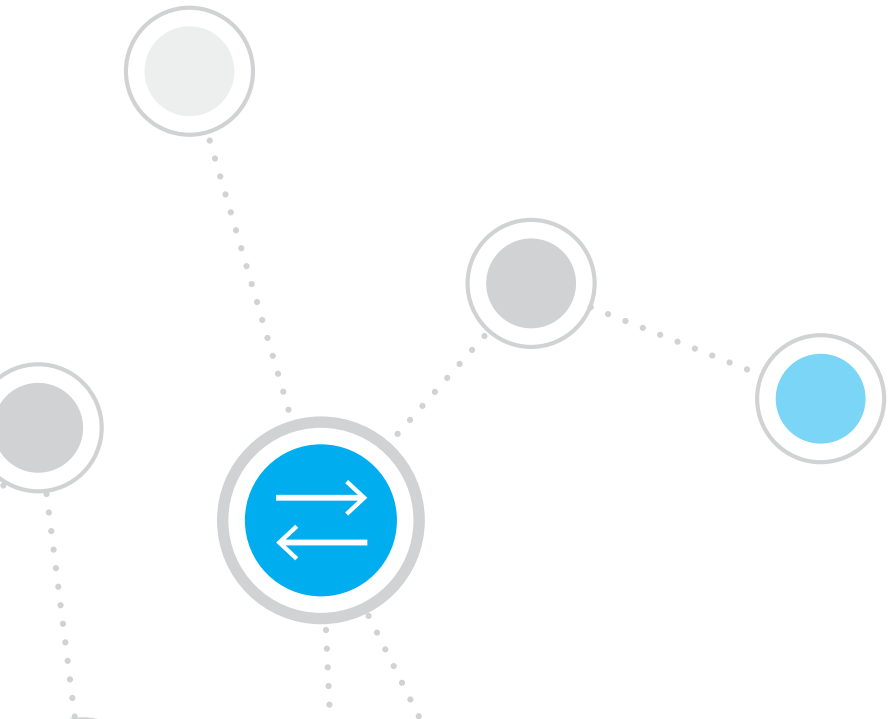
ForeScout

White Paper

# Automating System-Wide Security Response Through Orchestration



# The Situation

Data breach numbers keep going up every year. Costs per incident keep rising. Enterprise network security is tested daily as the numbers of BYOD endpoints, Internet of Things (IoT) devices and operational technology (OT) systems continue to climb. Most of these devices can't support software agents, and managing their security hygiene and compliance posture is challenging with traditional security methods, to say the least. With connected devices anticipated to grow to 29 billion by 2020,[1] recognizing and securing unknown operating systems will be a herculean challenge for security professionals the world over. Organizations are trying to keep pace by investing in more and more security tools, but is anything really changing for the better? Is anybody safer?

If that introduction wasn't enough to make you take notice, consider this: The vast majority of security tools that enterprises are adding to their arsenals require constant human intervention because they are not capable of communicating with each other. In fact, in a recent Frost and Sullivan survey of senior IT officials conducted on behalf of ForeScout, 52 percent of respondents from large enterprises (organizations with more than $1 billion annual revenue) said they operate more than 13 different security tools. Yet more than two-thirds of those surveyed reported they had only a couple of tools that could directly share security-related context or control information.[2]

More security tools require more oversight and even bigger security teams. In turn, bigger security teams must plod through and analyze more and more data from all of those new tools, slowing response times when real threats emerge. Enterprise security teams risk turning into perpetual motion machines.

What's the solution? In a word, orchestration. It's the answer on premises in the data center, off premises in the cloud, and everywhere in between. Industry analysts are on board. They're preaching the value of orchestrating and automating enterprise security tools not only because they've seen the light—they're hearing from their enterprise customers who have adopted orchestration solutions and are seeing results. Security vendors are getting in on the action as well, in some cases making preposterous claims that they have been orchestration vendors all along. But take that as a good sign, because it is now abundantly clear that orchestration's time has come. Now it's not a matter of whether or not to orchestrate; the real decision involves which security actions to automate and what technology is best for the job.

# Orchestrated Security and the Human Body Have a Lot in Common

A good way to think about how to make these decisions is to look at a complex model like the human body, and understand the decision mechanisms that we use to keep us safe.

