

# Continuous Visibility, Assessment and CARTA

## Why the Forescout platform is foundational to Gartner's CARTA strategic approach



“ One-time allow/deny gating for user authentication is as flawed as one-time allow/deny gating using signature-based antivirus protection.<sup>1</sup> ”

— Neil MacDonald,  
VP, Analyst, Gartner

### Introduction

Digital transformation represents real progress when it comes to improving business processes of all kinds. However, it has also broadened the environment for advanced threats and opened new opportunities for exploitation.

Gartner's CARTA strategic approach is an ambitious attempt to redefine the way security and risk management leaders define and address cybersecurity risks within this evolving environment. CARTA, which stands for Continuous Adaptive Risk and Trust Assessment, shifts security and risk management processes away from single allow/deny gating to more agile, context-aware and adaptive methods.

This paper describes how the Forescout visibility platform, with its continuous visibility, risk profiling, device control and extensibility, supports the core imperatives of a risk and trust management strategy based on Gartner's CARTA approach.

### Rapid Change and Opportunity Enablement Are the New Imperatives

Digital business transformation is driving the pace of technology adoption beyond the capabilities of conventional risk and security management solutions. In an effort to capitalize on the benefits of IP-connected data sharing, technologists are connecting agentless IoT and operational technology (OT) devices to enterprise networks. Business units are also contributing to business transformation by outsourcing services to the cloud to leverage on-demand and highly affordable elastic-compute resources—often unbeknownst to corporate risk and security teams. And while mobility may seem like old news, it still poses challenges as systems and data are in a constant state of motion.

## Previous Security Approaches Are Unsuitable for This New Reality

After investing in conventional security technology for years, organizations seek a new, more strategic approach to network security and risk management for the following reasons:

- **Hypergrowth of non-traditional devices and OSEs:** Unmanaged agentless devices are exploding in numbers and diversity, making traditional agent-based security approaches (antivirus signatures, etc.) largely ineffective.
- **Perimeter defenses no longer work:** What remains of the corporate perimeter is porous. Physical vendor access, phishing and insider credential abuse circumvent the perimeter every day.
- **Corporate device ownership has become irrelevant:** The days of corporate-owned-and-controlled endpoints and a

“gold master configuration” are over as BYOD, IoT, operational technologies and outsource services are the new normal.

- **Point-in-time is old news:** Today’s constantly evolving device and threat landscape requires real-time asset inventory and vulnerability assessment.
- **Security silos add inefficiency and delays:** Without true integration, layered security products add levels of complexity, and separate interfaces/applications require specialized knowledge and manual coordination between products.
- **One-time block/allow authentication methods miss the point:** They fail to address the ever-changing threat landscape and associated risk and trust levels. In addition, they can impede access to legitimate users and reduce productivity.

## Gartner’s CARTA Strategic Approach

CARTA builds upon Gartner’s Adaptive Security Architecture and includes both adaptive attack and access protection. Regarding the latter, CARTA replaces one-time security gates with adaptive, context-aware security processes. Gartner Analyst Neil MacDonald sums up the need for CARTA in this way:

“The CARTA strategic approach requires continuous discovery, monitoring, assessment and risk prioritization. It moves past static yes/no, allow/block decisions in favor of more intelligent, integrated and adaptive security. Security architecture based on the CARTA approach allows underlying systems to say yes more often when granting network access through conditional and continuous analysis of the behavior of devices and users.”

