illumio

CUSTOMER STORY

Hartwig Gains Efficiency With Zero Trust Segmentation for Servers and Endpoints

Leading machine tool distributor turns to Illumio Core and Illumio Edge to stop ransomware from spreading

HARTWIG

Customer Overview & Challenge

As one of the leading CNC machine tool distributors in the United States, Hartwig, Inc. has over 60 years of experience helping the manufacturers of some of our most valuable goods, from aerospace components to the quarter in your pocket. These machine experts are on a mission to help people in manufacturing control their destiny every day.

Fortifying the company's security posture while this innovation happens has never been more important. And after seeing others in the industry fall victim to ransomware attacks, IT Manager Tim Francis redoubled his focus on Zero Trust controls.

Francis has always been ahead of the curve on Zero Trust adoption. Attuned to the "never trust, always verify" philosophy for some time, he implemented user-focused controls, including multi-factor authentication and single sign-on years ago. The responsibility for keeping Hartwig's servers up and running and ransomware at bay led Tim to pursue micro-segmentation — a foundational component of Zero Trust.

After exploring a well-known hypervisor-based segmentation solution, Francis determined it was too costly and insufficient, with compatibility limitations and a separate purchase for visualization. Running a two-person IT shop at Hartwig required a flexible, unified approach to visibility and segmentation that's supported by automation.

The lean but mighty team of two also supports over 200 employees with remote workers spread across 14 states — representing the greatest risk area for ransomware. Francis ultimately wanted to extend Zero Trust to employee laptops and needed to find the right solution that could deliver on two fronts: powerful ransomware protection and simplicity.

Overview

Industry: CNC Machine Tools

Environment: On-premises data center with 40 servers; approximately 200 employee laptops

Challenge: Lack of visibility and control of east-west traffic

Solution: Illumio Core for visibility and Zero Trust Segmentation; Illumio Edge for Zero Trust on endpoints

Benefits: Fast time to Zero Trust; an upper hand against ransomware; unprecedented visibility

Illumio Solution

Backed by a company that understands the importance of investments in technology and has confidence in its IT leader to make savvy decisions, Francis chose Illumio Core for Hartwig's data center segmentation needs.

"Illumio Core looked about a million times easier and was significantly less expensive than the initial vendor we considered," Francis says.

He estimates that Hartwig spent a quarter of what they would have with the hypervisor-based solution — in both dollars and time. Saving tens of thousands of dollars is no small win for Hartwig.

As a visual worker, Tim gained immediate value from Illumio Core's built-in real-time map.

"I got a tremendous amount of insight into our environment and the traffic flows I need to understand before I could even think about building policies," Francis says. "The adage that 'a picture is worth a thousand words' definitely applies."

Francis took a deliberate approach to deployment, starting by understanding the connections and flows across the data center. He then began turning off unused services. Shutting down the associated open ports and potential connections that attackers could exploit significantly reduced Hartwig's attack surface.

Illumio Core's easy-to-understand labeling system further simplifies visualization and facilitates policy creation. The map makes it easy to craft policies that only allow trusted communications. Francis also took advantage of Illumio Core's test mode, allowing him to model and test policies against existing traffic flows to assess impact before enforcement.

While Hartwig successfully enforced Zero Trust segmentation server policies, the desire — and need — to extend Zero Trust protection to employee laptops increased when Hartwig's largely remote workforce became fully remote due to COVID-19 office closures. Alternative approaches like writing Group Policy Objects would be untenable. Francis wanted a centrally managed endpoint solution that is SaaS-based.

And then came Illumio Edge, a first-of-its-kind Zero Trust endpoint solution introduced in June 2020. Illumio Edge ensures that if an employee laptop is hit with ransomware, the attack will be contained to that machine.

It was the onset of the pandemic, and spending was closely monitored. But with established trust in Illumio and a sense of urgency for ransomware resilience, Illumio Edge was approved as the most efficient and economical way to protect the company's endpoints.

Hartwig quickly deployed Illumio Edge across its entire employee laptop estate, and the learning curve was easy. Setting up automated allowlist policies was as simple as selecting the peer-to-peer applications and services like Microsoft Teams that Francis wanted to permit.

Similar to Illumio Core, Illumio Edge provides the option to test policies before moving to enforcement. Hartwig can now confidently and safely prevent ransomware from propagating without disrupting employee productivity or business operations.

Policy follows the user whether on or off the network. Illumio Edge also provides a view to monitor blocked traffic between endpoints to identify any potential ransomware.

"With Illumio, we are doing Zero Trust very efficiently, effectively and inexpensively. And now that I have all the endpoints covered, I couldn't be happier," Francis says.

Customer Benefits

More Zero Trust in less time

Illumio Core and Illumio Edge give Hartwig fast and consistent Zero Trust control over its servers and endpoints, with time-saving automation — and without having to touch the network.

An upper hand against ransomware

Zero Trust segmentation shuts down unnecessary open paths that ransomware and cyberattacks use to spread, breaks up the attack surface, and gives Hartwig the control needed to contain a potential breach.

Unprecedented visibility

Illumio Core's application dependency map is a visual worker's delight, giving Hartwig a detailed view into the IT environment, with simple labels and context to build policies and monitor traffic.

> With Illumio, we are doing Zero Trust very efficiently, effectively and inexpensively. And now that I have all the endpoints covered, I couldn't be happier.
>
> **Tim Francis, IT Manager**

Illumio, the pioneer and market leader of Zero Trust Segmentation, stops breaches from becoming cyber disasters. Illumio Core and Illumio Edge automate policy enforcement to stop cyberattacks and ransomware from spreading across applications, containers, clouds, data centers, and endpoints. By combining intelligent visibility to detect threats with security enforcement achieved in minutes, Illumio enables the world's leading organizations to strengthen their cyber resiliency and reduce risk.

Gartner peerinsights™

See what customers have to say about Illumio.