Case Study

FORESCOUT

# Hubspot

## Innovative inbound sales and marketing solutions provider gains device visibility and automates security management with Forescout

**7**
**extended modules integrated**

**1**
**day installment for complete visibility**

**13H**
**response time to an issue spanning over 200 locations**

HubSpot

**Industry**
Marketing Automation

**Environment**
10,000 endpoint devices with diverse operating systems (mostly Apple Macintosh, along with Microsoft Windows and Linux), distributed across nearly 2,000 employees in eight locations worldwide

**Challenge**

- Discover network-connected devices and map users and user activity to devices without impacting productivity and workflow
- IT asset management and tracking
- Detect malicious file downloads and prevent propagation
- Enforce security compliance

## Overview

HubSpot provides a highly innovative platform for inbound online marketing programs – especially for small-to-medium-size businesses. The fast-growing company helps corporations attract traffic, generate leads and manage and track marketing initiatives, campaigns, and customer relationships from a single, centralized location. HubSpot employs nearly 2,000 people across eight worldwide locations. Approximately 10,000 devices populate its computing environment, comprising a mix of Apple® OS (70 Percent), Microsoft Windows® and Linux® operating systems.

Nick Duda, principal security engineer at HubSpot, and his team needed a way to gain better visibility of devices on their network and associate these devices to potential malicious activity. Additionally, HubSpot was looking to improve detection of advanced threats and boost intelligence sharing in their security operations center (SOC) among all their core security products. The company turned to the Forescout platform and multiple Forescout eyeExtend Modules to successfully drive its digital transformation and automate security processes.

## Business Challenge

***"We had no visibility. We didn't know what was on the network."***
**— Nick Duda, Principal Security Engineer at HubSpot**

With more devices than users and a diverse environment, HubSpot was faced with the same challenge encountered by most dynamic, fast-growing organizations, that is, lack of device visibility, which can lead to a whole host of security and compliance issues. The HubSpot security team understood that visibility is a baseline for addressing all the other challenges they had to tackle, which included:

- Orchestrate sharing of device, user, compliance and threat-intelligence data with third-party solutions to accelerate incident response and automate security and IT operations
- Discover, track and block threat activity across local network segments and east-west traffic
- Identifying and tracking assets

### Security Solution

- Forescout platform
- Forescout eyeExtend for Palo Alto Networks Next Generation Firewall
- Forescout eyeExtend for Palo Alto Networks WildFire
- Forescout eyeExtend for Splunk
- Forescout eyeExtend for Rapid7
- Forescout eyeExtend for CrowdStrike
- Forescout eyeExtend Connect
- Forescout Cloud Security Solution for Amazon Web Services

- Seeing devices on the network and ensuring that they are properly secured and patched in accordance with corporate policy, regulatory compliance and privacy standards
- Identifying and tracking computing assets to enable their SOC to remotely lock down lost, stolen or compromised systems
- Associating IP addresses to users for response to malicious URL activity
- Improving detection and response to advanced threats
- Sharing valuable device and threat intelligence across the entire environment
- Detecting new systems as they connect to the network, applying appropriate policies and addressing vulnerabilities to ransomware and other threats with greater immediacy

## Why Forescout?

When Duda joined HubSpot in 2014, building security compliance checks into all of HubSpot's endpoints was top of mind for the company's CSO. "How do we know which devices are encrypted and which are not?" was the question he posed to his security team. Determined to come up with a viable solution to the device visibility issue, Duda decided to give the Forescout platform a try. Within a day, Duda had complete visibility into the entire array of network-connected devices and endpoints at HubSpot and was able to easily access information about operating systems and applications in use, security posture, patching status, vulnerabilities and more. Needless to say, the CSO was impressed, as were Duda's colleagues.

From there, starting with the introduction of the Forescout eyeExtend Connect, the HubSpot security team saw the huge potential of the Forescout platform and leveraged its ability to integrate data exchange among solutions from multiple security vendors. This laid the groundwork for an automated and orchestrated security infrastructure, with the Forescout platform as the centerpiece.

## Business Impact

### Mapping Users to Devices

In an environment like HubSpot, where employees use a highly diverse set of devices, granular device visibility and device-to-user mapping is essential. Previous content protection solutions couldn't see who was trying to access what. The Forescout platform rapidly and dynamically identifies and categorizes devices—even non-traditional ones, like smartphones, tablets and Internet of Things (IoT) devices—that are already on or joining the network. It achieves this without requiring software agents or previous device knowledge. Next, it pinpoints which user is logged into each device and which device is accessing various content based on the user's name and department. Duda and his team now rely on the Forescout platform to determine the device type, user, owner and operating system, as well as device configuration, software, services, patch state and the presence of security agents.

After resolving the device-visibility issue, HubSpot made the decision to implement Palo Alto Networks NGFWs to further boost network security. Once they were deployed, Duda and his team needed a way to get the Forescout platform data to the NGFWs. Once again, it took less than a day. The team implemented a proof of concept for the Forescout eyeExtend Module for Palo Alto

> "Forescout is like having an automatic threat hunter on the team that hunts for threats around the clock across our global network. We are now addressing issues that we couldn't tackle before. Tasks that would have taken hours now take just minutes."
>
> — Nick Duda, Principal Security Engineer, HubSpot

## Use Cases

- Device visibility
- Asset management
- Device compliance
- Network access control
- Incident response
- Network segmentation

## Results

- Vastly improved visibility of devices and endpoints connecting to the network, including security health, compliance status and user activity
- Faster detection and resolution of advanced threats through interoperability and threat data sharing with NGFWs, SIEM solutions and other security tools
- Automation of otherwise labor-intensive scanning and patching processes
- Sharing IoC intelligence among tools, resulting in SOC efficiencies in global threat hunting, investigations, response and remediation

Networks NGFW and was able to get relevant device data to the appliances in no time. Now, with complete visibility to every device across the entire environment, Duda and his team can quickly detect malicious downloads and have significantly improved overall incident response.