The human body is an extremely complex amalgamation of systems that somehow manage to work together year after year. Of all of the body's systems, one—security—is especially ingenious in that it features two key decision-making mechanisms: the nervous system and the brain. Discrete components, they each have a unique role to play. But they also complement each other.

The nervous system's job is to keep us safe. It is fully aware of its surroundings and can react in real time and in a very instinctive, fight-or-flight way. Relying on its own network of sensors, the nervous system doesn't consult the brain in many of the thousands of decisions it makes every day because things happen too fast. Picking up a cup of coffee, for example. The nervous system tells the hand to put it down instantly if the cup feels hotter than it should be. It does so to give the brain the opportunity to do what it does best: pondering unknowns (aka thinking).

The brain focuses on higher-functioning decision-making to keep us safe. It is constantly looking for and perceiving patterns related to situations and things it has never seen before. It makes deductions based on experience and surroundings. It asks questions and does calculations all in the service of

1 ABI Research," 2017

2 Frost & Sullivan: Continuous Monitoring and Threat Mitigation with Next-generation NAC, http://resources.forescout.com/Frost-Sullivan_NAC_White-Paper.html

decision-making. But it's slow and can't keep you safe when there's a threat that requires split-second action. However, because the brain is higher functioning, it can override your nervous system. That hot cup of coffee? The brain can "tell" the nervous system that, yes, it's hot, but not hot enough to burn. So pick it up!

| | | |
|---|---|---|
|  | **Nervous System**<br>Instinctive reactions for keeping one safe | • Full awareness: sensors everywhere<br>• Real time and instantaneous: no time to think; immediate response<br>• Rules learned over time based on evolution and what makes you safe<br>• Does not involve the brain: protects the brain for higher-function decisions<br>• But informs the brain so it can make a conscious decision as to what is the appropriate response |
|  | **Brain**<br>Higher-functioning Decision-making | • Recognizes patterns based on multiple inputs<br>• Capable of making decisions when faced with new situations<br>• Can override the nervous system instinct<br>• Slower to respond |

**A real-world analogy:** *the human body features a bi-lateral security system that functions in a manner similar to effective network security solutions.*

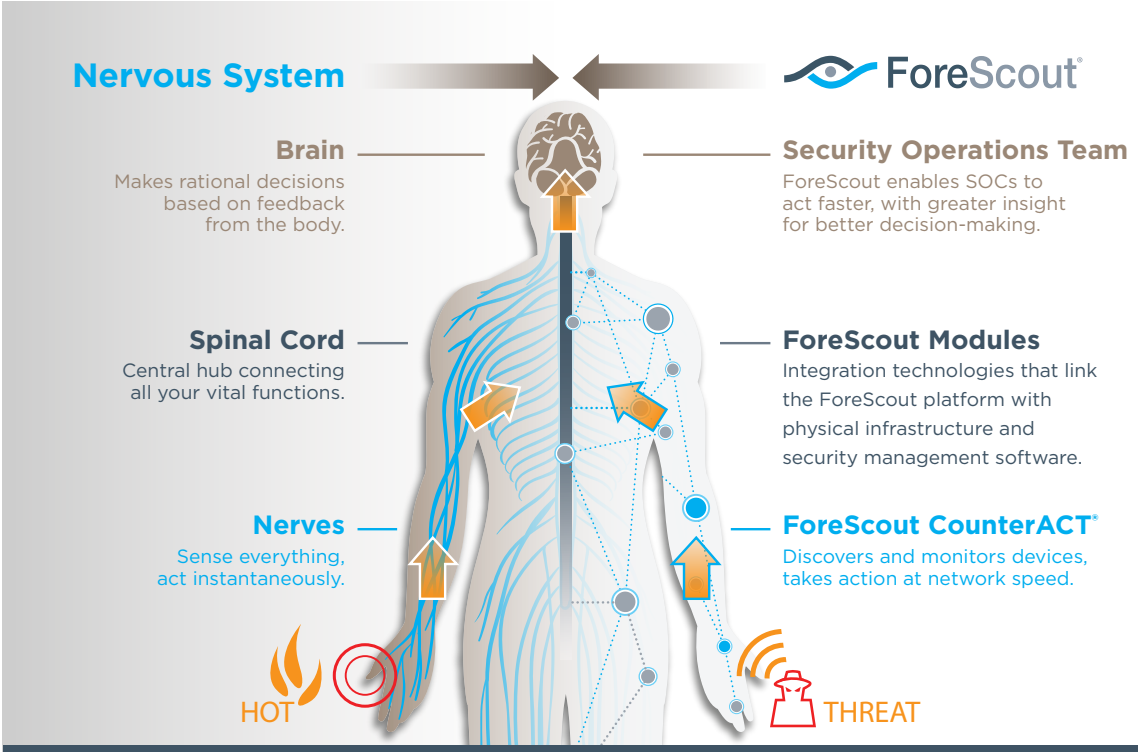
How does enterprise security relate to this? It's simple. For safety's sake, security architecture must have a lightning-fast cyber nervous system plus a smart, resourceful "brain," which is typically a security operations team that analyzes threats and decides whether they are real or not. Above all, the enterprise security brain needs absolute visibility and situational awareness when it comes to potential problems, and a safe interim in which to make decisions—an interim provided by the cyber nervous system.