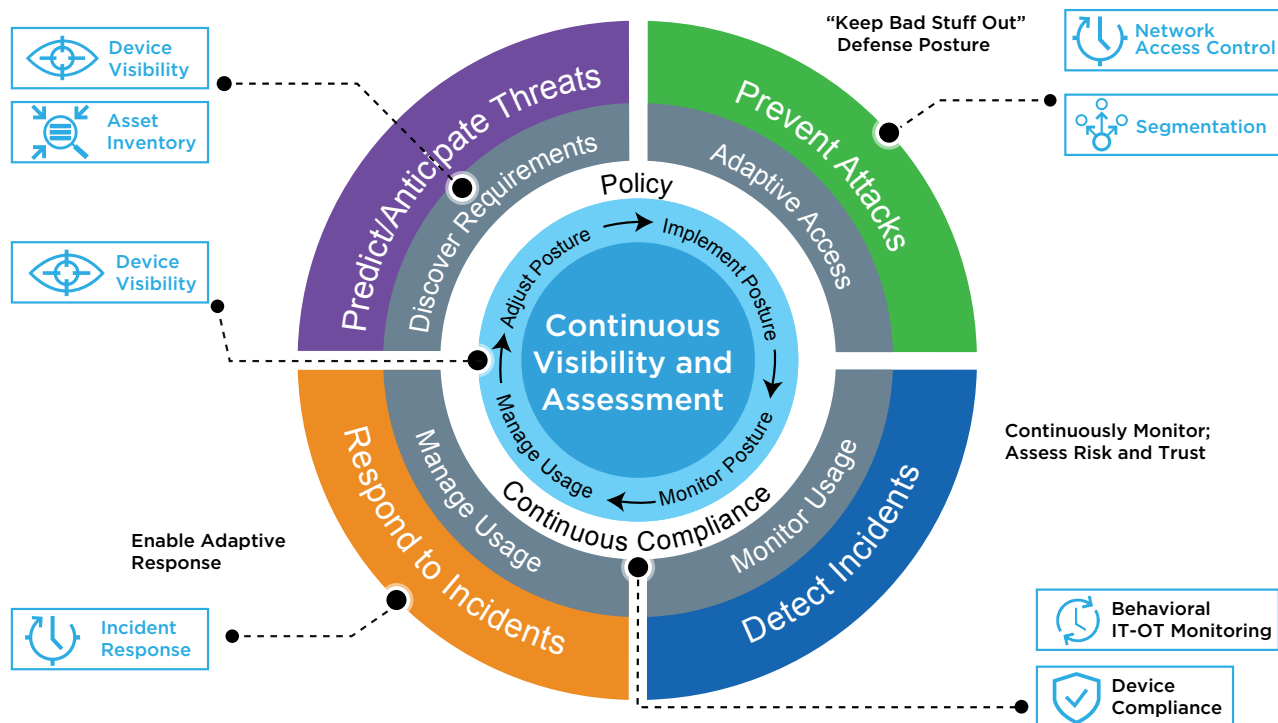


Figure 1: Continuous visibility and assessment are foundational capabilities of Gartner’s Adaptive Security Architecture and CARTA strategic approach.

## Continuous and accurate visibility is foundational to any security framework

Comprehensive visibility is foundational to security and risk management approaches such as the SANS Critical Security Controls and National Institute of Standards and Technology (NIST) frameworks—as well as any genuinely adaptive security architecture. In fact, both SANS and NIST also strongly recommend continuous monitoring capabilities. Gartner's CARTA strategic approach expands upon these framework principles, asserting that it is now essential to not only discover and monitor devices, but to “continuously assess security and compliance posture.”

## The Forescout Platform: Continuous Device Visibility, Control and Assessment to Suit CARTA

The Forescout device visibility and control platform is an agentless solution that dynamically identifies and evaluates physical and virtual network endpoints, non-traditional devices and applications the instant they connect to the network. Core technologies that power the Forescout platform have been built from the ground up to address today's visibility challenges and evolving business needs. These foundational technologies include agentless data collection, a data abstraction layer, a real-time and continuous policy engine, and distributed and scalable architecture. Upon detecting and classifying devices, the platform quickly assesses their risk profile and uses this real-time device knowledge to enforce compliance with corporate security policies. Enforcement comprises a broad range of policy-based network or host controls, including automated network segmentation assignment. The breadth of control actions is covered in greater detail later in this document.

### How Forescout defines visibility

“Visibility” has become such a buzzword these days among cybersecurity vendors that it's important to define what it means in practical terms. Forescout believes that true visibility means seeing 100 percent of the IP-based devices on the network. More than just discovering an IP address, visibility must encompass the ability to classify devices of all types, gather in-depth data about devices (what's on them and who uses them), and assess their security and compliance posture. In addition, there must be a way to visualize this data and make informed security decisions. Achieving this ambitious definition of visibility requires three core capabilities:

- **Agentless:** Comprehensive visibility of users and devices cannot be dependent upon agents or supplicants. That's true whether the endpoint is an IoT or OT device, a traditional PC, laptop or smartphone, or a virtual instance. In addition, comprehensive visibility must extend from the campus and data center to cloud and OT networks.

