Akamai | TechnologyAdvice

Microsegmentation Moves the Zero Trust Needle for Commerce

Commerce organizations across retail, travel, and hospitality sectors make attractive targets for cybercriminals, ransomware gangs, and fraudsters intent on monetizing sensitive company or financial data. According to the RH-ISAC Industry Insights Report, the most common types of information targeted for theft include credit card and payment information, personally identifiable information (PII) from reward or loyalty programs, and intellectual property.

Already within an attacker's line of sight, these organizations — and their security teams — must contend with many potential intrusion points into the network for threat actors to deploy ransomware and other types of malware. All organizations face fallout from phishing emails, stolen VPN credentials, and zero-day exploits, but many commerce companies have to manage additional risk introduced by kiosks, IoT devices, in-store tablets, POS terminals, guest Wi-Fi, and more! Adding complexity, each retail location — which must be open to the public to do business — exposes a company to a physical attack surface and an entire range of additional threats.

Lucrative data and numerous attack vectors raise the stakes for enterprise defenders to make up for the leading cause of accidents — human error — accounting for 82% of security incidents. Increased regulatory scrutiny from the payment card industry (PCI) or government regulations (GDPR, SEC, etc.) adds pressure and further consumes already-strained IT security budgets and resources.

While eliminating all risk is impossible, today's commerce organizations must adopt an "assume breach" mindset to quickly detect and stop the spread of an inevitable infection or bypass of perimeter defenses. Zero Trust segmentation solutions from Akamai make it easier and faster for commerce businesses to secure their applications, servers, and network environments, and prevent both the damaging encryption as well as the exfiltration of sensitive data.

Microsegmentation, a capability best powered by a software-defined approach, provides a cornerstone for Zero Trust security frameworks that delivers upon three key capabilities for commerce organizations. First, microsegmentation naturally limits the potential fallout from a ransomware infection by blocking lateral movement. Next, it can help reduce the cost of achieving and maintaining PCI compliance. Finally, microsegmentation enables the granular visibility and coverage needed to protect modern — yet more complex — ecosystems across hybrid, multicloud, and microservices environments, as well as legacy infrastructure.

Limit potential fallout from ransomware

A click on an email phishing link, security misconfigurations, open RDP ports, or compromised credentials regularly provide the opening for attackers to begin exploring the network in search of your organization's crown jewels as they prepare to execute a ransomware attack. Companies that fall victim to a successful mass encryption event — and possible double extortion via data exfiltration — suffer multiple levels of financial loss and damage to the business.

Direct business losses could occur immediately as online orders and store operations slow or grind to a halt, with customers unable to purchase items or make hotel or airline reservations. Ecommerce operations may not be able to process, fulfill, or ship existing orders, as critical systems and servers become inaccessible or are taken offline in an attempt to limit the spread of an attack.

Indirect business losses begin with public embarrassment and damage to brand reputation if sensitive company or customer data is compromised. As a favorite tactic, ransomware gangs publicize attacks and leak data as both proof on "name and shame" sites to further extort victims and add pressure for a successful payout. Recent SEC requirements also force organizations to notify the SEC within four days of material impacts to the business, which fuels headlines — and reputation damage.

Recovery costs for legal expenses, incident response, data forensics, and breach remediation directly related to ransomware recovery will be high as consultants and IT teams work to recover data, restore backups, and bring systems back online. Yet even these expenses could be exceeded by litigation costs or regulatory penalties and fines triggered by the breach of sensitive information. Cyber insurance premiums may dramatically increase, ransomware claim payouts may be denied, or coverage could be dropped altogether.

There's a lot on the line — and not surprising that ransomware attacks were cited as the number one risk concern of retail and hospitality CISOs for 2024, and that security leaders are ready to invest in controls that can help reduce risk once attackers have established a foothold. But for ransomware to spread, attackers must be able to pivot and move laterally once they've gained initial access for maximum impact. The Microsoft Digital Defense Report 2022 notes that 93% of ransomware incidents resulted from inadequate lateral movement controls that allowed threat actors to lock up critical applications and infrastructure — and the median time for an attacker to begin moving laterally from an endpoint within the corporate network is only one hour and 42 minutes.