# We Were Born to Orchestrate

ForeScout is uniquely qualified to fill the position of the enterprise cyber nervous system. A comprehensive, highly intelligent network security solution, the ForeScout platform offers the visibility, insight and data aggregations to provide comprehensive, in-depth awareness of what's in your environment. It has the ability to instantly recognize devices through base-level integration across heterogeneous network infrastructure and a combination of active and passive discovery and monitoring techniques. This allows the ForeScout platform to "touch" devices—including sensitive OT systems and business-critical devices—without disrupting them, to gain detailed sensory insights. It uses these insights to help classify devices you may have never seen before, and uses this knowledge to continuously monitor devices and assess whether they are safe.

Its rules engine and workflow engine are able to act at line speed and in real time. And, working with ForeScout Base and Extended Modules, the ForeScout platform can exchange information with network infrastructure and a wide range of third-party security tools throughout the extended enterprise network environment, allowing the ForeScout platform to take action against threats, either automatically or when the brain—your team—says to do so.

# The Vision of Orchestration




**Neural Network vs. Corporate Network:**
How ForeScout operates like the human nervous system.

Think about your security strategy in terms of a brain and cyber nervous system. Your vendors are all vying to supplement your brain—your security operations team. This is all well and good because ForeScout can partner with them to make their solutions and ours smarter and more effective. The various "brainy," siloed security solutions have specialties. They're good at something, whether it is correlating data and events, pinpointing vulnerabilities, detecting malware, issuing alerts, or whatever the case may be. In general, however, they aren't real-time solutions, are lousy communicators, and in most cases, are incapable of taking action.

That's why the ForeScout platform and ForeScout Extended Modules are so valuable. Together, they act as a central hub, connecting your vital security functions in the same way your spinal cord transmits data from nerve endings to the brain. ForeScout Extended Modules use open integration technologies to provide the data and uncover the contextual information that third-party security solutions need to make decisions. They enable the ForeScout platform to share insights about devices—both managed and unmanaged, agent-enabled and agentless—and automate workflows and security processes across leading security solutions of all kinds.

This is true integration—elevating and unifying enterprise security management at a system-wide level that has not existed before. The resulting newfound capabilities are a vast improvement over the previous status quo, enabling:

**Expanded device visibility –** Throughout the extended network environment, gain better insight into BYOD, IoT, OT, virtual machines and other IP-connected devices, including IPv6-addressable systems and devices managed by cloud network controllers such as Cisco® Meraki. The ForeScout platform "sees" them all. And, working in tandem with the ForeScout Device Cloud, the ForeScout platform provides cloud-based intelligence to auto-classify new devices—a powerful asset for creating security policies for network access, device compliance and network segmentation.

**Greater operational efficiencies –** Through integration, the ForeScout platform makes formerly disparate security tools capable of sharing information and improving security insights across the board. As a result, security tools and personnel are able to act upon prioritized and vetted security issues while reducing the need for manual oversight and intervention.

**Accelerated threat response –** Orchestration of security tools via the ForeScout platform and ForeScout Extended Modules enables automation of basic tasks and risk mitigation while providing your security operations team with real-time information on threats—optimizing incident response and reducing mean time to respond.

**Consolidated view of device landscape and compliance –** The ForeScout platform includes a customizable web dashboard that offers a consolidated view of the device landscape and compliance across the extended enterprise—providing real-time device intelligence that includes device classification, connection, compliance and risk status.

