Case Study

Boden

Fast-Growing UK Fashion Company Relies on ForeScout to Expand Visibility, Monitor Device Connectivity and Ease Management

INDUSTRY

Retail clothing

ENVIRONMENT

3 CounterACT appliances serving 6 global sites and 2 data centers comprising 7,500 predominantly Windows endpoints and some Mac endpoints, consisting of desktops, laptops, handheld phones and tablets.

CHALLENGE

- Reduce security risk by getting better visibility to devices connecting to the network, including Macs, personally owned devices and unauthorized devices
- Manage device connectivity across a geographically distributed environment
- Integrate with other security solutions to share device information and improve incident response
- Eliminate manual network configuration processes
- Support employees and reduce interruptions in productivity

SOLUTION

ForeScout CounterACT® (See, Control and Orchestrate capabilities)

ForeScout Enterprise Manager

Overview

Launched in 1991, Boden is a British clothing company that provides high-quality fashion apparel for the whole family, selling primarily online, by mail order and catalog. The company made its debut with only eight menswear items, and now has a broad presence in the UK, the U.S., Germany and Australia. Boden launched its first brick-and-mortar shop in London in 2004. Its 1,100 employees across six global locations keep the merchandise flowing, shipping tens of thousands of parcels daily from its Leicester, UK warehouse.

The network infrastructure at Boden is largely Cisco®-based, with Aruba® wireless switches, several HP® routers and switches and Juniper Networks® firewalls. Boden has approximately 7,500 endpoints connecting to the network, comprising desktop computers, laptops, handheld phones and tablets. While most of the endpoints run various versions of the Microsoft Windows® operating system, Boden also has a growing population of Mac devices. The retailer hosts its e-commerce sites internally and relies on its IT staff to manage application layers and the infrastructure. The company has three data centers in the UK, which house all sensitive personal and financial customer data and currently run Boden's e-commerce sites. Boden has plans to migrate its e-commerce sites to the cloud within the next year.

Bernard Crane, infrastructure architect, and Lalit Mandalia, head of technical services, at Boden were looking for a solution that would provide expanded visibility into user activity and the devices that connect to the network across Boden's UK headquarters, UK distribution center and U.S. distribution center. Constrained by a relatively small IT staff, they needed a solution that was easy to deploy and that enabled remote management. They were also looking to automate network-related security tasks and monitor endpoints for proper security hygiene. Boden selected the ForeScout platform along with ForeScout Enterprise Manager to provide the IT team with the visibility they required to ensure that rogue endpoints and routers were identified and were prevented from accessing the network and potentially putting the company at risk of a breach or noncompliance.

Business Challenge

"We needed to monitor and secure our endpoints and make sure we had better visibility to what devices were plugging into our network."

— Lalit Mandalia, Head of Technical Services, Boden

At Boden, with the exception of apparel production, which is outsourced, nearly everything is handled in house—from fashion design to order fulfillment to IT and security. In this fast-paced, geographically dispersed environment, a key concern is user behavior. Lack of visibility to these devices—which may be vulnerable due to a lack of proper security controls or may be infected with malware—could potentially put the entire network infrastructure at risk.

RESULTS

- Improved visibility to network-connected devices in its dynamic office and warehouse environments, with detection of endpoints increasing from 4,000 at deployment to more than 7,500 currently
- Virtual appliance deployments of the ForeScout platform provide the ability to manage remotely, easing the burden on its resource-strapped, UK-based IT and security department
- Gradual evolution to a more integrated and coordinated security ecosystem, on Boden's schedule
- Automation of network configuration and access changes save time and effort
- Easy, three-day implementation with minimal client-side configuration
- Potential operational savings of £161,082 annually, or £805,412 over a period of five years

Not wishing to hamper the creativity of Boden's designers and product development team or the productivity of its fulfillment team, Crane and Mandalia needed to get a clearer picture of which employee and guest devices were connecting to the network and get a better fix on device security hygiene—for the sake of ensuring security and gaining an understanding of their IT assets.

