

Protecting Users Everywhere, All the Time

Customer Case Study



Arup improves threat management and IT productivity, while lowering Internet security costs with Cisco Cloud Web Security

EXECUTIVE SUMMARY

Customer Name: Arup

Industry: Professional services

Location: U.K. headquarters with global operations

Number of Employees: 10,000

Challenge

- Strengthen web security and improve user experience for office and remote workers

Solution

- Cisco Cloud Web Security for real time scanning, reporting, and control of web traffic
- Cisco AnyConnect Secure Mobility Client, extending protection to roaming users

Results

- Better, cost effective protection for 10,000 users in 60 offices
- IT spends less time managing security, malware problems, and VPN provisioning
- Lower Internet security costs

Challenge

Arup is a global firm of designers, planners, engineers, consultants, and technical specialists offering professional services from building design and project management to software development. Some of its renowned client projects include High Speed 1 in the United Kingdom, Allianz Arena in Germany, and Bologna Railway Station in Italy.

IT security plays a crucial role in this success, enabling people to work productively in the office and remotely. With about 10,000 network users and 90 offices around the world, Arup often has to rapidly set up temporary site offices using portable routers and wireless access points to deliver connectivity. Coffee shops and other public Wi-Fi hotspots provide staff with more opportunities to get online and stay in touch.

However, the limitations of a traditional security approach started to stretch the firm's small but expert IT security team. "We had proxy servers approaching end-of-life with ineffective anti-virus controls. More and more computers needed cleansing, and we had no real reporting capabilities," says head of operations, Mark Judge. "The response from our previous vendor was to increase the hardware footprint, but this would have meant adding further costs and management overheads. We needed to streamline remote access, reducing costs on expensive two-factor authentication systems that were token-based."

Solution

Like many organizations, Arup saw massive advantages in moving from a box-based security model to one orchestrated in the cloud. "It was one of the easiest business cases to make," says IT security manager, Peter Kersting. "As well as improving security and user experience, it presented the opportunity to save bandwidth by introducing Internet breakouts and offloading WAN traffic."

Arup opted for Cisco® Cloud Web Security (CWS). This software-as-a-service solution underpins 99.999 percent network availability with zero-day threat protection through heuristics analysis. "We chose Cisco Cloud Web Security because it offered the best solution in terms of scalability, easy administration, and great reporting," says Kersting.



“Now we don’t spend anywhere near the amount of time we used to, dealing with security events and malware problems. In fact, since switching to Cisco CWS, I cannot recall a client being infected, and we seldom have to go into the admin portal.”

Peter Kersting
IT Security Manager
Arup

“Based on similar deployments, Cisco believes the Cloud Web Security solution lowers some elements of our Internet security spending by 30 to 40 percent, while being a lot more effective. Although we’re still to run the exact numbers, our experience so far shows we will make tangible savings.”

Mark Judge
Head of Operations
Arup

Users are protected everywhere, all the time. CWS connects to Cisco Security Intelligence Operations (SIO), a 500-strong global team of experts backed by the industry’s largest collection of real time threat intelligence, including:

- 100TB of security intelligence daily
- 1.6 million deployed security devices, including firewall, intrusion prevention system, web, and email appliances
- 13 billion daily web requests
- 150 million endpoints

The addition of Cisco AnyConnect® Secure Mobility Client enables Arup to extend protection and improve the experience for roaming users. Offering various licensing options, the software client is easy to download and covers a broad set of operating systems. “We especially liked the Cisco VPN software, which uses certificates to automate the process, so users do not have to authenticate using two-factor authentication tokens or re-entering any user credentials,” says Kersting.

Results

Under the previous security approach, which relied mostly on identifying bad URLs, the Arup IT team would catch one or two threats in a typical week. They would then spend 25 percent of their time cleaning contaminated PCs and laptops. Ineffective controls also required a growing list of websites to be excluded from malware scanning, leaving Arup vulnerable despite paying large sums of money each year to secure its web browsing.

Thankfully this is no longer the case. All inbound and outbound web traffic is analyzed in real time. Malware detection, with signature-based scanning and heuristics analysis, blocks threats before they can inflict damage.

“We have greater control of all web traffic on all connected devices,” says Kersting. “Now we don’t spend anywhere near the amount of time we used to, dealing with security events and malware problems. In fact, since switching to Cisco CWS, I cannot recall a client being infected, and we seldom have to go into the admin portal.”

Cisco CWS has reduced WAN congestion and bandwidth usage by enabling local Internet breakouts and eliminating the need to backhaul web traffic via the VPN. Arup has also cut the time that it takes to set up temporary site offices by incorporating Cisco Adaptive Security Appliances that introduce further benefits, especially around disaster recovery and business continuity planning. “VPNs are easier to segment and faster to provision, even with automated failover for site-to-site VPNs,” says Kersting. “And with Cisco CWS, IT doesn’t have to provide web usage reports to other parts of the firm anymore, because they can run their own.”

User experience has also changed for the better. With AnyConnect roaming, users are connected directly to the Internet through the nearest and safest cloud proxy. “Everything is so much smoother. Automatic session re-establishment eliminates the need to continuously keep re-authenticating VPN access,” says Kersting.

Looking ahead, Cisco CWS can be easily integrated with Cisco IronPort® security products, enabling Arup to leverage threat intelligence and further consolidate and centralize IT security management. Mark Judge sums up: “Based on similar deployments, Cisco believes the Cloud Web Security solution lowers some elements of our Internet security spending by 30 to 40 percent, while being a lot more effective. Although we’re still to run the exact numbers, our experience so far shows we will make tangible savings.”



For More Information

To learn more about the Cisco solutions described in this case study, go to:
www.cisco.com/go/security

Product List

Security

- Cisco Cloud Web Security
- Cisco AnyConnect Secure Mobility Client



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned 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. (1110R)