**Higher security ROI –** By taking security tools out of silos and plugging them in to a highly intelligent and unified central nervous system that can automate threat mitigation and policy compliance, the ForeScout platform enhances the value of your security tools and provides the foundation for a rapid return on investment (ROI).

**A much-improved network security and compliance posture –** Integration provides the ability to automate and enforce policies and helps to ensure that the right users and systems are appropriately accessing the right resources. By unifying security management, the ForeScout platform helps you automatically identify policy violations, remediate endpoint deficiencies and measure adherence to compliance mandates.

# The Value of Applied 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 be combined and benefit from the integration capabilities that the ForeScout platform and ForeScout Extended Modules provide—unifying disparate security tools into a singular platform in which information is shared and incident responses are coordinated, automated and accelerated.

Consider the possibilities:

### Next-Generation Firewalls

As defense perimeters, firewalls are effective at keeping large segments of the cybercriminal community out. However, they are completely ineffective when it comes to endpoint compliance. Orchestration can provide real-time intelligence about the devices and users on your network,

including BYOD, guest and unmanaged endpoints, without the need for agents. This is the basis for enforcing firewall policies and eliminating risks on a much more comprehensive level. It also allows real-time device context and behavior to be used to make segmentation decisions by the firewall.

**Security Information and Event Management (SIEM)**

SIEM solutions are only as good as the information that is fed into them, and the timeliness of that information. Orchestration can enable comprehensive, real-time discovery of network endpoint data, which can then be sent to the SIEM in real time, closing visibility gaps and broadening situational awareness. With orchestration, leading SIEM systems can also gain enforcement capabilities. Depending on the severity of the threat, actions can range from a gentle reminder to a device user to update a device, to quarantining the endpoint or even direct, mandatory remediation.

**Advanced Threat Detection (ATD)**

ATD systems within a unified security management platform can assess the extent of infection on your network and contain the threat. When an integrated ATD system detects malware, it shares data about the affected system(s) and indicators of compromise (IOCs). Then, based on your policy, it can scan other endpoints for presence of infection and collaborate with other security tools to take policy-based actions to contain and respond to the threat. Infected devices can be quarantined or lesser actions can be taken depending on the level of risk that the threat poses.

Either way, malware propagation is stopped and the cyber kill chain is broken.

**Enterprise Mobility Management (EMM)**

Integration of EMM systems can provide companies with automated security policy management for devices on the network regardless of the type (PC, Mac, Linux®, tablet, smartphone), the type of connection (wired, wireless, VPN) or the ownership of the device (corporate, personal or vendor/contractor). Forget manual monitoring, installing, updating and reactivating security agents on managed systems, and all of the lost time that it implies. In a unified security management system, EMM gains comprehensive information about devices and works within the system to take appropriate action when a device doesn't have a functional EMM agent—reducing the network's attack surface and closing windows that cybercriminals might otherwise use to propagate malware within the network and exfiltrate data.

**Vulnerability Assessment (VA)**

It's ironic, but Vulnerability Assessment systems typically have a built-in vulnerability: they scan the network periodically instead of continuously, which leaves organizations blind to risks that emerge between scans. However, through orchestration, VA systems can take advantage of other security tools' capabilities—sharing real-time information and initiating VA scanning of devices as necessary. Automated scanning can be triggered by endpoints that meet certain policy conditions, such as when they contain specific applications, or when endpoint configuration changes are detected.

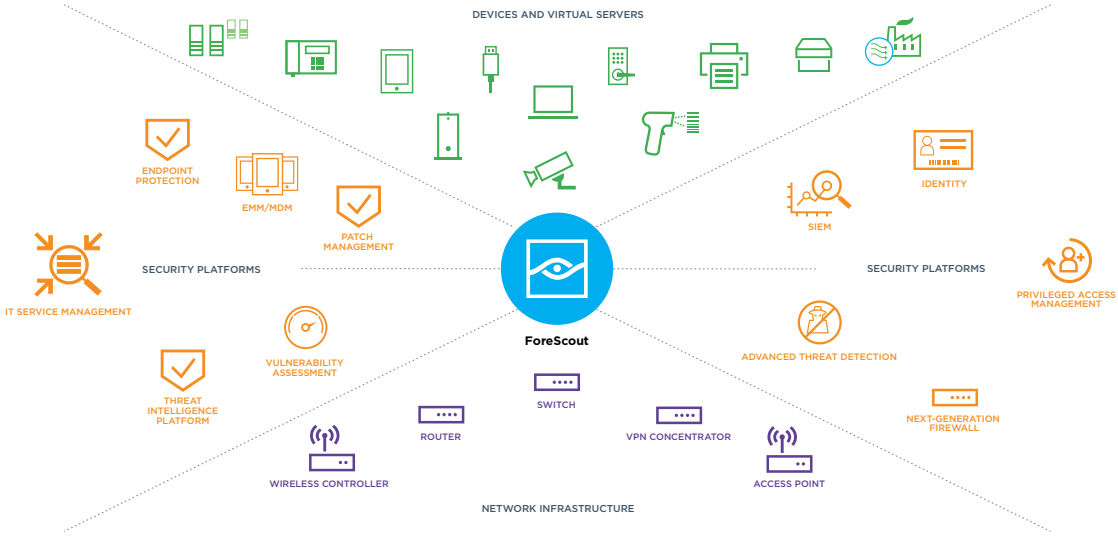
Then risk mitigation actions can be taken automatically if vulnerabilities are detected. In this way, through integration, VA becomes a much more valuable and much less vulnerable tool.