### Advanced Threat Detection

Concerned about the propagation of advanced threats across the corporate environment, HubSpot's CSO raised another critical concern: "How do we know that if someone downloads an infected file, others on our network don't have it?" Duda and his team turned to Forescout eyeExtend for Palo Alto Networks WildFire™, which provides real-time visibility and compliance management of endpoints, facilitates effective response to advanced persistent threats (APTs) and zero-day threats and uses automation to efficiently and accurately mitigate endpoint risks and advanced threats.

"Just the other day, we saw an example of how the Forescout platform solves the issue of east-west malware propagation. One of our users downloaded a malicious file from the internet, and, thanks to the integration of the Forescout platform with Palo Alto Networks WildFire, we were able to scan the whole network and rapidly look for other instances of infection," said Duda.

Once Palo Alto Networks WildFire detects that a user has downloaded a malicious file, it analyzes the file and, via eyeExtend for Palo Alto Networks WildFire, shares indicators of compromise (IoC) data with the Forescout platform. The Forescout platform, in turn, actively scans connected endpoints for the presence of this malicious file and passively monitors the network for this IoC as well. Even if certain locations don't have Palo Alto Networks NGFWs in place, the Forescout platform can use the data it gathers and engage in both active scanning and passive listening.

"Forescout is like having an automatic threat hunter on the team that hunts for threats around the clock across our global network," asserts Duda. "We are now addressing issues that we couldn't tackle before. Tasks that would have taken hours now take just minutes."

> "Forescout helps drive the intelligence of the SOC and integrates data feeds with all of our core security products."
>
> — Nick Duda, Principal Security Engineer, HubSpot

The outbreak of the WannaCry ransomware provides another example of the solution's advanced detection capability. By scanning entire subnets quickly and prioritizing and automating patching, the Forescout platform saved HubSpot's security practitioners many hours of labor that otherwise would have been spent on manual scans and patching efforts. New systems that join the network are immediately detected, checked for vulnerabilities and patched to safeguard against potential ransomware infections.

### Orchestration with Splunk SIEM

Forescout orchestration with the Splunk® security information and event management (SIEM) solution is driving comprehensive threat intelligence at the HubSpot SOC and enabling real-time views into endpoint activity.

> "Forescout enables us to tackle complex security challenges. We build something, set it and forget it. Basically, we are getting technologies to talk to one another and then solve problems in an automated way. Automation allows our employees, our security team and our security operations center to focus on what really matters."
>
> — Nick Duda, Principal Security Engineer, HubSpot

Because Forescout eyeExtend for Splunk allows bi-directional communication with Splunk; analysts gain detailed visibility into devices on the network, including bring-your-own-devices (BYOD), IoT and guest devices. Whenever the Forescout platform detects malware or suspicious activity, it shares information with Splunk. This helps enhance Splunk's ability to correlate and prioritize incidents and then take appropriate remediation actions on endpoints, as required. "Forescout helps drive the intelligence of the SOC and integrates data feeds with all of our core security products," Duda explains.

Duda summarizes the orchestration benefits of the Forescout platform in one word: automation. "Forescout enables us to tackle complex security challenges. We build something, set it and forget it. It allows our technologies to talk to one another and then solve problems in an automated way. Automation empowers our employees, our security team and our security operations center to focus on what really matters," he summarizes.

## Open Integration and Customization

The Forescout platform allows bi-directional information sharing and process automation among security and IT management products using common, standards-based protocols. This ability to create and enhance capabilities has changed the way Duda views security and IT management. "I consider Forescout to be an enterprise manager for all of our technology. The Forescout platform can take point solutions—whether they are security, IT management or whatever—and tell them valuable information about an endpoint, allowing these tools to make more intelligent decisions," says Duda. His point is nicely brought home by the way HubSpot automates help desk requests by integrating their help desk software with the Forescout platform:

- Help desk agents now automatically see where a system resides on the network, including its compliance status
- Help desk staff receive pre-populated help desk tickets—including incident details—instead of having to manually enter user and device data into help desk tickets
- HubSpot resolved a global configuration issue across its 200 conference rooms in 13 hours, which Duda estimates would have taken 100 hours without the Forescout solution

HubSpot has now implemented the Forescout platform across all HubSpot systems globally. The Forescout platform is also integrated into HubSpot's corporate Amazon Web Services (AWS) platform for increased visibility to the cloud. In the coming year, Duda looks forward to further evolving HubSpot's advanced threat detection and automated response capabilities by taking advantage of other Forescout eyeExtend modules for CrowdStrike® and Rapid7®. He's also excited about the next big initiative, which involves combining the power of Palo Alto Networks and The Forescout platform to dynamically segment, block and contain network traffic, complete with network access control lists that will define different access rules and policies for guests and employees connecting to the network.

FORESCOUT

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