

Nikon tightens security while simultaneously deploying more open access policies



EXECUTIVE SUMMARY
CUSTOMER NAME · Nikon UK
LOCATION · Surrey, London
INDUSTRY · Technology
COMPANY SIZE · 123 employees
BUSINESS CHALLENGE · Reduce the risk of internal system attack · Increase the level of network security without reducing access and flexibility · Build a more robust network security strategy
NETWORK SOLUTION · Cisco Self-Defending Network
BUSINESS VALUE · Allows a more open and flexible approach to network and system access · Reduces time and resources required to manage security · Enables a more proactive, rather than reactive approach to security · Provides a single, integrated security system that is easy to manage

Cisco Self-Defending Network architecture introduces a single, integrated security solution that enables Nikon to reduce the time and resources required to manage it.

Business Challenge

Nikon was founded in 1917 in Japan and although best known for its cameras, it also makes a range of different products including lenses for glasses, microscopes, and machinery for computer chip manufacture. In 1946, the company launched its first 35mm camera and has since gone on to produce a range of SLR and digital cameras with a global reputation for quality. Nikon ranks in the world's top five camera makers for both consumer and professional products. The UK business, a subsidiary of Nikon Corporation, markets and distributes the company's photographic equipment and microscope products.

As a business, Nikon UK maintains a rigorous computer security policy – for example, using computers physically separate from the main network. It also uses independent systems to view and repair cards from cameras coming into the UK office in Surrey, London. But when a virus came into the building inadvertently – although it did not cause any significant problems – it made the company reconsider its approach to security, especially internally.

Nikon has around 123 staff, 40 of whom work on the move. The latter are predominantly sales executives who

travel and use laptops as portable offices. They require access to corporate systems either in the office, or when they work from home or on the road. Nikon employees from other departments in the organisation often visit the Surrey office and need to access their own department's systems. In addition, Nikon has around 15 visitors every day attending various training courses who expect to use Nikon's public networking resources to catch up on work and e-mails during breaks.

Ian Fox, UK IT Coordinator, had the job of finding a solution which ensured everyone was protected, but which also increased access and employee mobility. “The threat of the virus incident alerted us to the fact here was a fine line, especially internally, between flexibility and security and although you can’t be 100 percent secure, we wanted to be as close as possible to 100 percent,” says Fox.



Nikon’s network is built on Cisco foundation network technologies and so Fox was keen to look at Cisco’s network security offerings. There is already a precedent for Cisco security technologies in the company with many of Nikon’s businesses worldwide using these solutions. The Cisco products have proved to be very effective at providing network security for other Nikon businesses, and Fox wanted the same level of protection for the UK.

Network Solution

Nikon uses the Cisco SMB Solution Portfolio to create a secure workspace. The company has upgraded its existing Cisco Local Area Network (LAN) at its Surrey office, which comprises 1 gigabit per second backbone connectivity and 100 megabits per second to around 80 desktops. There are two external links: one to Nikon’s European headquarters in Holland and via that to Japan, and the other to the Internet. There is also a Cisco wireless network at Surrey.

To deal with network security and internal security, in particular, Nikon uses the Cisco Self-Defending Network approach. This solution helps organisations protect themselves by identifying, preventing, and adapting to threats from both internal and external sources. As part of this approach, Nikon deploys a number of Cisco network security solutions.

Mobile staff have laptops which are used in a whole range of situations where they are vulnerable to a variety of threats. When employees return to the office, and indeed every time they attempt to access the company network, they pose a potential threat to the company. Cisco’s Network Access Control (NAC) checks any device attempting to access the network to ensure it has the necessary protection – such as the latest versions of anti-virus software – before allowing access. This technology can also be used by Nikon group employees who need to access worldwide Nikon systems, or by visitors who are given access to the Internet. Cisco NAC will even check a home computer when a Nikon employee attempts to log on to the network from home.

“In terms of being able to get products out to our dealers, if there was an attack we could survive in the short term, but any longer and we would start to struggle. It is vital to the business that we get our internal systems as secure as possible so that the people placing and releasing orders are protected, so that we get shipments out to customers and consequently money back in again. The flexibility and level of security that Cisco enables us to achieve is essential.”

Ian Fox, UK IT Coordinator, Nikon UK

In addition, Cisco Adaptive Security Appliances provide a range of network security features built into Cisco networking products. This provides Nikon with another level of anti-malware protection alongside anti-virus software on laptops and PCs. Nikon also uses Cisco Security Monitoring, Analysis and Response System (MARS) to provide a quick and simple way to monitor network security devices and host applications developed by Cisco, as well as other providers. Critical MS Windows Server auditing is achieved using Cisco development partner Honeycomb Technologies. Their mesh technology monitors the Windows Servers and filters key security events into MARS, translating IP attack information into meaningful User Identities.

The Cisco solution at Nikon was implemented by Satisnet, a Cisco SMB Select Partner.



Business Results

By using the Cisco Self-Defending Network concept, Nikon has been able to deploy a single, integrated solution for system security. It means that Nikon can be more flexible and open about network access without increasing risk. Security management is easier and helps the organisation be more proactive. It also prevents problems before they impact the business.

Fox says, "There has been a significant shift in the way we approach security at Nikon following the deployment of Cisco security technology. Now we are able to be much more proactive and can identify problems before they occur rather than react to events. I can even be at home and the Cisco security solution will automatically send an e-mail to my phone about a potential problem."

Cisco security technology will monitor Nikon's entire network infrastructure: networking equipment, security devices, software, and servers. If there is a problem or security alert, an e-mail highlighting the problem is sent out immediately. Previously, IT staff would have to go around to each device to identify and locate the problem. Nikon has a small IT team and having the Cisco technology means that staff resources are released from mundane activities, such as checking security alerts, to focus on more valuable application and computer service development. "With Cisco we know that there is a system constantly running in the background and if there is something we should know, it will tell us," explains Fox.

One of the most effective tools in dealing with the threat of attack internally – albeit unintentional – is Cisco NAC. Fox says, "If we have the measures in place that will protect us, then we can be a bit more flexible about the way people work."

Nikon has many visitors from outside the organisation coming into its building. They are connected to an external virtual LAN and, if their device contains a virus, it cannot infect the corporate network even though they may be using the wired or wireless LAN to access the Internet. Only when a device passes validation, checked by Cisco NAC, does the port it is connected to allow access to the corporate network.

Fox says, "In terms of being able to get products out to our dealers, if there was an attack we could survive in the short term, but any longer and we would start to struggle. It is vital to the business that we get our internal systems as secure as possible so that the people placing and releasing orders are protected, so that we get shipments out to customers and consequently money back in again. The flexibility and level of security that Cisco enables us to achieve is essential."

PRODUCT LIST

Routing and Switching

- Cisco Catalyst 3750 Series Switches
- Cisco Catalyst 2960 Series Switches
- Cisco Catalyst Express 500 Series Switches

Security

- Cisco Network Admission Control (NAC)
- Cisco ASA 5500 Series Adaptive Security Appliances
- Cisco Security Monitoring, Analysis and Response System (MARS)



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2008 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco Logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0609R)
The Print Consultancy (01483 771211) / Sept 08

Printed in the UK