Akamai's recent State of Segmentation data noted that ecommerce organizations reported the highest number of ransomware attacks over the past 12 months when compared to other industry sectors. That's why CISOs and security experts are turning to Zero Trust–based security tools like microsegmentation to reduce the risk of a successful ransomware infection, minimize attack surfaces, and "break" the ransomware kill chain.

By detecting and blocking exploration via lateral movement, attackers will struggle to access the IT assets needed to escalate privileges, locate sensitive information, and propagate large-scale ransomware attacks. By applying principles of least privilege access to critical workloads across the entire commerce infrastructure, Akamai's analyst-recognized microsegmentation solution enables deep visibility into east-west dataflows of applications and workloads, and granular protection via software-defined policies to restrict lateral movement and stop threat actors in their tracks.

Even leading cyber insurance companies understand the value of microsegmentation. With ransomware driving both purchases and a surge in claims, many insurers have been forced to increase security control requirements and scrutiny, raise premiums — sometimes as much as 96% year over year — and reduce ransom payout coverage limits to account for significant losses. Some businesses are even being priced out of the cyber insurance market or denied coverage altogether. While cyber insurance alone won't prevent a damaging intrusion and resulting financial fallout, there are security controls — like microsegmentation — that allow organizations to more easily meet the latest underwriting requirements.

"With a single agent on a machine, we've solved the problem of an endpoint attack by lateral movement for good."

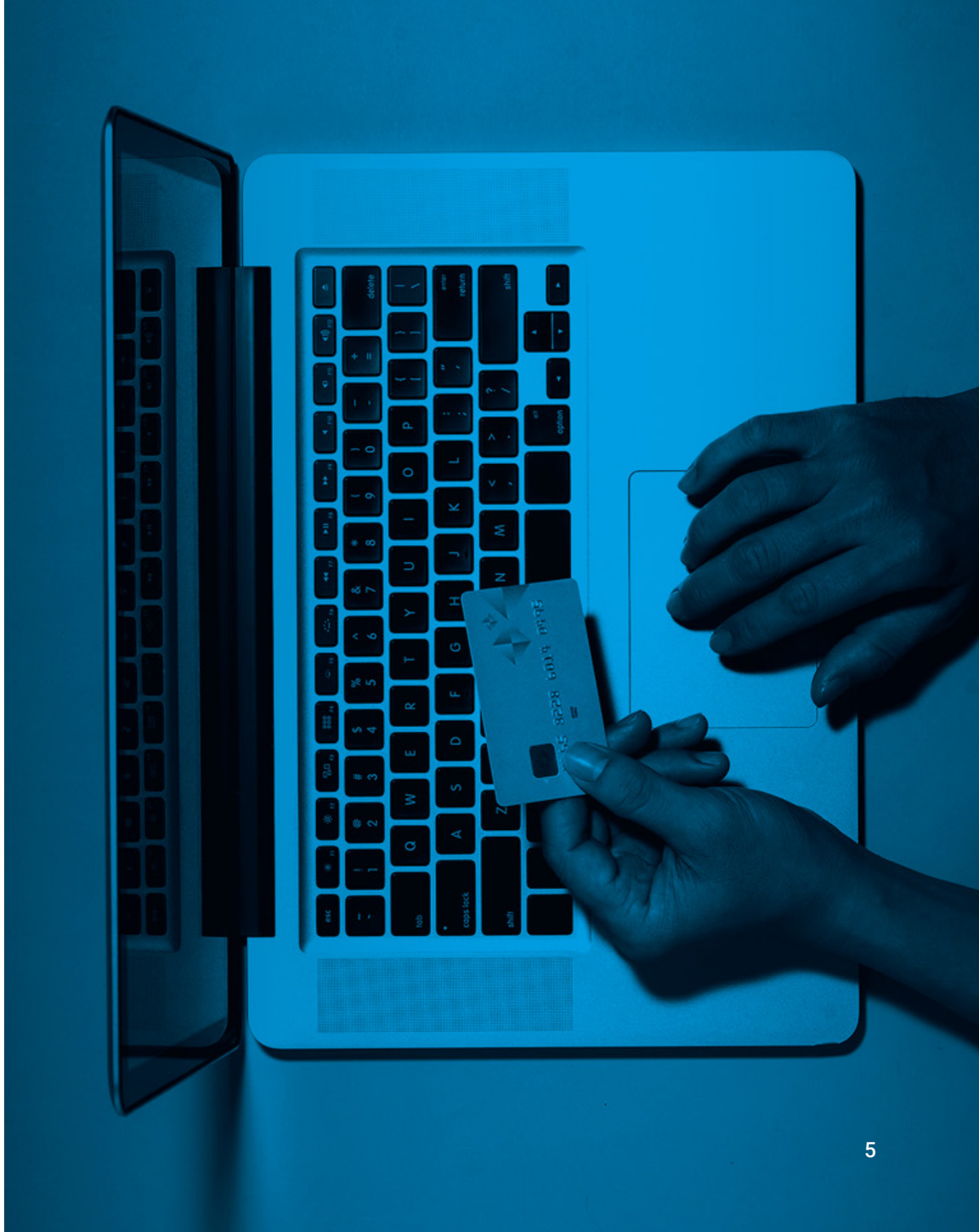
Infrastructure Architect,
Global Retail & Consumer Goods Manufacturer

