes enforcement expectations
- Imposes broad disclosure requirements (and fines) for data breaches
- Requires each organization to appoint a data protection officer and maintain detailed documentation to prove compliance
- In the event of a data breach, obligates organizations to notify GDPR authorities within 72 hours and impacted EU residents without delay

the ForeScout platform quickly isolates it on a secure self-remediation portal. The device will not be re-admitted to the network until the user has been informed and taken steps to fix the problem. In addition, guest access agreements can be enforced and staff can be automatically informed of equipment-use policies prior to granting access. Customers can be automatically limited to a guest network segment and can readily access services without compromising security. Likewise, visitors can be given Internet access through a guest VLAN, and lobby kiosks and other IoT endpoints can be placed on secure segments that cannot touch operational financial systems or the private information they contain.

Securing Data Processing Activities

Article 32 of GDPR, *"Security of Processing,"* stipulates that organizations handling EU residents' private data "shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk…." In other words, deploy serious data-breach detection and threat-mitigation solutions, or face the consequences.

ForeScout Extended Modules for SIEM enable bi-directional integration with leading SIEM systems, including HPE ArcSight®, IBM QRadar®, Splunk® Enterprise and Splunk ES. Extended Modules for SIEM combine ForeScout's device visibility, access control and automated response capabilities with the powerful correlation, analysis and search features of SIEM solutions. The result is enhanced threat insight, analytics-driven decisions and greater operational efficiency. With ForeScout and popular SIEM solutions, security teams can:

- Store ForeScout device visibility data in SIEM solutions for long-term trend analysis, visualization and incident investigation
- Correlate high-value endpoint context from the ForeScout plaform with other data sources to identify and prioritize incidents
- Initiate ForeScout control via network and host actions from a SIEM to automate incident response, remediation and threat mitigation
- Demonstrate what personal data is accessed, by whom, how it is used and when it is deleted
- ForeScout and Splunk customers can leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation

In the event of a data breach, a combined ForeScout-SIEM solution can help you document your actions, demonstrate compliance to the GDPR supervisory authority, and avoid fines.

Continuous Firewall and Device Monitoring

ForeScout Extended Modules for Next-Generation Firewalls (NGFWs) enable IT teams to orchestrate dynamic network segmentation and create context-aware security policies within next-generation firewalls based on continuous device monitoring and extensive endpoint insight from the ForeScout platform. Combined solutions from ForeScout and Palo Alto Networks® or Check Point® Software are designed to detect advanced persistent threats (APTs) and indicators of compromise (IOCs). The Extended Modules feed user ID information into the NGFWs as well as exact classifications of actual devices for automated policy enforcement and threat response.

ForeScout Extended Modules for Next-Generation Firewalls can also send GDPR compliance data collected by the ForeScout platform on connecting devices back to the firewalls. So, for example, if a device's encryption is sub-standard, that

information can be sent to the firewall and dynamically added to a rule that restricts access to certain services until the device is remediated.

Compliance Assurance

Preparing for Compliance with the General Data Protection Regulation (GDPR), a SANS Institute technology guide, advises security professionals to consult the CIS Critical Security Controls for Effective Cyber Defense.[2] Specifically, the guide cites CSC 4 *"Continuous Vulnerability Assessment and Remediation,"* which recommends that organizations "continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers."[3]

In addition to identifying, blocking or isolating vulnerable or compromised nodes, the ForeScout platform can initiate an immediate vulnerability assessment (VA) of newly connected devices using its own scanning capabilities or those of a partner solution such as Qualys®, Tenable® or Rapid7®. If a scan finds that the operating system or key applications are missing critical patches, the ForeScout platform can trigger an update by the patch management system. When repairs are complete, ForeScout can restore authorized access—all without manual intervention.

Learn More

ForeScout Extended Modules for SIEM Solution Brief

ForeScout Extended Modules for Next-Generation Firewalls Solution Brief

GDPR: A Europe-Based Regulation with Global Impact white paper

How ForeScout Technologies Inc. is Preparing for GDPR Case Study

EU GDPR home page

To view on-demand videos, run a Business Value ROI Tool, or request a demo, please visit https://www.forescout.com/demo/

ForeScout®

ForeScout Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591

*As of December , 2017
[1]https://www.eugdpr.org/
[2]*Preparing for Compliance with the General Data Protection Regulation (GDPR) A Technology Guide for Security Practitioners,* https://www.sans.org/reading-room/whitepapers/analyst/preparing-compliance-general-data-protection-regulation-gdpr-technology-guide-security-practitioners-37667
[3]SANS Institute, "Monitoring and Measuring the CIS Critical Security Controls Poster: Products and Strategies for Continuously Monitoring and Improving Your Implementation of the CIS Critical Security Controls," www.sans.org/media/critical-security-controls/SANS_CSC_Poster.pdf