"In the last few years, security has become a priority for all businesses, including ours. The threat of somebody plugging in an unknown device and spreading malicious code or a virus across our internal network is quite a scary thought. That's why we decided to deploy the ForeScout platform," remarked Mandalia.

Gaining visibility to unauthorized routers and other rogue devices that connect to the network was just one of the challenges faced by the Boden IT and security team. In addition, they needed a way to:

- Monitor the security posture of endpoint devices and strictly enforce policies that disallow devices that do not have updated antivirus protection
- Integrate and orchestrate IT and security resources for improved response
- Automate and transparently implement network changes when a new device appears on the network without impacting user productivity or interrupting network services

Why ForeScout?

Crane, who had a positive experience with ForeScout at his former job, recommended the solution to Boden as a way to increase visibility and make life easier for the IT team. "The IT resource here is not huge, and I wanted to avoid burdening our staff, so ForeScout was a natural fit for what we were trying to do," says Crane.

He and his team found it particularly easy to introduce the ForeScout platform to the network during the proof-of-concept (POC) phase. Because of its agentless deployment, the ForeScout platform doesn't require any significant endpoint configuration, such as enrollment in a management system or installation of a software agent. In addition, it provides instant visibility into a wide variety of devices connecting to the network—from desktops and laptops to smartphones, network infrastructure components and rogue devices—complete with granular details about devices, users and applications, along with continuous monitoring of security posture.

After supporting the Boden team through the POC process, BlueFort Security, a certified ForeScout reseller in the U.K., helped Boden quickly identify how and where to implement the solution in its network. BlueFort's ForeScout-accredited technical team assisted Boden through the installation and integration phase. Deployment took only three days in both the UK and U.S. locations.

Following purchase and full integration, Bluefort continues to provide Boden with ongoing access to technical expertise, support resources and customer events. "Our initial implementation proved to be so well received that we promptly bought further network infrastructure into scope and continue to work with BlueFort to develop and expand the system," says Crane. "We enjoy working with the knowledgeable BlueFort team and would recommend them to anyone considering investing in the ForeScout platform."

Crane chose virtual rather than physical implementations of the ForeScout solution, extending visibility to all office and distribution centers, including the U.S. facility in Pittston, Pennsylvania. This flexible deployment option enables him

> **In the last few years, security has become a priority for all businesses, including ours, and I think the threat of somebody plugging in an unknown device and spreading malicious code or a virus across our internal network is quite a scary thought. That's why we decided to deploy the ForeScout platform."**
>
> — Lalit Mandalia, Head of Technical Services, Boden

to manage locations via ForeScout Enterprise Manager from the London office, where the infrastructure teams are based.

Business Impact

Uncovering Unexpected Devices

Device discovery is an ongoing process at Boden, and Crane noted that he and his team are always surprised by the number of unaccounted-for devices that the ForeScout platform discovers.

For example, during a recent remodel of one of their offices, ForeScout identified devices related to the building management system that contractors had plugged into an eight-port switch. In addition, at the U.S. distribution center, it's not uncommon for employees to add switches in areas of the warehouse where there is no structured cabling and connectivity is required. Users don't always inform the IT team about their activities. Even so, the ForeScout platform is able to immediately detect these types of devices, classify and profile them and continually monitor device hygiene. At the time of deployment, the ForeScout platform detected 4,000 endpoints, and now it's detecting more than 7,500. All of this visibility provides Crane and his staff with greater control and provides a strong foundation for better security.

Still in the early stages of their evolution with the ForeScout platform, Crane and his team are focusing primarily on fine-tuning its device classification and clarification rules. They are just starting to take action based on those rules.

> **The IT resource here is not huge, and I wanted to avoid burdening our staff, so I think ForeScout was a natural fit for what we were trying to do."**
>
> — Bernard Crane, Infrastructure Architect, Boden

Boden runs different VLANs for its Apple Macintosh estate. Every device that initiates a connection first plugs into a standard data network. When ForeScout identifies a device as a Mac, the device is then switched to a Mac-specific VLAN, a process that is totally transparent to users. The primary reason for segregating Macs is to have better control over the resources that Mac users can access internally and externally. Typically, Macs are used by employees engaged in the creative side of the business, such as product photography, which is done in house, or website design and development.

