Device visibility remains a daunting challenge for the modern enterprise. Forescout provides a multifaceted information technology (IT) and operational technology (OT) platform designed to solve visibility challenges for the modern enterprise by providing complete device discovery and classification, risk assessment, compliance, orchestration and automated security controls.

Forescout’s latest release significantly extends the platform’s long-standing reputation for network admission controls and device visibility. In addition to deep device visibility in IT environments, the updated platform uses passive analysis to assess devices at all layers of the OT network, as outlined in the Purdue Enterprise Reference Architecture model. Passive analysis is particularly important in terms of ensuring safety and avoiding disruption of critical services in OT and medical device networks, given the business processes those networks and devices support.

Gartner has recently stated that CIOs and IT leaders who understand the need for higher levels of IT and OT integration and awareness will reach critical mass by 2020. The research firm further predicts that IoT will significantly impact the overall economy, support numerous business process use cases, lead to cost savings for some sectors.

---

1 SANS investigated version 8.1 of the Forescout platform for this review.
2 “Purdue Reference Model for CIM,” www.pera.net/Pera/PurdueReferenceModel/ReferenceModel.html
and represent a significant component to solution-level thinking. Therefore, increased usage of IoT on the enterprise network presents an increased need for device visibility, which Forescout satisfies.

In line with that expectation, we’ve identified six key questions facing modern enterprises and IT leaders:

- What devices are on the network? IT must have a full inventory of all IT, IoT, cloud, data center and OT assets accessing the network.
- How can IT gather and maintain relevant information about any device on the network in order to implement asset management practices?
- How can organizations detect and respond to unknown, insecure or vulnerable devices?
- Once a device gains network permission, how can IT provide assurance that IT, OT and IoT devices are operating to the organization’s security standards?
- How does IT minimize staffing requirements while maintaining the security state in various IT systems, even when adverse device conditions occur?
- Aside from campus and OT networks, how are these questions answered in data center and cloud environments?

This paper will answer these (and other) questions and discuss five major product features of the Forescout platform.

Considering the statistics highlighted in the “SANS Research” sidebar, it is clear why device visibility is such a hot topic. Forescout tackles the requirements of modern enterprises and IT leaders who need to empower their teams and want to get ahead of the proliferation of network-aware devices—providing insight into device discovery, auto-classification of endpoints, risk and posture assessment, automated security controls, and scalability and flexibility. This SANS review answers the key questions as it investigates the core capabilities of the Forescout platform, considering each in the context of the needs of IT, OT and security professionals.

---

**SANS Research**

SANS Institute’s own surveys reveal how organizations suffer when it comes to device visibility, corroborating the concerns raised in the six key questions.

The 296 respondents to the 2018 SANS SOC Survey stated that full inventories are lacking:

- Only 19 of 296 respondents (6%) had a 100% device and endpoint inventory.
- 103 respondents (35%) had a 76% to 99% inventory.
- 174 respondents (59%) had less than 75% inventory.

The 2018 SANS Industrial IoT Security Survey reveals rapid growth in IoT devices, a significant portion of which do not follow the Purdue model:

- Most organizations envision 10% to 25% growth in their connected devices for the foreseeable future.
- A further 32% of IoT devices connect directly to the Internet, thus bypassing traditional security layers as referenced in the Purdue model, which presents a significant risk should an IoT device suffer a compromise.

---


In our review of the Forescout platform, it was easy to see the larger tapestry against which Forescout could be a useful tool to counter threats to the organization. While there are multiple scenarios in which Forescout would be an asset, we investigated four specific instances the author has encountered firsthand:

- **Inability to discover and classify assets networkwide**—Without a well-maintained configuration management database (CMDB), it is incredibly difficult to have an accurate networkwide view that can be both searched by analysts and consumed in a downstream, data-dependent system like a SIEM tool. When a SIEM system receives metadata (such as name, owner, CVE and location), it can use that metadata when processing other event data to generate an alert. When data in the CMDB is also present in the SIEM system, analysts have a significantly lower click rate because they don’t have to look up data in many different systems. Forescout can help consolidate the real-time view of assets for integration or import, thanks to its ability to discover and provide in-depth context for devices across all environments—the campus, data center, OT networks, AWS and Azure cloud, and VMware—and supply a single view of organization-wide assets. This capability is integral to providing the level of asset awareness that security operations centers (SOCs) need when reviewing alerts.

