Arup Empowers its Cloud-First Workforce with Secure Access and Zero Trust

ARUP

Industry:	Location:	Organization:	Solution:
Global Professional Services	London, England	90 offices, 34 countries, 20,000 employees worldwide	Cisco Secure Access Cisco User Protection Suite Cisco Breach Protection Suite

Founded in 1946 and headquartered in London, Arup is a global professional services organization with advisory and technical expertise across more than 150 disciplines. With a focus on construction and engineering, Arup plans, designs, and creates offerings that deliver sustainable and innovative solutions for complex challenges across industries. With 20,000 people working across 90 offices in 34 countries, the employee-owned firm is driven by a commitment to excellence, collaboration, and shaping a better world.

From metro systems and concert halls to water utilities and wind farms, Arup's projects in sustainability and infrastructure are shaping a better world. Arup is a global professional services organization with advisory and technical expertise across more than 150 disciplines. Tackling some of the biggest questions facing the built and natural environments, Arup's highly collaborative and distributed 20,000-person workforce depends on secure, reliable remote access to keep teams connected and productive.

However, as Arup expanded its footprint across six continents into a network of over 90 offices in 34 countries, their existing patchwork of legacy on-premises VPNs made it increasingly difficult to manage secure access at scale – introducing operational friction, inconsistent user experiences, compliance risks, and growing security concerns.

- **Managing a Complex Infrastructure:** Arup relied heavily on a large deployment of Cisco Adaptive Security Appliance (ASA) firewalls, supporting Cisco AnyConnect VPN for secure remote access. "Our existing infrastructure had served us well – delivering critical reliability, including during major disruptions like the COVID-19 lockdown," explains David Noble, Cyber Engineer for Arup. "But as we continued to grow our business, managing so many physical firewalls – along with the patching and maintenance required – became increasingly time intensive."
- **Demonstrating Compliance:** As a UK-based organization, Arup is required to maintain Cyber Essentials Plus certification, an annual exercise that requires an independent audit, rigorous documentation, and up-to-date systems to verify Arup's use of effective security controls. "Tracking, securing, and demonstrating the compliance of every firewall across the business was a huge headache for our IT team," says Noble.
- **Strengthening Zero Trust:** Arup wanted a solution that could deliver true zero trust access, specifically to address the risk of lateral movement within their network. "We have a very large, distributed, and diverse workforce – from engineers and designers to coders and economists," explains Noble. "They handle extremely sensitive data and work on high-stakes projects involving critical infrastructure, transportation systems, government initiatives, and more." To protect both their employees and their customers, Arup needed the ability to enforce least-privilege access to ensure users were granted permission to only those systems they needed to perform their jobs – and nothing more.

Secure Access Delivers Cloud-Ready Security for a Hybrid Workforce

To address these challenges, Arup looked to adopt a Security Service Edge (SSE) solution to secure remote access to the web, cloud services, and private applications without relying on traditional, hardware-based perimeter security like firewalls. While Arup evaluated several solutions, they ultimately chose Cisco Secure Access, a cloud-delivered SSE platform that offers integrated ZTNA and VPNaaS for an easy transition to zero trust security. Already a Cisco Umbrella customer, moving to Secure Access would continue to provide existing Umbrella protection and web proxy capabilities plus additional critical security features Arup wanted like zero trust.

Noble says their decision was guided by their long-standing relationship with Cisco, confidence in Cisco's track record, and Secure Access' comprehensive security and compliance capabilities. "Secure Access offered us a straightforward path to zero trust implementation. We could eliminate the operational headaches of managing on-premises infrastructure while strengthening security and compliance and improving the user experience," says Noble. Building on a platform Arup already knew and trusted would also help reduce risk, minimize the learning curve and business disruption, and enable the company to expand on the benefits of their existing Umbrella investment.

"Cisco Secure Access has delivered exceptional value. With one unifed agent for web security, zero trust network access, and VPNaaS, we've significantly simplified and improved the user experience while maximizing protection. The process of securing applications through ZTNA was straightforward and easy to implement – building seamlessly on our existing VPN foundation."

– Chris Lyth,
Chief Information Security Officer, Arup

A "Seamless" Migration from Umbrella to Secure Access

Arup's journey with Cisco security solutions began years ago with Umbrella DNS, followed by Umbrella Secure Internet Gateway (SIG) and, most recently, Secure Access. This stepwise adoption has allowed Arup to continuously raise its security posture while leveraging familiar, trusted interfaces and technologies. "Our migration from Umbrella DNS and SIG to Secure Access was completely seamless," explains Noble. "We literally moved directly from a proof of concept (POC) to production without any reconfigurations. It was a painless, smooth transition, due in part to the tremendous support from Cisco and our partner CAE Technology Services Limited (CAE)."

To date, Arup has deployed several Secure Access features – including VPN as a Service (VPNaaS), DNS security, and ThousandEyes – for approximately 20,000 users, in just six weeks. Noble shares that the IT team has found the ThousandEyes integration especially valuable during their Secure Access rollout. They've been using ThousandEyes to test and compare network performance between rural sites and more central locations.

Noble says over the coming weeks, they will be rolling out the updated Cisco Secure Client along with "all the bells and whistles," including ZTNA along with additional advanced capabilities like Remote Browser Isolation (RBI), Data Loss Prevention (DLP) and next-generation firewall controls – security capabilities not available with their previous Cisco solutions.