Agentless discovery occurs at the network layer using multiple discovery techniques, avoiding the pitfalls of solutions that discover and authenticate devices using only an 802.1X supplicant (client) or those that simply rely on a MAC Authentication Bypass (MAB) list. This is important for several reasons. First, the majority of networked devices today (IoT and OT systems) cannot run a supplicant to facilitate 802.1X authentication, requiring the device to be “authenticated” via a MAB list. This approach is unreliable, difficult to manage and rarely maintained over time. Moreover, it opens the door to MAC spoofing, allowing a malicious user to attach easily to the network using a known MAC address (easily found on a phone or printer).

- **Continuous:** A solution must continuously see devices in incredible detail and monitor their behavior and compliance status as they come and go from the network. It must also be capable of continuously sharing device compliance and threat data with third-party solutions and initiating access enforcement and remediation actions.
- **Heterogeneous:** Visibility (and control) must extend across mixed network infrastructure and third-party security solutions. This capability allows organizations to use their preferred switches, wireless routers, firewalls or VPNs—with or without 802.1X authentication. It also allows for rapid modification to accommodate mergers and acquisitions as well as business evolution.

---

“Assessments and visibility of risk/trust and the exchange of context become the immune system for digital business.”<sup>2</sup>

— Neil MacDonald, VP, Analyst, Gartner

---








 <b>Device</b> Type of device NIC vendor Location Connection type Hardware info MAC and IP address Certificates	 <b>Operating System</b> OS type Version number Patch level Services and process installed or running Registry File names, dates, sizes	 <b>Security Agents</b> Antimalware/Virus/DLP agents Version number Encryption agents Firewall status Configuration
 <b>User</b> Name Authentication status Workgroup Email and phone number	 <b>Applications</b> Installed Running Version number Registry settings File sizes	 <b>Network</b> Malicious traffic Rogue devices
		 <b>Peripherals</b> Type of device Manufacturer Connection type

Figure 2: The Forescout platform uses a combination of active and passive techniques to query heterogeneous network infrastructure and gather in-depth details regarding physical and virtual devices on IP networks.

## Using visibility to add control

Forescout uses continuous, in-depth visibility to apply the appropriate control actions. A broad range of controls avoids the standardized use of “yes/no, allow/block” responses. Instead, intelligent actions can be initiated based on real-time context (for example, allow on network but limit to specific network segment; or, allow on but initiate a vulnerability assessment scan, confirm antivirus is functioning, etc.) A user with disabled or outdated antivirus software or missing patches can be allowed internet-only access and notified to update their software. Upon verification of the update, more appropriate access can be automatically granted according to policy.