- **Users with elevated access (local admin) disabling security tools**—It is common to have users with admin rights turning off a security tool in response to a real or perceived issue. Forescout, through its automation features, re-enables security tools to maintain device compliance and provide a notification to security admins who can then resolve the issue and fine-tune the settings.

- **Users connecting unauthorized devices to the LAN**—Vendors, external auditors, temp workers and others routinely connect to corporate networks with non-corporate computers, digital media devices using peer-to-peer networking, unauthorized wireless access points or even small computers the size of a deck of cards with a “security” distribution installed. Regardless of the source, organizations face considerable risk from unauthorized devices accessing the network via a wired connection. Forescout can be configured to identify rogue devices, even if the user has cloned the MAC address of an authorized device such as a rarely used PC that will not be noticed for several days.

- **Scattered infrastructure staff and numerous systems**—It is not uncommon for incident responders to consult half a dozen different infrastructure systems and staff to gather various data in response to a single threat incident. Forescout streamlines data collection processes by providing a single focal point for device data. It organizes a significant amount of observed and collected data about an endpoint as it connects to and uses network resources. Examples include port/switch information, network-accessible services, user data, recently running processes and services, and vulnerability data.
The Forescout platform provides a wealth of endpoint device discovery and visibility options, and it does so through a highly unified interface that follows a natural flow from left to right. Forescout’s primary console is so well-designed that one can get the impression that the system is “simple”—even though its capabilities and features are deep and rich.

Interface Simplified
The user interface is designed to provide the information needed expediently. Forescout’s primary console provides tools that reflect what the user actually does, keeps things simple, is consistent, maintains high utility and is arranged to make it very easy to locate endpoint data. For example, the upper section of the left panel selects the primary view and the lower section applies filters, as needed (see Figure 1).

As the user applies views and filters, the results are updated in the upper primary view and are responsive to the tab selected (home, asset inventory or policy). The full details of a selected device appear in the Host Details pane. Last, each of the three navigation views has its own search capability, a handy feature that simplifies investigations.

New to the latest iteration of Forescout is a customizable dashboard. An analyst can configure a dashboard to provide a consolidated view of the entire device landscape across all environments or tune the dashboard to provide a view for the security operations team. See Figure 2 for an example of the detail the dashboard shows.
Device Discovery Options

Forescout features a variety of device discovery options, offering detailed visibility to the endpoints connected to the network—be they on premises, in the data center or in the cloud. The options include learning from existing network sources and full-traffic monitoring. These methods use passive network discovery, which collects data about endpoints as they come onto the network (also referred to as admission events).

Full-traffic monitoring is attained by actively monitoring traffic from a device through network extraction of data provided by a SPAN/mirror port or a TAP.

Forescout’s different passive and active techniques play a key role in enabling customers to gain 100% device discovery and visibility without having to redesign the network or deploy additional hardware.

Passive Network Device Discovery

Forescout leverages a wide variety of techniques to passively identify endpoints with minimum network intrusion or reconfiguration. For medical, ICS, SCADA and other OT networks, the ability to passively identify assets with no network change or disruption is critical, to avoid impacting the line process.

Passive discovery methods include monitoring DHCP leases, receiving SNMP traps from dozens of network device manufacturers, monitoring RADIUS connections, receiving NetFlow data, polling network infrastructure devices and wireless controllers, querying a CMDB and traffic monitoring via SPAN. Flow data can also be used to profile systems because traffic flow can help define a device’s function. These techniques all occur “naturally,” and Forescout’s structure leverages all of those events. Forescout also supports discovery for data center and cloud environments through API integrations.

Active Profiling and Rogue Device Detection

In contrast to passive techniques, Forescout’s active techniques use both network and device querying. Each of these feature sets can be enabled on a segment-by-segment basis. That way, at the initial network connection event, the platform can prompt non-corporate users to authenticate over a captive web portal, which in turn means they can authenticate against a variety of different authentication stores and establish user identity at the very beginning of a network connection.

