



Value Chain Overview

At Forescout, we believe that managing access and trust within enterprise environments is a serious responsibility. Whether it's an international industrial enterprise or the Department of Defense, Forescout is committed to maintaining the highest levels of security and privacy for critical infrastructure and information. Internally, our information security policies and procedures take into account the value, criticality and sensitivity of information, which we strive to protect at a level that reflects the business risk from unauthorized access, disclosure, modification or loss. In addition, Forescout complies with international, federal, state and local regulations. We practice and employ numerous international and industry standards in order to safeguard the security and privacy of information, physical property, and – most importantly – people.

SDLC SECURITY

At Forescout, security is baked in, not bolted on.

We take product security seriously through the entire software and hardware system development lifecycle. The Forescout platform is certified to Common Criteria and DoDIN standards for which we achieved Evaluation Assurance Level (EAL) 4+, the highest level for any NAC-related vendor. We also maintain other security certifications across our product line.

As cybersecurity practitioners, we know that security comes not just from what we build, but how it's deployed. That's why we maintain a DISA STIG, a security technical implementation guide validated by the U.S. Department of Defense, in order to ease secure deployment and configuration. But even before they're deployed, our products are built securely—Forescout uses a tailored version of secure Software Development Lifecycle models. Our primary SDLC reference model is the NCSC 2018 application security lifecycle, although we also reference best practices as described in BSIMM and the Microsoft SDL models.

SECURE SDLC TRAINING

At Forescout, we know that security starts with awareness. That's why we've adopted and customized gamified application security training modules for our developers. This developer security training starts on the employee's first month with a mandatory online course and continues throughout their employment. Training is required for all engineering-related personnel, as per Forescout security policy aligned with NIST 800-171.

DESIGN

Forescout's product security architecture and Systems Development Lifecycle encompass both hardware and software. By design and through careful review, each physical component that goes into the Forescout platform receives supply chain and product security attention. To ensure privacy and security is baked in, the Forescout Product Feature Lifecycle includes privacy and security requirements in its Product Requirements Documents (PRDs). Although the focus of product security design review is on how we build rather than what we build, new product features involving

Policy focus areas

Forescout's Information Security Policies are the foundation of our information security, privacy and protection efforts in alignment with NIST 800-171. They are used as a reference for all aspects of our Information Security Program, including activities such as:

1. Designing security into applications
2. Defining logical and physical access privileges
3. Classifying information sensitivity
4. Conducting threat and risk analysis
5. Coordinating incident response
6. Planning for business continuity
7. Planning for disaster recovery
8. Managing audit and regulatory compliance

security do receive extra design scrutiny. Forescout's security architecture activities are holistic, covering, for example, how Forescout handles input validation and output encoding. Security-conscious design also extends to our internal and external-facing cloud infrastructure.

DEVELOP

Forescout applies state-of-the-art automatic scanning and validation tools to find potential code vulnerabilities early in the development lifecycle. All source repository commits undergo continuous code scanning and CI/CD checks for open source and third-party vulnerabilities.

RELEASE

Forescout is committed to the ongoing certification, compliance audit and security testing of our products. Product security feedback is formally collected and risks addressed before the Forescout SDLC Product Release phase. We conduct third-party penetration tests for every major release by industry-leading, CREST-accredited companies. Further, moving beyond deployment, we have implemented policy and standard operating procedures for decommissioning end-of-life hardware.

RESPOND

To stay ahead of product security issues and deliver timely vulnerability remediation, Forescout maintains a Product Security Incident Response Team (PSIRT). The Forescout PSIRT is responsible for delivering practical fixes and actionable Plans of Action and Milestones (POA&Ms) for hardware supply chain and [vulnerability management](#) issues.

END-OF-LIFE POLICY

Forescout strives to deliver innovative products that create value for our customers by regularly releasing new products and product versions. Therefore, as part of a product's lifecycle, older product versions eventually reach their

natural end of life, for which we maintain a product [end-of-life policy](#). It is Forescout's goal to make this process as transparent as possible to our customers and partners, thereby enabling them to plan for upgrades, migrations and purchases associated with their Forescout environment.

SUPPLY CHAIN COMPLIANCE & ASSURANCE

Forescout carefully reviews and performs regular audits of its supply chain vendors.

Supply Chain security is extremely important to Forescout. Forescout strives to ensure secure supply chain processes are in place with top-tier manufacturers and integrators to protect customer physical appliances and data. Our key partners integrate ISO standards and certifications (ISO 9000, ISO 14001, ISO 27001) for manufacturing processes and quality control to help ensure integrity of our physical appliances and minimize the risk of counterfeit components.

Forescout sells through best-in-class IT distribution partners and resellers to minimize the risk of product tampering during delivery. Forescout distribution partners rely upon strong logistics relationships to ensure safe passage of Forescout products to our end customers. Goods are always in direct control of these trusted partners, and processes are in place to respond and remedy any scenario where goods are reported as damaged or tampered with. In the event a customer needs to return a Forescout appliance for repair, refurbishing or scrap dispositioning, Forescout's reverse logistics processes incorporate strict physical access control and secure data destruction that ensures confidentiality while reducing our environmental footprint.

At Forescout, we have institutionalized industry-standard security policies for physical security, asset management, antivirus and endpoint protection, backup and recovery, cloud governance, encryption, firewalls and intrusion prevention systems (NIST CSF, NIST 800-17, CIS CSC).

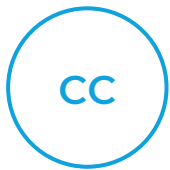













CLOUD SECURITY

The Forescout Cloud Security Program includes industry-standard practices designed to protect Customer Data from accidental or unlawful destruction, loss, alteration or unauthorized disclosure or access. Forescout regularly tests, assesses and evaluates the effectiveness of the Cloud Security Program, which it may periodically review and update to address new and evolving security technologies, changes to industry standard practices and evolving security threats.

Compliance

Forescout maintains certifications or conforms to the standards associated with the following:

 Common Criteria	 US Department of Defense Approved Product	 CSA/UL 69050 (Safety)	 Part 15, Class A	 Certified Penetration Testing	 Security Technical Implementation Guide (STIG)	
	 2018 Application Security Lifecycle	 Standard Names	 Software Assurance Maturity Model	 Critical Security Controls		

Acronyms

- | | | |
|--|---|--|
| 1. BSIMM – Building Security In Maturity Model | 6. DoDIN APL – Department of Defense Approved Products List | 10. OWASP – Open Web Application Security Project |
| 2. CC – Common Criteria | 7. ISO – International Organization for Standardization | 11. SDL – Security Development Lifecycle |
| 3. CIS CSC – Center for Internet Security Critical Security Controls | 8. NCSC – National Cyber Security Centre | 12. STIG – Security Technical Implementation Guide |
| 4. CREST – Council for Registered Ethical Security Testers | 9. NIST – National Institute of Standards and Technology | |
| 5. DISA – Defense Information Systems Agency | | |

*This security documentation does not fully apply to products from recent Forescout acquisitions, including SilentDefense by SecurityMatters and Dojo by Bullguard.



Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

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

Learn more at [Forescout.com](https://forescout.com)

© 2020 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found 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 07_20