Leading Global Law Firm Prevents the Spread of Ransomware with Illumio Edge

Endpoint Zero Trust complements endpoint security and relieves NAC headaches
Customer Overview & Challenge

Law firms have plenty to protect, which can be difficult with thousands of employees working globally on mobile devices. A well-meaning employee clicking on a phishing email can trigger malware or ransomware that locks up entire network segments and laptop fleets. One of the world’s top law firms with 2,000 laptops needed a solution to address this risk.

Endpoint security will stop many attacks, but for never-before-seen malware or ransomware, endpoint security tools like endpoint detection and response (EDR) need time to detect a file as malicious, leaving a window of vulnerability. Network Access Control (NAC) solutions, while good for letting devices onto the campus network, are costly and complex to deploy for access control and segmentation to limit attack surfaces.

Given that malware and ransomware can take out entire networks in seconds, the firm sought capabilities that complemented their endpoint security tools to prevent threats from spreading while EDR worked to detect files as malicious.

They spent three frustrating years attempting a segmentation project to contain threats with their NAC product. It was operationally draining and fell short without visibility to help determine how to write policies. The project was ultimately derailed by the need for a $10M network upgrade to see it through.

Illumio Solution

Given their security challenges, the team turned to Illumio as they sought a new approach to segment their environment to prevent the spread of threats. With Illumio Edge, they were up and running in a day since Zero Trust segmentation is enforced on the endpoint, not on the network – which they did not have to touch.

To enforce with total confidence, Illumio Edge was first deployed in policy test mode to understand and see current peer-to-peer communications between user laptops. With this visibility as their baseline, they enforced Zero Trust policies that blocked all network communications between endpoints, except inbound traffic and services that were explicitly whitelisted.

The team could breathe easy knowing that by creating policies with a baseline of visibility, they would not interrupt employee productivity or spark help desk calls.

Illumio Edge also gives them the ability to immediately see blocked traffic between endpoints to understand any potential lateral movement of malware or attempted employee peer-to-peer traffic. With this visibility, they can investigate suspicious traffic or, if needed, refine policy to account for business needs.

These communication insights are easily reportable and shown in list views from the Illumio Edge dashboard. The firm can quickly and efficiently respond to client audits to prove that they are adequately protecting their campus network from ransomware and malware threats.

Summary

Industry: Legal Services

Environment: Employee laptop estate of more than 2,000 devices

Challenge: Stop propagation of ransomware and malware between laptops and on campus networks

Solution: Illumio Edge for endpoint Zero Trust, replacing NAC as a solution to stop threats from spreading

Benefits: Ability to block peer-to-peer propagation of malware and ransomware with a solution that’s invisible to end users and has no performance impact
Customer Benefits

Greater ransomware protection

By augmenting their endpoint security with endpoint Zero Trust, threats are contained while other tools detect and respond to advanced malware or ransomware as quickly as possible.

Zero-risk Zero Trust

Whitelist policy are only put into enforcement after weeks in visibility mode to make sure the right business-critical services are permitted. This took the risk out of whitelisting and prevented annoying help desk calls. They didn’t have to write GPOs or manual host firewall rules.

Tiny footprint, network free

Without having to touch the network, the team segmented user laptops in a day, amounting to the same segmentation they attempted for three years with their NAC vendor on the campus network. The Illumio Edge agent did not tax employee laptops, never slowing down productivity.
Illumio enables organizations to realize a future without high-profile breaches by providing visibility, segmentation, and control of all network communications across any data center or cloud. Founded in 2013, the world’s largest enterprises, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com.