Enabling Integration with Other Security Tools

For Boden, a big benefit of the ForeScout platform is its ability to integrate with existing software tools to create a more cohesive and coordinated security ecosystem. They plan to leverage this orchestration capability to share contextual insights with their IT, security and management solutions.

Boden has been taking advantage of the easy-to-deploy ForeScout Base Modules, which are providing a foundational level of integration. Recently, the company has been migrating its wireless network to Aruba and creating base-level integration with ForeScout. They are also in the midst of deploying Microsoft System Center Configuration Manager (Microsoft SCCM) for server patching and more robust endpoint management and are using the ForeScout Base Modules for that as well. Down the line, Crane's goal is to go deeper and explore how the ForeScout platform can help them make the most of other tools, such as their vulnerability management solution from Qualys®.

Automation Saves Time, Effort and Money

Aside from the great benefits reaped from increased visibility and control, another important benefit that Boden has derived from its ForeScout deployment is the vast reduction in the amount of time and effort that goes into configuring

> **The whole time-consuming process has now completely disappeared. Effectively, the user makes that change, and the ForeScout platform just deals with it, and we don't have to get involved at all. Our users are happier because they don't see any interruption to the service. It's completely transparent to them."**
>
> — Bernard Crane, Infrastructure Architect, Boden

and implementing network changes when devices connect. In the past, Crane's team members would manually address requests that were in the queue, and that would often entail coordination with the user. For example, if a Mac user connected to the network and wished to access certain applications, the user would submit a request to the service desk, which would remain in the queue until Crane's team was able to get around to it.

As Crane explains, "The whole time-consuming process of making a very simple change has now completely disappeared. Effectively, the user makes that change, and the ForeScout platform just deals with it, and we don't have to get involved at all. Our users are happier because they don't see any interruption to the service. It's completely transparent to them."

Business Value

Translated into business value, ForeScout's calculations indicate that Boden will realize substantial cost savings in multiple areas. Annual savings are estimated at £161,082,* broken down as follows:

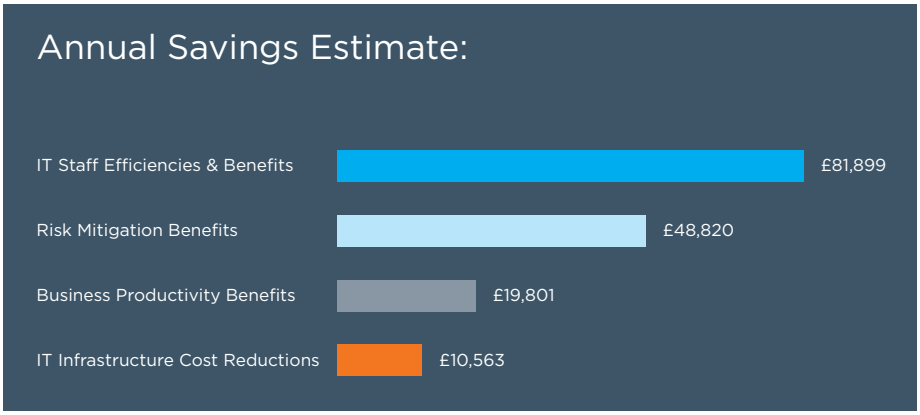

Figure 1. A summary of return on investment using the ForeScout ROI tool (based on IDC methodology), as determined by the firm's SecOps team.

Over a period of five years, Boden will likely save as much as £805,412.

Deepening Exploration of the ForeScout Platform

Crane and his team are evolving with ForeScout at their own pace and are eager to delve deeper. He indicates that the next phase will be "to let it a little bit off the leash and get into more advanced capabilities around identifying the device posture in more detail." For example, he sees the potential for moving devices that lack the latest patches or security protections into restricted VLANs temporarily where they can be updated and then allowed to connect.

Learn more at
www.ForeScout.com

FORESCOUT

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

* One British pound is roughly equivalent to $1.34 USD, as of mid-2018. Conversion rates are subject to change.