CUSTOMER SUCCESS

The Go-Ahead Group plc.

The Go-Ahead Group Fights Off Cyber Attack and Supports a Billion Passenger Journeys a Year with Solutions from Symantec and Threatscape

When a network critical to bus and train service in the UK began to slow down, the IT team at The Go-Ahead Group plc. suspected a cyber attack, and turned to Symantec and Symantec Platinum Partner Threatscape. Results include a malicious worm identified and contained on thousands of devices within 24 hours, a new central remote management capability that conducts daily scans to identify new and unprotected devices, and an estimated 10 percent cost reduction in 36 months.

Rising risk for transport titan

Something was wrong. The network was slowing to a crawl, and much was at stake.

Thousands of buses and trains were in the middle of routes that total 250,000 miles each day for The Go-Ahead Group plc, one of the UK's biggest transport providers. Go-Ahead operates eight bus and three train companies throughout the central and southern UK, supporting a billion passenger journeys a year.

On this day, however, computer services that support the routes were slowing down, and the risk of disruption was growing. Go-Ahead called Symantec, and on Symantec's recommendation, they called Threatscape, a Symantec Platinum Partner and endpoint specialist. An executive at Go-Ahead wanted to know what was happening to the networks. There was an attack, he said, and why wasn't Symantec Endpoint Protection software stopping it?

Threatscape immediately sent an engineer on site, and he detected that computers were under relentless attack by the Conficker worm, a form of malicious code that uses various encryption and stealth techniques to mask its spread across a network. First identified in 2008, Conficker has infected an estimated three million computers worldwide. "Network communication was getting saturated," says Mick Legge, Head of Information Security for The Go-Ahead Group.

ORGANIZATION PROFILE

Site: www.go-ahead.com

Industry: Transport

Headquarters: London, UK

Employees: 26,000

KEY CHALLENGES

The Go-Ahead Group needed to identify and remove a cyber threat slowing a network that is critical to its bus and train companies.

SOLUTION

Go-Ahead turned to Symantec and Symantec Platinum Partner Threatscape for help with Symantec™ Endpoint Protection and Symantec™ Client Management Suite.

BENEFITS

- Elimination within 24 hours of system-wide worm threatening to disrupt critical network
- Identification and protection of thousands of previously undocumented devices in 340 locations from central console
- Daily automated scans identify new and unprotected devices
- Cost reduction with a wide range of business benefits such as centralization, consolidation, and simplification

"Threatscape helped us triage the problem, get the Conficker worm off infected systems, and protect each device with Symantec Endpoint Protection. Within two hours, we knew exactly what was going on, and within 24 hours, we basically put out all the fires."

John Jordan
IT Infrastructure Manager
The Go-Ahead Group plc.

An unexpected source of trouble

The engineer determined that the problem wasn't Symantec Endpoint Protection, which was successfully defending every system it was installed on. "The problem was that the network contained many undocumented and unprotected systems," Legge explains. "People had connected systems to the network and not told Go-Ahead about them, or they hadn't been properly registered."

The unprotected systems didn't seem like computers, Legge adds. They lacked keyboards, but had processors and Windows operating systems embedded, making them vulnerable. "They control digital displays, sell tickets, operate the ticket gates, and power the public address system," says Legge. "The people that plugged them in just thought they were boxes. But if they have Windows, they need protection."

Two-part solution: mend and defend

The team worked quickly to control the attack. "Threatscape helped us triage the problem, get the Conficker worm off infected systems, and protect each device with Symantec Endpoint Protection," says John Jordan, IT Infrastructure Manager at Go-Ahead. "Within two hours, we knew exactly what was going on, and within 24 hours, we basically put out all the fires."

One of the multiple layers of defence that Symantec Endpoint Protection uses to safeguard each device is a rules-based firewall. Threatscape used the central Symantec Endpoint Protection Manager console to push out a stricter firewall policy to all endpoints. "The fact that a firewall was already on each device helped contain the problem a lot quicker," says Stephen Bull, IT Security Analyst at Go-Ahead.

Threatscape then suggested that Go-Ahead conduct a deep inventory scan across the network. "We needed to identify just how prevalent the issue of undocumented and unprotected systems was," says Legge. "Threatscape recommended Symantec Client Management Suite. They did a temporary installation, ran a network inventory, and discovered many more unprotected systems—our device count grew by 40 percent to about 38,000. We said, 'Wow, we need to keep this tool!'"

Centralizing control

Symantec™ Client Management Suite is part of a new centralization strategy at Go-Ahead. The company uses it to enable a lean, centralized IT team to remotely deploy, manage, secure, and troubleshoot systems across the 340 locations of Go-Ahead's 12 companies. "We gain visibility, control, and governance," says Legge. "A relatively small IT team has oversight of a widely distributed and business-critical network."

The initial role for Client Management Suite is to identify devices that have just been added, and ensure that they are protected with Symantec Endpoint Protection. "Our various subsidiary companies had different approaches to security and endpoint management," says Jordan. "Now Symantec Client Management Suite enables us to enforce standardized policies and keep them consistent across all the companies we operate."