The benefit of this technique is that Forescout maintains the “user to IP to MAC address” correlation as endpoints arrive on the network. The obvious attack vector is to clone and then attempt to reuse an authorized device’s MAC address. Because Forescout is the LAN and WLAN gatekeeper, when the cloned MAC address connects to the network, Forescout immediately detects the spoofing event and can take appropriate actions to block the attacker.
On initial network connection and periodically thereafter, Forescout also collects an inventory of installed applications, packages, vulnerabilities and system compliance states via remote Windows Management Instrumentation (WMI), remote procedure calls and SSH. The system will also query switches every 60 seconds so that it has visibility into OSI Layer 2 for the enterprise.

The platform has a variety of active service and software discovery capabilities. At the lowest level, the system can run the well-known nmap scanning tool to fingerprint the IP stack and operating system (see Figure 3).

Data Center and Cloud Asset Inventory

Forescout queries specific cloud systems through API calls enabled through a plug-in module, like many other cloud integrations today. This enables cloud asset inventories to be displayed together with local asset inventory.

For AWS, the platform retrieves Elastic Compute Cloud (EC2) instance or endpoint configuration information, identity access management users and virtual private cloud configuration information. The platform also detects Elastic Block Store (EBS) encryption status. The AWS plug-in can be set up for read access to support visibility and read/write for control functions. Forescout has flexible policy settings to ensure cloud environments are maintained in accordance with the organization’s security policies. For example, analysts can set policies to determine which security groups should be attached to EC2 instances. See Figure 4.
Forescout has similar capabilities for Azure. These capabilities bring cloud systems into a centralized asset awareness and management plane. It can read VM instances and VNets and monitor delete protection status.

For an on-premises cloud provided by VMware, Forescout retrieves highly granular VM host data and reads guest OS properties. VMware NSX, which is an integral part of VMware’s software-defined data center strategy, can also be co-managed along with other data center and campus network segments. See Figure 5.

Without this single asset inventory plane provided by Forescout, analysts would have to extract data on an as-needed basis and manage a cobbled-together inventory, which would have to be painstakingly maintained by importing CSV data into Excel and struggling through unwieldy spreadsheet functions and vLookups across multiple tabs in order to resolve heterogeneous data into a consolidated asset view.

Classification and Asset Management

Once devices are discovered on the network, Forescout automatically classifies them by mapping device properties against a library of thousands of device profiles. The result is an inventory of devices that is searchable based on asset categories. Forescout has dozens of functional categories, ranging from traditional IT devices and healthcare devices to enterprise IoT and ICS/OT devices.

Organizations can use Forescout’s asset inventory as a single source of insight into all of their assets. Or, they may continue to use their CMDB platform and create bidirectional communication between Forescout and the CMDB to send all of Forescout’s device intelligence, including classification, in real time.

Network Extraction

Organizations can significantly increase asset discovery and asset intelligence by enabling network extraction through a SPAN/mirror port or a TAP. Forescout mines full packet capture data by performing protocol parsing and packet inspection and using the data to auto-classify devices into three dimensions: device function and type, OS and vendor and model.
Network monitoring is particularly important when it comes to ICS devices and OT networks. Forescout supports parsing more than 60 ICS protocols. When connected to a SPAN port at Supervisory, Level 3, of the Purdue model, the system uses the natural access control boundary and therefore allows for real-time OT device discovery through nonintrusive means.

Forescout has robust network extraction capabilities that also uniquely assist healthcare organizations. The platform has endpoint detection and classification support for the top 20 medical device manufacturers along with many others. Forescout can also handle medical imaging data flows and system traffic using the Digital Imaging and Communications in Medicine (DICOM) protocol. This protocol visibility is a huge boon for not just hospitals but all healthcare organizations, providing visibility for remote offices, diagnostic centers and any organization that consumes medical imaging, including insurance providers, medical colleges, and test and quality assurance environments.

When Forescout is monitoring the network segments and DICOM data flows into monitored environments, organizations have a more complete picture of which devices are using imaging data. As a result, they have a more complete picture of protected health information, which helps ensure data security compliance. Figure 6 illustrates Forescout visibility into medical devices.