Reduce the scope of PCI compliance audits

As ecommerce organizations are well aware, achieving and maintaining PCI compliance accounts for a sizable portion of annual governance, risk, and compliance budgets, and can place significant burden on security FTEs and resources. The PCI Data Security Standard (PCI DSS) requires ongoing audits of security policies and controls to protect the cardholder data environment (CDE). PCI scoping — which refers to the identification of people, processes, and technologies that interact with or could otherwise impact the security of cardholder data (CHD) — can also dramatically increase costs associated with conducting a PCI audit.

While network segmentation is not an official requirement of PCI DSS, commerce organizations have been using traditional methods of network segmentation for years — like vLANS, ACLs, and internal firewalls — to help reduce the scope, cost, risk, and difficulty of maintaining compliance. However, as the IT environments of modern retail enterprises have become more dynamic across hybrid, multicloud, and microservices architectures, legacy segmentation technologies and techniques can't keep pace, driving operational overhead, complexity, and application downtime — as well as security gaps.

This is because legacy segmentation methods are cumbersome to manage and maintain, consuming resources to ensure systems, networks, and applications within the boundaries of the CDE are properly secured and controlled. As organizations operate from the data center and cloud to container-based assets, many lack comprehensive visibility into application and system communication flows, and struggle to maintain PCI-required firewall configuration standards.



This leads to poor segmentation practices that can create security gaps and result in a failed PCI audit. That's why commerce organizations are turning to software-defined segmentation to more easily enforce separation between the CDE and out-of-scope systems across infrastructures, reduce the scope of a PCI audit, and accelerate compliance by enabling segmentation and enforcement up to process Layer 7, which is far beyond what legacy tools can support. Akamai's lightweight agent requires no firewall, network changes, or reboots to servers, and operates independently of the underlying infrastructure — which means no application downtime, as well as the ability to avoid change control or maintainance windows.

Because software-defined segmentation decouples security from the underlying infrastructure and operating systems, segmentation can be performed independently without touching the network or application. By taking this approach, commerce organizations can achieve granular network and asset visibility across environments, with a solution that acts as a distributed stateful-inspection firewall, to achieve complete coverage. And with less effort and resources required to deploy and manage, combined with a ~95% improvement in SecOps productivity, organizations can achieve a stronger security security posture while avoiding the many PCI compliance–induced headaches. As an added bonus, our solution enables commerce organizations to leverage real-time and historical views of the network to validate compliance during audits.