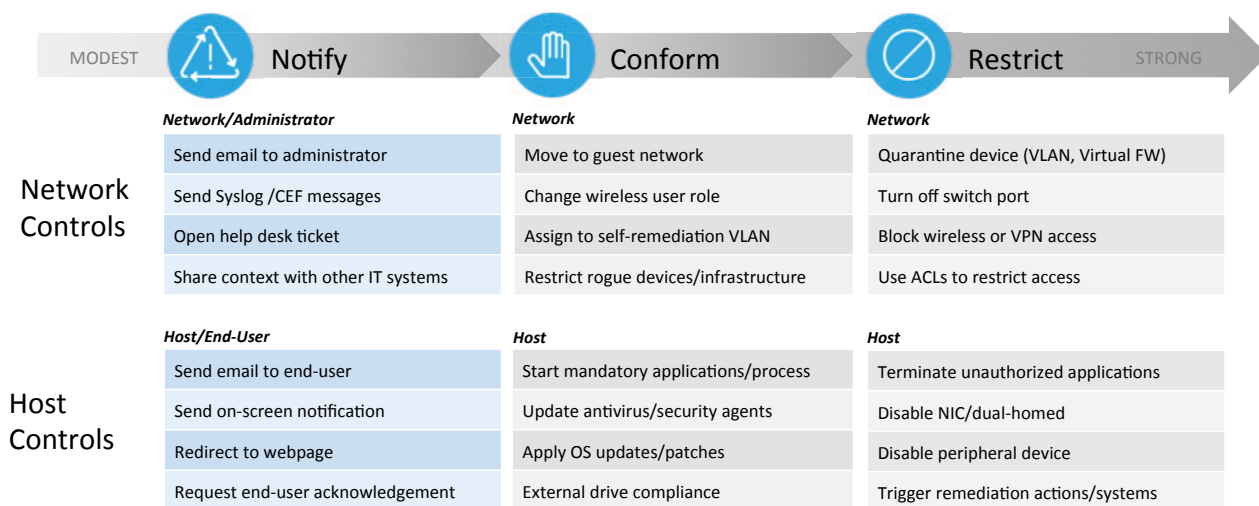


Figure 3: A broad array of network and host control responses allows companies and individual business units to define adaptive access policies that accommodate different levels of risk tolerance. Based on device context, changing risk status or user behavior, the Forescout platform adapts to apply the appropriate level of control.

## Automating multivendor orchestration

In most organizations today, enterprise security management breaks down (in every sense of the term) into several rigidly defined product areas. These product areas can benefit from the integration capabilities that the Forescout platform, Forescout Base Modules and eyeExtend products provide—unifying disparate security tools into a cohesive unit that exchanges information and responds to incidents in a coordinated, automated and accelerated manner.

Forescout Base Modules and eyeExtend products extend the visibility and control functionality of the Forescout platform to more than 70 third-party products\* to coordinate the full gamut of adaptive attack-protection actions, allowing organizations to better prevent, detect, manage and predict risk. Specific examples are covered later in this paper.

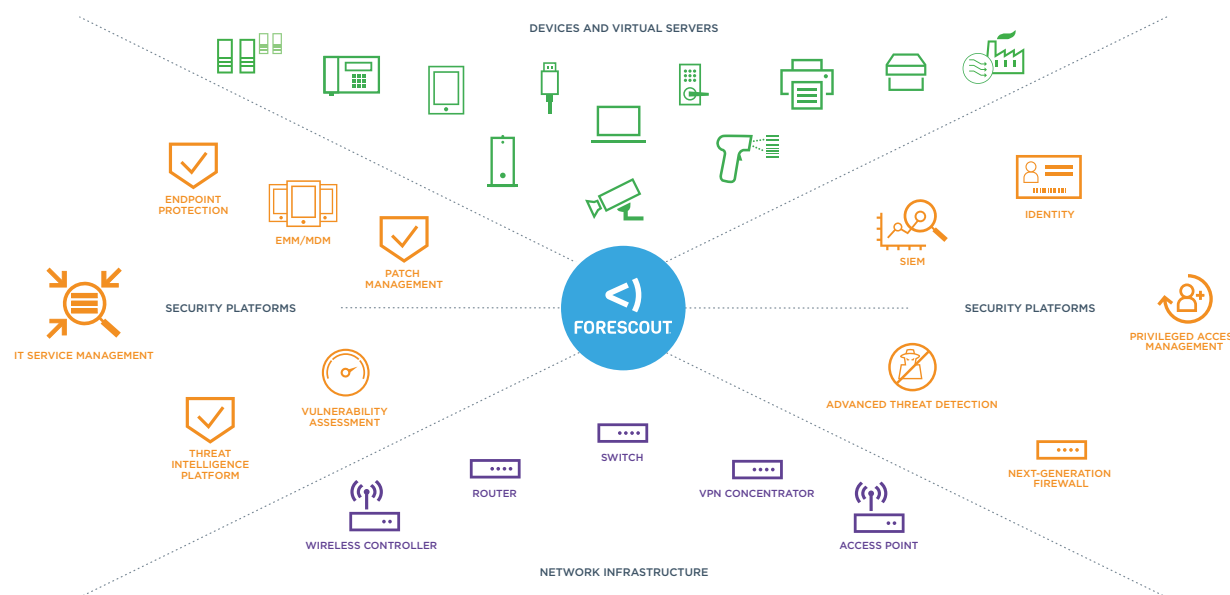


Figure 4: In addition to providing continuous visibility and posture assessment of all devices on the network, the Forescout platform serves as an open platform for integration, sharing device context with popular security and IT management solutions and coordinating response actions. This ability to orchestrate workflows among disparate tools helps security operations teams automate adaptive protection and attack response.