**Auto-classification**

Accurately auto-classifying network assets based on observed data allows Forescout to create contextual policies based on device type. IoT and OT devices can’t support an agent, which makes it necessary to look beyond traditional authentication approaches to apply access control policies.

The Forescout policy engine uses collected device intelligence to automate workflows for populating a CMDB. This will help keep the organization’s CMDB current and accurate. Forescout can send an event to several different SIEM solutions via syslog or a more direct integration; apply network segmentation via integration with next-generation firewalls (NGFWs), network infrastructure and software-defined networking technologies; and notify an administrator of unknown devices.

![Figure 6. Medical Device Classification by Device Function](image)
Forescout’s device auto-classification process has these main aspects:

- Agentless data collection (See examples provided in previous discussions of discovery and network extraction.)
- Ability to map device attributes to out-of-the-box device profiles, enabling devices to be classified by their function, OS and vendor and model
- Device sorting by OS and vendor and model, providing a full asset inventory
- Forescout device cloud, a crowdsourced device repository used to improve device identification (Organizations can still receive new device profiles if they choose to opt out of device cloud.)

As illustrated in Figure 7, the Forescout classification engine maps devices into a wide variety of device profiles and functions. Once device attributes are identified and classified, the endpoints are added to asset groups. When the engine cannot find an exact match, the analyst can manually classify the device and, if desired, share unknown device information with Forescout’s device cloud R&D team. Forescout updates its device profile library on a monthly basis.

Risk Assessment and Device Compliance

Once analysts gain confidence and familiarity with Forescout 8.1’s ability to discover and auto-classify devices, they can tap into the platform’s risk assessment and device compliance capabilities. The platform has more than a dozen predefined policy enforcement templates that organizations can quickly adapt to meet their needs. For example, security teams can use Forescout’s overall endpoint compliance template to assess client firewall status, remove unauthorized applications by application type and then check for specific compliance settings such as current antivirus and OS patch levels. Once the policy has been configured, system admins can roll the policy out by IP segment or apply a policy network-wide.

To provide a single source of truth for device compliance state, Forescout provides integrations with a variety of enterprise tools—including vulnerability assessment tools, endpoint protection tools, patch management, endpoint detection and response platforms, and IT service management systems.

The threat policy is also important to OT networks. As an example, organizations can configure this policy specifically to check for dual-homed systems, which can provide an unintended bridge between IT and OT networks.
Maintaining Compliance

Not every device attached to the network is deployed in a secure configuration. This is why analysts can configure Forescout to assess risk in real time at a network admission event or soon after as a device is profiled, and then take appropriate action.

In particular, organizations are adopting and installing IoT devices at an accelerated pace: HVAC, building monitoring, conference rooms, multifunction printers and the like can all benefit from Forescout’s approach of assessing a device’s posture as early as possible.

For enhanced risk posture assessment, Forescout integrates with mainstream vulnerability assessment (VA) scan tools. The Forescout platform enables organizations to initiate a VA scan for segments under network admission monitoring. Once the scan is complete, results can be sent back to Forescout. Analysts can remediate manually on a case-by-case basis, or the Forescout platform can be set to automate remediation. That means if the vulnerabilities are critical enough, the platform can isolate the endpoint onto a VLAN at the switch level or trigger installation of a patch by a patch management platform.

These policies are provided out of the box (see Figure 8).

Forescout makes it easy to complete multiple compliance checks. Figure 9 illustrates a particular system within AWS being identified as out of compliance.

As shown in Figure 10, further detail detects how a system is out of compliance and highlights why that system failed its compliance check.
Because Forescout can perform WMI-based remote device query, it has application awareness and can apply that application awareness for several purposes. Figure 11 shows an alphabetical list of applications, how many hosts are running a given application or service and which applications are on the “Blacklisted applications” list.

These checks help the security team isolate malicious software or policy violations and help the operations team identify inappropriate applications in the environment. Quickly finding these results is another example of Forescout’s efficient interface, because with just a few clicks, the analyst has an inventory of suspect endpoints running processes that match a list of blacklisted software.

