Davies Provides Innovative, Secure Services to its Insurance and Financial Services Customers

Illumio Core and Endpoint secure a global, rapidly expanding network with Zero Trust Segmentation

Business Goals

As a leading global professional services and technology firm serving highly regulated markets, Davies must consistently protect its servers and endpoints from business-impacting cyberattacks while providing the highest quality services to its customers. A single breach of an endpoint has the potential to disrupt its operation, and downtime or curbed innovation are not options.

Davies' 8,000+ team works across more than 40 countries including the UK and U.S., serving 1,500+ clients in insurance, financial services, and highly regulated markets. Davies puts quality and data security and protection at the heart of everything it does. At minimum, the organization complies with audits and regulations and consistently measures against NIST, Center of Security (CIS) frameworks, ISO 27001 for organizational controls, and other regulations.

CISO Sam Hart oversees cybersecurity, governance, privacy, and compliance. With strategic M&A playing a part in Davies' growth strategy, Hart's team is involved in the due diligence process of new, potential acquisitions early on, assessing the security posture of target businesses so they know how much work will be needed post-deal.

Hart also sees her team as business catalysts, showing the value of their secure network to customers, insurers, and potential acquisitions. According to Hart, Illumio allows Davies to future-proof their overall business. She explained: "Davies' security team serves as business enablers, but we also must establish guardrails that protect the organization without impacting business innovation."

Industry: Insurance Professional Services and Technology Firm

Challenge: Securing an innovative professional services and technology business serving insurance, financial services, and highly regulated markets.

Solution: Illumio Core & Endpoint

Use cases:
- Critical Asset Protection
- Environmental Separation
- Ransomware Containment
- Network Visibility
- Vulnerability Risk Reduction

Location: Global, 40+ countries, including the UK and North America

Benefits:
- Provides network and endpoint visibility and insights
- Protects the expanding attack surface from M&A without hampering growth or innovation
- Stops lateral movement from ransomware and other cyberattacks
- Serves as a business enabler, providing assurance and value for potential acquisitions
- Validates security capabilities for insurers and satisfies regulatory requirements

> "
>
> Illumio's dashboards are brilliant and show me week to week how my lateral movement risk is closing out.
>
> Sam Hart
> CISO
> **Davies**

Technology Challenges

Keeping the business safe and providing the best services for customers are Hart's top priorities. When Davies integrates with a new business, it's critically important to map and see all network connectivity routes to ensure controls are consistent across the business.

Major focus areas include MITRE ATT&K framework defense, protecting their crown jewels, and securing all environments and endpoints from any threat actors that might have an ingress route to move laterally across the network. Asset mapping, visibility, and Remote Desktop Protocol (RDP) blocking are essential.

"One of the things that helps me sleep at night is knowing that we can lock down at any attempted lateral movement," says Hart. From her perspective, having a partner and not just a supplier is key. Zero Trust gives Davies the confidence that its firm is always protected, wherever its team members are in the world.

> "
>
> Illumio has given me complete insight into our network and gives me actionable risk-reducing measures I can implement.
>
> Illumio was a no-brainer because it locks in at the network layer, and I can focus on each endpoint. For us, there was no other option.
>
> Sam Hart
> CISO
> **Davies**

How Illumio Helped

According to Hart, the "massive value" of Illumio and its Zero Trust Segmentation platform is demonstrable and has "taken Davies' network security to the next level." Illumio's holistic view of the network equips the team with a wealth of actionable insights to mitigate risks effectively.

"Illumio Endpoint provides the assurance that our vital data, systems, and resources remain shielded, irrespective of an employee's location. Moreover, its proactive management of endpoint access and adaptive segmentation policies based on device location provide us with a safety net. This gives us peace of mind and added response time in a worst-case scenario," says Hart.

The Illumio professional services team also added value by working in partnership with Davies, applying lessons learned from other businesses to get the best and the most expedient use of Illumio Endpoint and Core.

"We wanted a long-term partner; we didn't just want a supplier. Illumio takes the time to understand our business, how we are growing, and how the tools and the team can support us on this journey."

Results & Benefits

- **Secure network and endpoints:** Visibility, insights, and control to stop lateral movement in its tracks

- **Business enabler:** Security assurance is presented to cyber insurers and highly regulated M&A prospects

- **Confidence in M&A:** Ensures the secure growth of the business without compromising on security, cyber resilience, or inhibiting innovation

About Illumio

Illumio, the Zero Trust Segmentation Company, stops breaches from spreading across the hybrid attack surface. The Illumio ZTS Platform visualizes all traffic flows between workloads, devices, and the internet, automatically sets granular segmentation policies to control communications, and isolates high-value assets and compromised systems proactively or in response to active attacks. Illumio protects organizations of all sizes, from Fortune 100 to small business, by stopping breaches and ransomware in minutes, saving millions of dollars in application downtime, and accelerating cloud and digital transformation projects.