**Endpoint Protection Platform (EPP)**

In a unified security management system, EPPs can be much more intelligent—managing endpoint security not only on corporate-owned (managed) devices but on BYOD and IoT (unmanaged, agentless) devices as well. In fact, orchestration can help close visibility gaps and facilitate automated compliance with antivirus, patch management, encryption and other endpoint management policies. The ForeScout platform can quickly discover devices with missing or broken endpoint protection applications or encryption agents and coordinate with patch management solutions to ensure that endpoints are quickly returned to compliance.

# Orchestration, ForeScout and the Ties that Bind

While still common, enterprise security tools working in silos is a legacy paradigm. Today, with the integration between products and the orchestration that the ForeScout platform and ForeScout Extended Modules provide, unified enterprise security architecture is a reality for many organizations. These forward-thinking organizations are experiencing the synergies and added functionality that come with information sharing. By establishing once and for all that formerly disparate security tools can work together as one, ForeScout and its partners are proving that cooperation and heterogeneity trump proprietary concerns when it comes to providing customers with superior solutions—solutions that offer decision-makers freedom to pick and choose the security components that work best in their particular environments.




*The ForeScout platform integrates with popular security and infrastructure solutions, offering bi-directional contextual exchange and intelligent, automated responses. New partners continue to join the ecosystem and Extended Modules are constantly under development to expand the platform's capabilities to third-party security management tools.*

# See Multivendor Orchestration In Action

At ForeScout Technologies, expanding security tool orchestration is a no-holds-barred initiative. We're all in. We are dedicated to integrating leading network, security, mobility and IT management products with our security platform—to help our customers overcome silos, automate workflows and obtain significant cost savings.

ForeScout has released more than 70 integration modules so far,* mostly due to customer requests, and we plan to roll out new ones rapidly going forward. In addition, custom integrations can be developed via the ForeScout Open Integration Module, which allows customers, systems integrators and technology vendors to integrate key security and management systems with the ForeScout platform.

ForeScout offers many ways to gain greater insight into the ForeScout device visibility and control platform, including:

**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.

**Request a Demo:** Visit the ForeScout demo page to request a personal demo and access a full complement of on-demand demos and video options.

**Use the ForeScout Business Value ROI Tool:** Quantify the business value the ForeScout platform can provide to your organization (as calculated by IDC's Business Value Model) in just 10 minutes.

**Explore ForeScout Base and Extended Modules:** Visit the ForeScout website for extensive resources that show you how to get the most from your existing infrastructure, security tools and people.

Learn more at
**www.ForeScout.com**


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
**Fax** +1-408-371-2284

## About ForeScout

ForeScout Technologies, Inc. is transforming security through visibility. ForeScout offers Global 2000 enterprises and government organizations the unique ability to see devices, including non-traditional devices, the instant they connect to the network. Equally important, ForeScout lets you control these devices and orchestrate information sharing and operation among disparate security tools to accelerate incident response. Unlike traditional security alternatives, ForeScout achieves this without requiring software agents or previous device knowledge. The company's solutions integrate with leading network, security, mobility and IT management products to overcome security silos, automate workflows and enable significant cost savings. As of March 31, 2018, more than 2,800 customers in over 80 countries improve their network security and compliance posture with ForeScout solutions.

*As of March 31, 2018