Forescout makes it very easy to identify where blacklisted applications are in the environment and which hosts were observed running those applications as of the last system check interval, as shown in Figure 12.

When possible, malware and adversaries will establish persistence on a system. They can do so in several ways, with Windows services being one of them. In this example, Forescout allows analysts to sort the service name inventory by hostname so that single or unique service names are easily visible. See Figure 13.

Some results might be easily explained (for example, in a network with one Windows Domain Controller, a single instance of the
DNS service makes sense), but a “FileZilla” service, as seen in Figure 14, may not be authorized. Forescout makes it very easy to identify the system involved and will show the last known user in the asset details. Figure 14 also shows that the user details pane includes key user attributes, saving the analyst from having to consult a secondary system to retrieve critical properties, including group membership, email address and account status.

This figure shows yet another stellar example of Forescout’s highly efficient interface, data collection and data presentation. By making key details of the investigation accessible in a single user interface view, Forescout has minimized the hours analysts need to invest in this process.

**IoT Device Proliferation and Assessment**

Organizations today are adding devices that support all kinds of automation—running the gamut from IP cameras and network display devices to HVAC controllers, environmental monitoring stations, and security and fire control systems. It seems that every semi-intelligent device has an RJ-45 jack or built-in wireless. Because of this near ubiquity, device proliferation is a very real problem. The Forescout platform can help minimize risk presented by IoT device proliferation. First, the platform can discover and classify all IoT devices so there are no blind spots. Next, it can detect factory default or weak, commonly used credentials on network endpoints by leveraging its built-in credential database for SSH, Telnet and SNMP protocols. Overall, Forescout can mitigate risk through device discovery and classification as well as by assessing IoT devices, alerting analysts and proactively limiting or blocking the device from the network, as illustrated in Figure 15.
OT Vulnerability Assessment

New as of version 8.1, Forescout can passively scan OT/ICS devices for vulnerabilities to ensure that OT/ICS processes are not adversely affected. Figure 16 is an example that shows devices Forescout found with a “High” host criticality level.

Automating Controls

So far, several examples presented demonstrate Forescout’s ability to automate host and network controls. For example, the platform inspects devices continuously and can take a specific host or network action if a device’s compliance state changes. Examples include launching a network scan or vulnerability scan, forcing antivirus or patch updates or taking an action on systems with blacklisted applications. The platform can also send user notifications via email, browser or balloon pop-up prior to enforcing any host or network controls, so users have the chance to self-remediate. The platform can also restrict devices to specific segments via VLANs, access control lists (ACLs), virtual firewalls and NGFW tags; perform IoT device and credential checks; and launch a variety of cyber incident response scenarios.

Figure 17 shows some of the control actions Forescout provides as configured by default. All of these actions can be automated using Forescout’s robust policy engine framework, which uses simple if/else Boolean logic, making the platform easy to use and configure.
Device Auto-mapping into Target VLAN

As previously discussed, Forescout classifies and assesses devices on initial network connection and continuously for as long as they are on the corporate network. As the system identifies users or devices in particular groups—for example, human resources, IT, finance, call center, printers and IP cameras—the system can segregate these users into their respective VLANs or apply a restrictive ACL (be it custom developed or chosen from an ACL library) on the switch. These functions provide 802.1X-like behavior without the deployment complexity or requirements for network redesign or any hardware and software upgrades.

Device Auto-remediation

Forescout’s policy engine makes it easy to view and edit a policy definition as appropriate. For example, corporate endpoints require that antivirus be installed and running. Sometimes these agents get out of date or a user with elevated access has either stopped or disabled the service. Upon connecting to the network, Forescout can detect that the antivirus agent is installed and enabled. If definitions are older than one week, it can remediate the devices by updating the antivirus on the endpoints and then notify users that the antivirus is being updated on their system. Organizations can opt to also apply network restrictions while the device is being remediated; as shown in Figure 18, we could limit network access until remediation is complete by putting this device into a restricted VLAN.