## Addressing Gartner's CARTA Imperatives

In Gartner's April 2018 Research Note, *Seven Imperatives to Adopt a CARTA Strategic Approach*, analyst Neil MacDonald outlined core capabilities that security and risk management leaders must embrace when adopting a CARTA strategic approach. Here is a quick overview of how the Forescout platform helps address these imperatives:

### 1. Replace one-time security gates with context-aware, adaptive and programmable security platforms

Today's security threats are so sophisticated and fast-evolving that one-time, pass-fail gating processes, no matter how robust, are simply not secure enough. All systems with access to network resources must be monitored continuously for state or behavioral change, and all require immediate control response. From the company's inception, Forescout platform architects understood that simple yes/no, allow/block mechanisms would not meet changing business needs and security requirements. Our device visibility and control platform was designed to acquire rich contextual data on every device, continuously monitor state and behavior, and automatically initiate policy-based responses at defined trigger points.

The Forescout platform is highly adaptive, uses standard, out-of-the-box policies for basic controls, and offers endless opportunities to customize policies or add new ones. It allows both pre-connect and post-connect options on both wired and wireless networks. For example, requiring users to authenticate prior to being granted access (pre-connect) can accommodate proactive risk discovery and assessment for sensitive applications while post-connect provides effective reactive risk discovery. Forescout allows both approaches to run simultaneously, providing architectural flexibility in risk policy design.

Using this layered policy approach and real-time device and compliance context, the Forescout platform can perform less restrictive actions to maintain user productivity while ensuring security. This has allowed customers to adopt a trust-but-verify, post-connect model in most instances, while still supporting stringent pre-connect authentication for highly sensitive applications.

## 2. Continuously discover, monitor, assess and prioritize risk—proactively and reactively

Asset intelligence is key to understanding the risk an endpoint introduces to the network. It's essential for knowing with certainty who and what are on your network, including detailed knowledge about compliance status. Without 100-percent, real-time visibility into all devices, there will be gaps regardless of how many security tools are deployed across the extended enterprise.

The Forescout platform provides continuous, detailed visibility—without requiring agents—across the campus, cloud and data center environments. It supports a wide range of OSES (Windows, Mac, Linux, Android and iOS, as well as proprietary IoT and OT) to discover, classify and profile physical, virtual and remote devices.

The Forescout platform performs a detailed posture assessment upon each device, then can feed up-to-date device and configuration details into asset management tools, providing the foundation for a real-time configuration management database. It then continuously monitors devices and alerts IT management and security operations teams of changes in device compliance status.



Figure 5: The Forescout platform's customizable web dashboard provides IT and security operations teams with a comprehensive view of devices, their classification context and their security posture, allowing for real-time risk prioritization.

Having an accurate, up-to-date asset management database of device compliance status provides essential knowledge for proactive risk management. Continuous monitoring validates security posture, discovers noncompliant behavior and provides nonstop security context, allowing the Forescout platform and security operations teams to prioritize risk and react instantly to policy violations or anomalous behaviors.

## 3. Perform risk and trust assessments early in digital business initiatives

Gartner points out that eliminating one-time security gates can't stop with production systems; continuous risk assessment should also be applied to new business initiatives and the IT infrastructure created to support them. If predictive risk assessment during development is combined in a continuous loop with reactive assessments as new systems move through testing and deployment, the entire DevOps cycle can be refined and accelerated.

Inevitably, however, some ad hoc initiatives or thoughtless actions (rogue cloud facilities, personal wireless gateways, etc.) will bypass proactive screening. In these instances, the Forescout platform's ability to discover, inspect, profile and control devices or systems as they connect to the network, and its continuous monitoring capabilities, are essential for the establishment of a comprehensive risk and trust management solution.

One other important consideration in this regard is flexibility. As IT infrastructure evolves due to new initiatives, merger and acquisition activity, or incremental upgrades, security solutions must be able to adapt. The Forescout platform is infrastructure-agnostic, allowing rapid integration across any choice of architectures, switches and heterogeneous networks. This facilitates continuous risk and trust assessment even as enterprise infrastructure undergoes dramatic change.