Throughout the Cisco Secure Access project, Arup found immense value in working with CAE as their trusted partner. From day one, CAE took a proactive, hands-on approach – offering expert support, maintaining clear and open communication, and ensuring a consistent presence through every phase of the deployment. Their engagement kept the project on track and aligned with Arup's goals.

CAE's technical expertise and recognition as Cisco Security Partner of the Year 2024, were clearly demonstrated during the proof of concept, where they quickly addressed setup challenges and provided in-person support. Arup appreciated their exceptional collaboration, guidance and commitment when it mattered most.

> “Switching to Cisco Secure Access took a huge weight off our shoulders – we were able to move away from the hassle of maintaining physical firewalls almost overnight. Now, everything from security controls to compliance reporting is centralized in one portal, which makes life so much easier.”
>
> – David Noble,
> Cyber Engineer, Arup

Unified Control with Tight Integration Across the Cisco Security

Beyond Secure Access, Arup leverages Cisco’s User and Breach Protection Suite to provide a comprehensive solution to protect its business, including:

User Protection Suite

- Duo to provide strong identity security, visibility, and posture management through integrated Identity Intelligence capabilities
- Cisco ISE (Identity Services Engine) for network access control; the team is exploring further opportunities for optimized use such as leveraging ISE security group tags (SGTs) in Secure Access policies to protect users and IoT devices

Breach Protection Suite

- Cisco XDR (Extended Detection and Response) for advanced analytics and visibility, with AI-driven automation and native telemetry to quickly detect and remediate threats
- Cisco Secure Endpoint for endpoint detection & response capabilities, integrated within Secure Client
- Cisco Secure Malware Analytics for detecting, analyzing, and responding to malware, integrated across Cisco’s security products
- Cisco Secure Email Threat Defense (ETD) for protection against advanced email-borne threats such as phishing, business email compromise (BEC), ransomware, and malware; ETD is seamlessly integrated with Arup’s Microsoft 365 environment, detecting and categorizing threats previously bypassed, which Noble says “has been quite a revelation”

Also, Cisco Security Cloud Control is being used for centralized management of security policies, configurations, and analytics. For Arup, the deep integration between these Cisco tools and the ability to centrally manage policies and updates via a single, unified management portal is invaluable – improving visibility and efficiency while strengthening security and compliance.

Empowering a Hybrid Workforce While Securing the “Crown Jewels”

Chris Lyth, Chief Information Security Officer for Arup, says the shift to Cisco’s modern access solution has been both smooth and strategic. “Cisco Secure Access has delivered exceptional value. With one unified agent for web security, zero trust network access, and VPNaaS, we’ve significantly simplified and improved the user experience while maximizing protection. The process of securing applications through ZTNA was straightforward and easy to implement – building seamlessly on our existing VPN foundation.”

Granular Access Control, Powered by Zero Trust

Unlike traditional VPNs that expose broad internal segments to users, Secure Access can strictly limit application access to only those resources users need – simplifying compliance and reducing the risk against the spread of internal threats within flat, boundaryless networks. “We work with governments, critical infrastructure, and huge enterprises, so it’s vital that we are able to protect our client’s confidential data,” explains Noble. “Our ability to segment access and control lateral movement is critical to controlling our apps and securing our crown jewels.”

Eliminating Firewall Fatigue with Unified Control

"Switching to Cisco Secure Access took a huge weight off our shoulders – we were able to move away from the hassle of maintaining physical firewalls almost overnight," says Noble. "Now, everything from security controls to compliance reporting is centralized in one portal, which makes life so much easier.'"

Delivering a Familiar User Experience Without the Friction

Thanks to an interface with a similar look and feel to Umbrella, employees have transitioned to Secure Access with ease – reducing the need for training and minimizing disruption. With the Secure Client local agent and built-in zero trust capabilities, users now enjoy seamless, always-on access to critical resources– eliminating the need for repeated VPN logins or manual connections. Previously, accessing systems like Arup's HR portal required users to log into a VPN, launch a browser, and navigate to the app – a process that typically took ~60 seconds. With Secure Access, that same task now takes just 15–20 seconds, cutting access time for users by more than two-thirds (~66%).

Optimizing Agility While Minimizing Administrative Burden

The ability to centrally manage firewalls, security policies, and client devices through Secure Access has significantly reduced administrative overhead. Features like auto-updates and enhanced visibility make it easier for IT to maintain compliance, keep systems current, and quickly identify and remediate issues. Although the organization is still fine-tuning aspects of the deployment, long term they expect minimal administrative burden and a more agile security posture.

Partnering for a Secure Tomorrow

By moving to Cisco Secure Access, Arup is not only simplifying their infrastructure and compliance landscape but also building a future-ready security posture that meets the demands of a dynamic, distributed workforce. "At the end of the day, we chose to standardize on Cisco Secure Access because it gave us what we needed – zero trust access, simpler operations, and a scalable path for the future as our security needs keep evolving," explains Noble. "What really gives us confidence is how well the solution brings everything together – advanced security, solid vendor support, and seamless integration across our broader Cisco environment. With Secure Access, we are staying ahead of today's challenges and ready for whatever comes next."