Each day, the solution scans the network to map devices. A summary report enables Jordan to enquire about any device that has been added. "On a weekly basis, we need to challenge about 10-15 devices, and that number is coming down rapidly," he says. Another report identifies devices that haven't received security updates in the last seven days. "They are a prime target for closer analysis," says Jordan.

TECHNOLOGY ENVIRONMENT

- **Network endpoints:** 38,000+ including 30% desktops and laptops that are mostly Dell and HP; 30% mobile devices (smartphones, tablets and mobile phones); and 40% ticket machines, ticket readers, displays, and other devices, running mostly Windows 7 and Windows XP

SOLUTIONS

- Symantec™ Endpoint Protection
- Symantec™ Client Management Suite

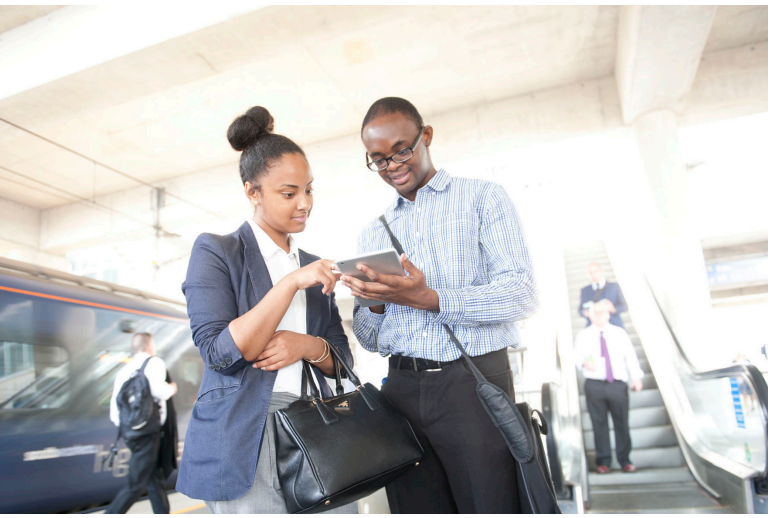
SYMANTEC PLATINUM PARTNER

- Threatscape (www.threatscape.com)
  - Symantec Competencies (Principal): Data Security, Endpoint Management, Endpoint Security, Mobility, Certified Trainer

THREATSCAPE SERVICES

- Critical Incident Response
- Endpoint Security Consulting
- Endpoint Management Solution Design & Deployment
- Custom Scripting
- Support Services

Symantec



> "Threatscape has extraordinary endpoint protection expertise, and they are invaluable to us on a day-to-day basis. Because we have a small IT team, they are a critical resource for us."

Stephen Bull
IT Security Analyst
The Go-Ahead Group plc.

A few months ago, Go-Ahead was awarded a contract to operate an additional train company, adding about 8,000 new employees. The IT team used Symantec Client Management Suite to quickly map the company's devices and plan for their integration. "We can make sure the systems meet our security standards," says Jordan. Go-Ahead kept the trains running seamlessly while the IT team deployed Symantec Endpoint Protection across the new systems.

Centralizing IT

In the next phase of centralization, Go-Ahead created a central IT help desk which has taken over the role of desktop support from IT teams in the individual companies. When a desktop system has issues, the IT team plans to use the ability of Client Management Suite to re-image it remotely instead of troubleshooting it, reducing what could be hours of work to about 20 minutes.

The IT team also plans to centralize patch management with Client Management Suite. "Two or three technicians will be able to push out a patch enterprise-wide," says Jordan. "The job used to be done by two to three IT staff in each of 12 companies. They will all have more time for more valuable tasks."

Ongoing teamwork

Only quick action by Threatscape kept the Conficker worm from causing a major disruption, and the company has been helpful to Go-Ahead ever since. "Threatscape has extraordinary endpoint protection expertise, and they are invaluable to us on a day-to-day basis," Bull says. "Because we have a small IT team, they are a critical resource for us."

Some Go-Ahead business critical applications run on operating systems that are end of life, Jordan adds. "These systems were too old for Symantec Endpoint Protection, and Threatscape helped us deploy older versions of Symantec AntiVirus instead. They know so many little things that we wouldn't have known. That's a big measure of how they help us."

Says Jordan: "Given the time they save us, we estimate that Symantec solutions will help us achieve a 10 percent cost saving within 36 months. They help us be proactive rather than reactive. They give us more time for higher value projects like smart card applications that deliver a better experience for our customers."

For more information

Please contact your local Symantec Sales Representative or Business Partner, or visit:
www.symantec.com/endpoint-protection or

www.symantec.com/client-management-suite

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

About Threatscape

Based in Reading, UK and Dublin, Ireland, Threatscape delivers solutions that perform at scale. It has proven expertise in securing and managing business-critical IT assets at network endpoints, perimeters, data-centres and in the cloud for enterprise-scale clients in the UK, Ireland and elsewhere. It has been awarded Symantec Principal Competencies in Data Security, Endpoint Management, Endpoint Security, and Mobility—recognising its technical abilities, revenue achievements and customer satisfaction. For more details, see www.threatscape.com

Threatscape
SECURING THE DIGITAL LANDSCAPE

Symantec