In addition, Forescout leads the industry in scalability and per-rack density, resulting in the ability to scale to 20,000 devices per appliance, minimizing the need for additional hardware. What's more, a single Forescout eyeManage deployment can manage up to 2 million devices, ensuring the Forescout platform grows with customer needs.

**4. Instrument infrastructure for comprehensive, full-stack risk visibility, including sensitive data handling**






The Forescout platform can be the cornerstone of a full-stack risk-detection solution. It can complement and augment behavioral analysis products in several ways. Specifically, Forescout has a proven track record for sharing real-time device and user context data with third-party tools such as SIEM solutions, many of which now offer users behavioral analytics capabilities. Increasingly, Forescout is seeing security operations teams adopt the Forescout platform as their primary platform for continuous access management, monitoring and incident response. Many are using Forescout’s ability to share real-time contextual data with SIEMs and provide automated response for security enforcement and remediation.




Forescout continues to expand upon its cloud visibility and continuous monitoring capabilities through ongoing development and integrations with Amazon® Web Services (AWS®) and VMware®, as well as recent integrations with Microsoft® Azure® and Cisco® ACI. As applications and data extend to the cloud, these integrations allow the Forescout platform to discover, profile and monitor virtual instances, including their users and security parameters, and ensure that VMs are properly decommissioned once a workload is complete.

**5. Use analytics, AI, automation and orchestration to speed the time to detect and respond—and to scale limited resources**

Given the complexities of today’s distributed networks and the evolution of digital business ecosystems, there is no single “silver bullet” that can prevent cyberattacks. Gartner recommends using “multiple layers of analytic techniques to better surface meaningful risk to focus our limited resources on real and important risks.”<sup>3</sup> The real challenge in doing this, however, is to avoid disjointed silos and manual processes that can delay response and turn enterprise security teams into perpetual motion machines.

As mentioned previously, Forescout allows significant automation through deep integration with leading security, analytics and IT management tools. Here’s a partial list of automation and orchestration capabilities Forescout provides through add-on Base Modules and eyeExtend products:

<p><b>Advanced threat detection (ATD).</b> Shared intelligence about affected systems and indicators of compromise (IOCs) allows the Forescout platform to automatically hunt for, contain and respond to threats across managed and unmanaged endpoints. Partners include:</p>	
<p><b>Client management tools (CMTs).</b> Forescout eyeExtend for CMT fortifies endpoint defenses, enforces compliance and reduces the attack surface by sharing data and automating enforcement actions such as ensuring the latest patch updates with:</p>	
<p><b>Cyber risk modeling and prioritization.</b> The combined Forescout-RedSeal solution provides an accurate, up-to-date model of your network so you can visualize access paths, check for policy and compliance violations and prioritize what to fix.</p>	
<p><b>Deception techniques.</b> Deception platforms share device and user data with the Forescout platform, which immediately blocks or quarantines the source of the threat and alerts security personnel. Integration partners include:</p>	
<p><b>Enterprise mobility management (EMM).</b> Through orchestration, the Forescout platform detects devices that lack functional EMM agents, then quarantines them until they are compliant and provides optional agent reinstallation. Partners include:</p>	

<p><b>Endpoint protection, detection and response (EPP/EDR).</b> These integrations allow the Forescout platform to verify device compliance for functional agents, up-to-date signatures, encryption and other endpoint policies and facilitate remediation actions. They also enable the Forescout platform to automate threat hunting and response across managed and unmanaged endpoints.</p>	
<p><b>IT service management (ITSM).</b> This eyeExtend product creates a real-time asset inventory to true-up your configuration management database while providing contextual asset intelligence.</p>	
<p><b>Next-generation firewalls (NGFWs).</b> eyeExtend products for these solutions simplify dynamic network segmentation, automate controls for secure access and create context-aware security policies within NGFWs using real-time device context from the Forescout platform.</p>	
<p><b>Privileged access management (PAM).</b> Defend against privileged credential misuse and rapidly respond to sophisticated privileged account threats with Forescout eyeExtend for CyberArk.</p>	
<p><b>Security information and event management (SIEM).</b> Forescout eyeExtend products automate information sharing and policy management between the Forescout platform and these leading SIEM systems to improve situational awareness and mitigate risks.</p>	
<p><b>Vulnerability assessment (VA).</b> Initiate VA scanning of devices as they come and go from the network and automate policy-based enforcement actions as necessary using these eyeExtend products.</p>	