> "Software-defined segmentation allowed us to create and enforce segmentation policies at the process level, significantly improving both our security posture and the ability to meet PCI-DSS technical requirements."
>
> Sr. Infrastructure Engineer, The Honey Baked Ham Company

Gain visibility and coverage across IoT to legacy infrastructure

From stopping the spread of ransomware to managing PCI compliance security controls, commerce organizations also face the added complexity of securing physical locations like brick-and-mortar stores, production facilities, and distribution warehouses. For airlines, IoT sensors and devices can enable real-time monitoring and predictive maintenance of aircraft systems to enhance performance and safety. And hospitality organizations deploy IoT-powered devices to enable smart hotel rooms designed to drive customer experience and operational efficiency.

It's clear many of these locations and environments contain myriad internet of things (IoT) or operational technology (OT) assets that can't run host-based security agents, making them even more prone to hardware and software vulnerabilities. Research from Forrester's The State of IoT Security, 2023, noted that 33% of senior global security leaders cited IoT devices as the number one target for external cyberattacks. Organizations therefore need to deploy a segmentation solution with agentless functionality that can protect IoT and OT environments, and minimize risk that a threat actor will exploit a device vulnerability in an attempt to gain access to the broader IT infrastructure.

This type of solution must be able to continuously monitor for newly connected devices and automatically block unsanctioned devices from communicating with the network. Through integrated device fingerprinting, Akamai's solution automatically discovers and classifies connected devices into logical groups that form the basis for scalable, abstract security policies. Segmentation policies can be created for IoT and OT devices through a unified interface, and like other policies, they will follow the fingerprinted device regardless of where they are located (even as devices roam to new network locations) or how many there are in the environment.

Zero Trust–based policies are enforced via network switch ACLs without the need for an agent, eliminating enforcement gaps that can create risk across IoT and OT deployments. Establishing these secure boundaries still allows necessary connections to IT management systems, dedicated update servers, and logging servers to reduce security friction. Our solution allows you to discover, visualize, and map all IoT and OT systems alongside your IT infrastructure for a single view of your enterprise assets.

In addition to securing IoT/OT assets and other air-gapped endpoints, many retail organizations notoriously rely on systems, servers, and applications that run on legacy or end-of-support operating systems and infrastructure that can't be patched, creating significant risk. Many of these legacy servers can't be removed because they are still driving revenue for the organization or serve as the backbone of the company, especially for non-"born in the cloud" ecommerce enterprises. With the broadest industry-leading coverage and compatibility, Akamai's agents run on both modern and legacy operating systems, providing full visibility into network flows, down to the individual process and service levels for both Windows and Linux operating systems, along with coverage for MacOS endpoints.

Other solutions only provide partial visibility for legacy operating systems, with no optics into Microsoft Windows systems earlier than Windows Server 2008 R2. This is because the traditional microsegmentation solutions' agent relies on a Windows firewall to enforce policy, which was only available with systems later than 2002. Agents for Linux systems support Layer 4 visibility only, with no Layer 7 process-level rules for Linux environments, and are dependent on iptables to enforce policy. Akamai Guardicore Segmentation functionality is supported on almost all Windows and Linux operating systems — new and legacy — as our solution is not dependent on the underlying infrastructure to work.

Simple, fast, intuitive — and more secure

From the headquarters to the retail store and from the data center to the cloud — and beyond, microsegmentation is critical for adopting Zero Trust to secure and protect critical IT assets.

The simplicity of Akamai Guardicore Segmentation dramatically reduces the time and level of effort for deployment and enforcement, monitoring, and incident response compared to slower, traditional network segmentation methods. Any change in policy can be implemented rapidly and will not require complex network changes, which can be critical during peak sales seasons, promotions, product launches, or other high-profile events.

The bottom line: Just as you wouldn't ask your customers, guests, or passengers to choose between quality and safety — a good microsegmentation solution won't ask you to choose between security and agility. It's time to stop segmenting the hard way.

Ready to learn more?

Discover how to reduce your attack surface, secure critical applications, and streamline compliance with Akamai Guardicore Segmentation, part of the Akamai Zero Trust Portfolio.

Learn more

TechnologyAdvice | Akamai

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn.