How JLL combats insider risk with Netskope SSE

Headquartered in Chicago, Illinois, Jones Lang LaSalle (JLL), is a real estate company that helps clients buy, build, occupy, and invest in a variety of assets such as industrial, commercial, retail, residential, and hotel real estate. Its clients range from tech startups to global firms and span industries including banking, energy, healthcare, law, life sciences, manufacturing, and technology. JLL also operates an independent investment management subsidiary.

How can a global real estate company quantify and prevent data exfiltration?

JLL's Information Security team has a fine balance to maintain. On the one hand, they need to give their workers the freedom to do their jobs. On the other, they must ensure the integrity of their data.

Jeffrey Sarnowski, Director and Senior Technical Investigator at JLL, explains: "The rise of working from home was a challenge. Before Netskope, we didn't force users through a web proxy, so we were unable to inspect what users were doing when they were not in the office. This increased the risk that we would lose data through insiders, accidentally or otherwise, exfiltrating data."

JLL has an extensive global footprint with offices all over the world. They needed a solution that could enhance their security posture irrespective of location with no issues to end user experience. Using a 'defense-in-depth' cybersecurity strategy was crucial; block what needs to be blocked, and is unsanctioned, and inspect everything that goes out. This way they can identify anomalous behavior, coach users, and improve employee behavior while simultaneously enhancing their enterprise security posture.

A final challenge was that some of JLL's developers tended to pick their own cloud tools and APIs rather than those approved by the Information Security team. Doug Shepherd, Senior Director, Global Insider Risk Program at JLL, comments: "Ensuring standardization across the tech stack was a big consideration for us, both for reducing data loss and ensuring our investments are optimized."

JLL

Profile

Industry	Region	Employees	Founded In
Financial	Global	102,000+	1783

Click here to visit the JLL website

Challenges
- Push to evolve to a security-first culture
- Limited visibility with end user transactions
- Lack of targeted controls that identify unapproved data movement

Solution
- Netskope SWG and CASB for data governance and protection
- Netskope Advanced Analytics for detailed reporting
- Netskope Premium Plus for strategic guidance and support

Results
- Improved insights on data movement to applications
- Detection of anomalous user behavior and coaching teams
- Enhanced security by using targeted blocks to limit data exfiltration

"The rise of working from home was a challenge. Before Netskope, we didn't force users through a web proxy, so we were unable to inspect what users were doing when they were not in the office. This increased the risk that we would lose data through insiders.

Jeffrey Sarnowski, Director and Senior Technical Investigator, JLL

netskope

Ready for anything

Analyzing user behaviors with the Netskope SSE

JLL turned to Netskope to help address its data loss challenges. "The choice to go with Netskope was easy," comments Shepherd. "Not only is Netskope an industry leader, but we have confidence from prior deployments that Netskope would achieve the results that we need."

JLL today uses the Netskope Security Service Edge (SSE). The Netskope Cloud Access Security Broker (CASB) capability prevents data exfiltration between corporate and personal app instances and automatically audits JLL's application traffic to determine risks and mitigate threats. Meanwhile, the Netskope Next Gen Secure Web Gateway (SWG) provides web and cloud inline security and delivers threat and data protection. Finally, Netskope Private Access (NPA) securely and directly connects JLL's users to private resources hosted on-premises or in the cloud for rapid and reliable application connectivity.

In addition, JLL uses Netskope Advanced Analytics and UEBA to analyze and visualize factors such as data loss and insider activity to better understand the company's risk profile. And to ensure coverage in China, a region known for specific internet regulations and cross-border internet performance challenges, JLL uses the Netskope NewEdge China network to support instances of its Netskope solution in the jurisdiction.

Exposing risky user behaviors

Netskope provides JLL with deep insights into user behavior, allowing the team to rapidly identify and investigate risky insider activities such as the bulk transfer of data from corporate to personal application instances. "Netskope enables us to quantify data exfiltration and link risky behaviors to individuals, allowing us to take timely action," says Sarnowski.

JLL is finding wider applications for intelligence around users' online activities, including in HR and legal. Sarnowski adds: "You can use behavioral analytics to predict what people are going to do, and that's a big help in everything from threat mitigation to employee retention."

Netskope also helps JLL configure its applications. Many employees had inadvertently mapped their personal OneDrive accounts onto their corporate computers. JLL used Netskope to identify affected endpoints and restore the corporate accounts. "This was an unexpected benefit of our deployment and has helped us quickly remedy the situation," says Shepherd.

Finally, Netskope has helped JLL realize just how complex its IT systems have become and take action. Shepherd concludes: "With Netskope, we have the visibility and control we need to enforce technology standards. That helps us avoid tech debt and ensure that our developers only use approved storage and APIs."

> "With Netskope, we have the visibility and control we need to enforce technology standards. That helps us avoid tech debt and ensure that our developers only use approved storage and APIs."

Doug Shepherd, Senior Director, Global Insider Risk Program, JLL