## 6. Architect security as an integrated, adaptive and programmable system, not silos

The Forescout platform can break down organizational and technology silos in several ways. It provides visibility of risk and compliance status across organizational groups (including IT management, endpoint, infrastructure, security operations and compliance teams), allowing personnel to operate on shared, consistent data. It helps break down silos that often exist between departments and business units, which may control their operational technologies or use cloud-based services. The platform's customizable dashboard allows up-to-date, graphical views of key risk and device context data points. As an integration platform, the Forescout solution can orchestrate security management and response workflows to avoid technology silos, disjointed operations and delayed incident response. Using a common visibility and control platform that spans the extended enterprise also means fewer tools to purchase, learn and use.

In addition, the Forescout platform is inherently programmable in two ways: 1) Organizations can create an endless array of access control policies based on continuous assessment of device compliance and link response actions as they see fit;



and 2) In addition to offering more than 70 Forescout Base Modules and eyeExtend products for out-of-the-box integrations, Forescout enables custom integration of third-party risk management products or custom applications via its Open Integration Module, which supports the following open, standards-based integration mechanisms:

- Services API for sending and receiving XML messages
- SQL, allowing reading from and writing to databases, such as Oracle®, MySQL, and Microsoft® SQL Server
- LDAP, enabling reading from standard directories

## 7. Empower business units and product owners with continuous, data-driven risk decision-making

Forescout provides several capabilities that facilitate better security and risk decision-making and collaboration between network, security operations and business units. For example, customizable dashboards can provide up-to-date device compliance metrics and risk reports to SecOps, IT management teams and executives, regardless of organizational structure or location. Sharing consistent, up-to-date device context and KPIs among compliance, security, IT management, OT management and DevOps teams allows for common security and risk management views and dialogue. The ability to support centralized and distributed deployment architecture can facilitate this process as well.

Production lines and OT sensors (as well as critical infrastructure and cyber-physical systems) are sensitive to active monitoring techniques, making these systems extremely difficult to inventory and profile—leaving OT and IoT technology owners unwilling to collaborate with security and risk management teams. By offering non-disruptive, passive-only techniques for device discovery and profiling, Forescout

is opening doors and bringing formerly reluctant business and organizational units to the table.

Segmentation is likely the only practical way to secure legacy and agentless systems. Forescout automates network-based segmentation to satisfy business units that require more stringent device security—or to protect sensitive data from business units with higher risk-tolerance levels. Because the Forescout platform is completely vendor- and architecture-agnostic, we are able to natively apply segmentation policies across products from more than 30 switch and wireless vendors. In other words, there's no need to standardize on a single network infrastructure vendor, technology or version level. Given the realities of today's heterogeneous networks and the promise of more diversity through mergers and acquisitions, this is a significant advantage. In addition, Forescout allows pre- and post-connect authentication methods to run simultaneously on various network segments to appropriately match enforcement methods with risks.

## Forescout Is Foundational to Gartner's CARTA Strategic Approach. Learn More.

Continuous visibility and assessment are the cornerstones of continuous adaptive risk and trust assessment. Learn more about Gartner's strategic approach, and how the Forescout device visibility and control platform plays a key role in addressing CARTA requirements with these resources:

- [Forescout Agentless Device Visibility and Control White Paper](#): Learn how the Forescout platform delivers foundational capabilities for effective cybersecurity.
- [Contact Forescout Consulting Services](#): Need help planning and implementing the Forescout platform or integrating third-party solutions into an adaptive security architecture? Forescout Consulting Services has expert consultants who can assist you.
- [Take a Test Drive](#): Experience the before-and-after difference of the Forescout platform with a hands-on test drive that takes you through five powerful use cases.

\*As of March 31, 2019

1 Neil MacDonald, Gartner Security and Risk Management Summit, June 2018

2 Zero Trust Is an Initial Step on the Roadmap to CARTA, Gartner, December 2018

3 Seven Imperatives to Adopt a CARTA Strategic Approach, Gartner Research Note, published: 10 April 2018



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://www.forescout.com)

© 2019 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://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 08\_19