IoT Device Segmentation

With more and more devices that can’t support an agent or authentication when connecting to the network, it’s important to apply a strategy to onboard these devices securely. For example, a marketing user doesn’t need to have access to IP cameras. Forescout’s classification and control automation allows analysts to segment IoT devices into their own zone, thereby ensuring only credentialed users can access IP cameras and that the IP cameras talk to only DVR recorders. Because Forescout integrates with leading switch and NGFW vendors, it provides flexibility to enforce segmentation at multiple network layers based on the network design. For example, segmentation can be enforced at the switch layer by ACLs or VLANs, or it can also be enforced by the NGFW if some of your access switches don’t support ACLs.
Figure 19 shows an example of an IP camera being placed in its own segment via ACL and NGFW tags, with access limited to privileged admin users and DVR recorders.

**Incident Response for Known IoCs and Threat Intelligence**

One of the core SANS tenets is, “Prevention is ideal; detection is a must; and detection without response is useless.” Forescout’s indicators of compromise (IoC) integration and scanning modules enable an enterprise to adhere to this philosophy:

The platform’s threat hunting capabilities enable security teams to keep up with recent threats. Forescout has a wide variety of capabilities in the IoC integration module, which can be fed by a variety of threat intelligence providers. We identified five of the most useful capabilities and the scenarios they help resolve by automating host and network controls:

- **Known file IoCs stored as both a binary file hash identifier and a process identifier**—Because of this, Forescout can kill off a suspect binary that’s found running, while files present on disk can trigger further action.

- **Real-time monitoring**—Forescout’s automation capabilities allow it to monitor real-time network sessions for command-and-control (C2) IP addresses and DNS hostname queries. If a device is communicating to a C2 IP address or DNS name, it can be found, whether it is managed or not. The platform can automatically restrict or block access from vulnerable devices and send a notification to the administrator.

- **System scans for potential abnormalities**—Upon initial connection to the network for a NAC-monitored segment, the platform scans the endpoint for known hash values and registry key entries, the presence of a file identified by a hash value, an installed service by name and mutex objects. Forescout handles scanning for these points because malware can use any of these techniques as it executes on a system. The resulting IoC table can be exported, so security admins can build up a history of IoC criteria used over time.

- **Notifications**—Like other policies defined within the system, Forescout can notify an admin via email or initiate a remediation action, reducing the time required before action can be taken on a potential threat.
• **IoC repository**—Forescout’s IoC repository stores key details: date reported, severity, threat intel source, and name and file details (name, hash and type, and size). For example, if a host protection system notifies a security analyst that it has identified a new malicious browser extension, the analyst can add this IoC to the inventory as a “user-defined” IoC, sweep the enterprise and remediate as necessary (see Figure 20).

**Orchestration Through Integration**

Forescout provides a wide variety of direct integrations with third-party systems that help maximize your IT investment. With the right integration, the intelligence and capability of one system can be applied across the enterprise so the contextual insight provided by a focused, targeted solution can be generally applied elsewhere. Let’s look at one of the many use cases Forescout can solve through integration.

For example, Forescout has integrations with several endpoint detection and response (EDR) solutions. EDR applications are more likely to be licensed and provisioned for end-user systems because the end user is a common target for attackers. We identified two common EDR scenarios in which Forescout can be useful:

- **EDR agent to IP segment validation**—Forescout can run a check against IP segments that should have an EDR agent as the endpoint connects to the network and is within scope for a given EDR deployment. For example, a user may connect a laptop or computer to the network that was moved from one location to another. If the agent is not present, Forescout can notify an administrator, push the client to a remediation network, initiate EDR agent installation and even restrict access to the network.

- **Attack alerts and IT hygiene**—When an EDR platform detects an issue, it can share an indicator of attack (IoA) or IoC with Forescout, including details such as the file hash. Forescout can restrict or block access from that malicious device and take that IoA/IoC and search the network for similar matches.
Enterprise Scalability and Flexibility

Like many mature enterprise management systems, the Forescout platform can be deployed across devices using different models—centralized, decentralized or hybrid—and can include a mix of physical and virtual appliances. The platform supports failover clustering for organizations with a need for high resiliency.

