illumio

CASE STUDY

Major Health Insurer Ensures PCI Compliance and Reduces Risk with Illumio

Tackling regulatory requirements and fortifying security with Zero Trust Segmentation

Customer Overview & Challenge

Cybersecurity stakes are higher than ever for the healthcare sector – only amplified by the COVID-19 pandemic and a growing ransomware epidemic. For a major health insurance company in the U.S. that provides benefits to millions, doing the work to mitigate cyber risk has been a growing priority. Being targeted by an attack put an onus on the company to shore up defenses against increasing threats and protect financial and health data.

Enhancing payment security for PCI DSS compliance was a priority initiative for which micro-segmentation was essential. The company had to isolate its payment infrastructure from out-of-scope systems. Failing to prove compliance could bring fines, drive up audit expenses, and be a reputational setback.

The team looked for a micro-segmentation solution that would get them compliant quickly. They explored a potential option from an existing vendor and ultimately ruled out its "heavy" approach that required additional hardware installation and a significant amount of human intervention to operationalize.

Beyond the initial PCI-driven case for micro-segmentation, new mandates to strengthen the company's security practices and incorporate Zero Trust principles called for enterprise-wide deployment. Traditional network-based segmentation would limit the ability to move fast, scale, and achieve granular control. The company needed a solution that would alleviate the complexity in segmenting an increasingly complex hybrid cloud environment.

Summary

Industry: Health Insurance

Environment: 35,000+ workloads (bare-metal, containerized, VMs) across hybrid cloud

Challenge: Meeting PCI DSS compliance requirements and extending micro-segmentation to the entire estate

Solution: Illumio Core to achieve PCI compliance and implement scalable Zero Trust Segmentation

Benefits: Significant time and cost savings; compliance with confidence; Zero Trust control and reduced risk

Illumio Solution

The team chose Illumio Core for Zero Trust Segmentation – and reaped significant operational and security benefits from its host-based approach, eliminating the need to re-architect the network or take on new hardware.

With an initial focus on PCI DSS compliance, the team gained centralized visibility of all services, workloads, and applications connecting to the payment and processing systems through Illumio Core's real-time application dependency map. Leveraging those insights, the team can quickly create policies to segment the PCI environment. Since Illumio Core follows an allowlist model, nothing will access the cardholder data environment (CDE) without explicit authorization; all other connections are denied by default. If there are any environmental changes, the policies automatically update, which gives auditors further assurance that compliance can be maintained and is part of an ongoing business process.

By isolating the CDE down to only critical components, the company reduced its scope, saving time and costs on compliance and increasing the chances of a simpler, successful PCI DSS audit. Within four months of deployment, the team achieved compliance with PCI standards.

The quick and early win set the foundation for continued success. The team has full confidence in Illumio Core to deliver on the need for stricter security measures and mitigate risk through intelligent visibility and Zero Trust controls. They are actively expanding Illumio Core across the entire estate – to the tune of over 35,000 workloads.

Customer Benefits

Time and cost efficiencies

Accurately scoping and reducing the CDE to the bare minimum ultimately lowers compliance and audit costs, while QSA-friendly reports and flow logs help speed up the process.

Security automation for compliance confidence

The company can maintain compliance in the face of changes since Illumio Core automatically adapts and updates policies if the PCI environment changes.

Increased Zero Trust, reduced risk

Implementing a Zero Trust model that provides full visibility and segmentation to limit the lateral movement of ransomware and attackers markedly reduces the health insurer's overall risk exposure.

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.