illumio

CASE STUDY

Dutch Municipality Bolsters Defense-in-Depth with Zero Trust

Saving them millions in both hardware and headcount costs

Customer Overview & Challenge

Cities around the world must protect large amounts of sensitive information on both their residents and the vital applications supporting municipal services ranging from water management to crime.

This major European city takes such responsibility seriously. Supporting and protecting the prosperity and well-being of residents means ensuring important, sensitive data like personal identification numbers, financial and debt-related information, and crime data always remain protected and confidential.

Aware of attacks and breaches happening around the world, the city proactively initiated a security audit to understand any weaknesses that should be addressed to further strengthen their security posture to keep sensitive data safe.

They had all the vital threat-centric technologies like firewalls and web and email security properly deployed for defense-in-depth. However, the audit unearthed some areas for improvement.

One finding needed immediate attention: the city had a largely "flat" network, without segmentation, that would have allowed attackers free reign if they got inside.

> "We have never had a breach, but we know that if a breach occurred in a flat network, any attacker would have had access to all of our workloads," noted a Senior IT Project Manager.

The audit made clear that a key to reducing overall security risk was closely linked to reducing their attack surface with segmentation.

Like many organizations, the city's IT team initially turned to a familiar technology to attempt segmentation: firewalls. The city scoped out a segmentation program using firewalls, but quickly realized it would be too hard and too expensive. The project would have taken four to five years, required 12 additional employees to implement new firewalls with thousands of rules, and cost millions of Euros.

Summary

Industry: Local Government

Environment: Around 2,000+ workloads

Challenge: Reducing their attack surface to limit the potential for attacker lateral movement

Solution: Illumio Core™ for precise protection of critical applications, enabling Zero Trust control against the spread of potential attacks

Benefits: Fast time to value and tremendous cost savings; newfound application visibility; Zero Trust segmentation that reduces security risk without misconfigurations

Having seen the cost and complexity of this approach, the municipality quickly discarded the plan and contacted a trusted analyst firm for suggestions on an entirely new approach to segmentation that was easier, more effective, and less costly.

Illumio Solution

From the moment the Illumio proof of concept was set up, the IT team realized Illumio Core was the right approach to segment their data centers. What immediately stood out was the powerful visibility and insights they gained from the Illumination map – visibility they had never had in the past. This let them unearth countless data flows in their environment of which they were previously unaware.

With an Illumination map of all application flows, the team was able to meet with application owners to jointly design segmentation policies based on a single source of truth.

What is more, Illumio's four-dimensional easy-to-understand labels were very helpful in creating a map that is useful to everyone in the organization. It allows the team to see and understand all flows, including how new applications behave to then create policy for. The map proved that a picture is worth a thousand words.

What initially prompted the need for segmentation was the need to address their flat network to reduce the attack surface. To do this, Illumio put automated, Zero Trust segmentation in place. Illumio adopts a Zero Trust, default-deny approach, where only allow-listed flows are permitted.

For example, with one of their key applications, they ran Illumio in visibility mode without enforcement for months to ensure they understood every flow from that application that must be accounted for by policy. Once that baseline was in place, they used Illumio's policy automation tool to segment the application to block all unauthorized flows – all in the matter of a few clicks.

Customer Benefits

Incredible application visibility

The Illumination map delivers full application visibility and a true understanding of application behaviors, meaning application owners could be involved in the segmentation process.

A stronger Zero Trust security posture with less risk

Micro-segmentation has allowed the city to do away with a flat network that made them vulnerable to a large data breach. They now have a Zero Trust segmentation model to restrict lateral movement, complement defense-in-depth, and reduce overall security risk.

Fast time to value and real cost savings

Illumio delivered segmentation in less than half the time a segmentation project with firewalls would have taken. They avoided tens of millions of euros in firewall spend and the need to hire 12 new employees.

All the security without the misconfigurations

With visibility into all application flows, Illumio allows this city to model policy before going into enforcement. This ensures that they don't accidentally block a critical application.

> The best thing about Illumio is the application insight we gained in our complex environment and how easy it is to then go into segmentation.
>
> **IT Project Manager**

Illumio enables organizations to realize a future without high-profile breaches by preventing the lateral movement of attackers across any organization. Founded on the principle of least privilege in 2013, Illumio provides visibility and segmentation for endpoints, data centers or clouds. The world's leading organizations, including Morgan Stanley, BNP Paribas, Salesforce, and Oracle NetSuite, trust Illumio to reduce cyber risk. For more information, visit www.illumio.com/what-we-do.

Gartner peerinsights™

See what customers have to say about Illumio.