A centralized deployment will co-locate all appliances in a primary data center and then configure a variety of forwarding techniques for remote locations. A decentralized deployment has appliances sized for network segments based on the number of endpoints and LAN monitoring requirements, with distributed devices reporting back to a central enterprise manager. Hybrid models mix these centralized and decentralized models; for larger sites, a dedicated appliance can be deployed, while for smaller remote locations Forescout can use other passive collection techniques (DHCP helper, NetFlow, infrastructure polling, etc.) to achieve device visibility without deploying appliances at every site. Organizations can deploy different-sized appliances at different locations. Larger devices have a higher port density, which supports multiple SPAN ports for network extraction functionality.

Conclusion

The Forescout platform is a strong addition to the infrastructure stack for the enterprise because it provides holistic device visibility and control from the first point a device touches the network or is provisioned in either VMware, AWS or Azure. Once devices are identified, its full-stack management capabilities provide the foundational elements to keep devices off the corporate network that don’t belong, maintain the devices that should be on the corporate network and provide an orchestration platform for IT, IoT and OT devices.

Forescout is much more than a device data collection and presentation platform. The platform can leverage the breadth of collected data to provide holistic device visibility, use all of that data to take action against misconfigured endpoints and maintain the organization’s security posture. It can also integrate with many other related products and pull data from secondary systems. Collectively, these capabilities can further strengthen the overall organizational security state.
About the Author

**Don Murdoch** is a SANS community instructor specializing in incident response and security operations. A solutions-oriented IT director and consultant, he has hands-on experience leading software/infrastructure/system development efforts for financial and healthcare systems, including requirements definition, executive-level strategy and communications, solution design, architecture, deployment, production and dissolution. Don is the author of two prominent blue team handbooks, the first of which focuses on incident response and the second on SOC, SIEM and threat hunting. He holds the SANS GSE, Cyber Guardian Red and Blue Team and 17 other GIAC certifications, and he is also a certified TOGAF Enterprise Architect and SABSA Chartered Security Architect. Don is the author of two industry-impacting Blue Team Handbooks.

Sponsor

SANS would like to thank this paper’s sponsor:

<> FORESCOUT
<table>
<thead>
<tr>
<th>Event Name</th>
<th>Location</th>
<th>dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Philippines 2019</td>
<td>Manila, PH</td>
<td>Sep 02, 2019 - Sep 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Munich September 2019</td>
<td>Munich, DE</td>
<td>Sep 02, 2019 - Sep 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels September 2019</td>
<td>Brussels, BE</td>
<td>Sep 02, 2019 - Sep 07, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Canberra Spring 2019</td>
<td>Canberra, AU</td>
<td>Sep 02, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Network Security 2019</td>
<td>Las Vegas, NVUS</td>
<td>Sep 09, 2019 - Sep 16, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Oslo September 2019</td>
<td>Oslo, NO</td>
<td>Sep 09, 2019 - Sep 14, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai September 2019</td>
<td>Dubai, AE</td>
<td>Sep 14, 2019 - Sep 19, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>Oil &amp; Gas Cybersecurity Summit &amp; Training 2019</td>
<td>Houston, TXUS</td>
<td>Sep 16, 2019 - Sep 22, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Rome September 2019</td>
<td>Rome, IT</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Raleigh 2019</td>
<td>Raleigh, NCUS</td>
<td>Sep 16, 2019 - Sep 21, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bahrain September 2019</td>
<td>Manama, BH</td>
<td>Sep 21, 2019 - Sep 26, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS San Francisco Fall 2019</td>
<td>San Francisco, CAUS</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas Fall 2019</td>
<td>Dallas, TXUS</td>
<td>Sep 23, 2019 - Sep 28, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Kuwait September 2019</td>
<td>Salmiya, KW</td>
<td>Sep 28, 2019 - Oct 03, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Northern VA Fall- Reston 2019</td>
<td>Reston, VAUS</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Cardiff September 2019</td>
<td>Cardiff, GB</td>
<td>Sep 30, 2019 - Oct 05, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Riyadh October 2019</td>
<td>Riyadh, SA</td>
<td>Oct 05, 2019 - Oct 10, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Doha October 2019</td>
<td>Doha, QA</td>
<td>Oct 12, 2019 - Oct 17, 2019</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>