SPOTLIGHT

Sponsored by: Akamai

Retailers require security that defends against myriad complex threats, makes business sense, and ensures a delightful — and secure — customer experience.

Shifting from Silos to Holistic Security: Microsegmentation as the Defensive Glue for Zero Trust

August 2022

Written by: Christopher Rodriguez, Research Director, Security and Trust

Introduction

Digital transformation has reshaped the world, improving the way businesses interact with customers, workers, and each other. But the process has not been without growing pains. New technologies and business practices have opened previously unimagined attack vectors. Simultaneously, advanced malware, insider threats, and zero-day vulnerabilities have returned to prominence, with ecommerce and retailers in the crosshairs. Cybercriminals are using ransomware, data theft, "name and shame" data leakage campaigns, and distributed denial-of-service (DDoS) attacks to extort and pressure victims.

These campaigns of extortion, disruption, and destruction can be devastating to business operations. Ransomware can render critical systems and servers inaccessible, grinding business — both in-store and online operations — to a halt. Cybercriminals steal sensitive data such as customers' personally identifiable information (PII), payment information, or intellectual property (IP). Data is then leaked or auctioned on the dark web to the highest criminal bidder, causing further damage to brand reputation and loss of customer trust. Retailers need not be targeted directly to be impacted, either — supply chain attacks have already led to an erosion of trust among partners and suppliers.

AT A GLANCE

KEY STATS

- » Digital trust programs were considered a "priority" investment by 57% of retailers and a "top priority" investment by 29% of retailers.
- » For 72.1% of retailers/wholesalers, "security" was the top choice overall among top factors deemed important to be perceived as trustworthy.

Source: IDC's *Future Enterprise Resiliency and Spending Survey, Wave 6*, July 2021 (n = 791).

Unfortunately, security can be a challenge for retail organizations as they must navigate a complex cyberthreat landscape with limited budgets, time, and personnel. For these organizations, the primary focus is always on the business, with priorities to ensure delightful — *and secure* — customer experiences. New security investments must make business sense and reduce operational complexity for retailers in addition to protecting against the latest security concern of the day.

Definitions

- **Microsegmentation:** A zero trust-based security technology to enforce granular access control, monitoring, and visibility at a workload level
- **Zero trust:** A framework of principles, controls, and best practices designed to modernize security architecture in response to new technologies and modern threats
- **Zero trust network access (ZTNA):** A technology that enables access to specific resources under well-defined, controlled conditions
- **Endpoint detection and response (EDR):** The next stage of endpoint protection software that detects and responds to threats that evade initial detection (Automation and predefined workflows assist in reducing time to response.)
- **Extended detection and response (XDR):** An architecture that combines telemetry from EDR with other sources such as network, web, and email to identify and mitigate sophisticated attacks
- **Security orchestration, automation, and response (SOAR):** A system that connects disparate security tools and processes to streamline workflows and automate security functions for improved efficacy and efficiency of the security operations center (SOC)

Microsegmentation Benefits Span Security and Business Objectives

Retailers have demonstrated a keen awareness of the importance of security. When survey participants were asked to identify the top factors that their organization deemed important to be perceived as trustworthy, 72.1% of retail/wholesale respondents selected "security" as the top choice overall compared with an average of 66.4% of respondents across all industries (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 6,* July 2021, n = 791). For retailers, security is important, but solutions must also make business sense.

Security Benefits

Implement Zero Trust Strategy

Zero trust strategy advocates minimization of trust zones, strong enforcement of context-based access policies, and continuous monitoring and threat detection. These principles require a more granular level of control than is possible through traditional segmentation approaches such as firewalls and virtual LANs (VLANs). Firewalls provide only a basic level of visibility into passing traffic via limited positions at the network perimeter or internal network chokepoints. Similarly, VLANs provide a coarse-grained Layer 2 approach to segmentation that cannot separate specific resources — systems on a VLAN can access other systems on the VLAN. The software-defined approach used by microsegmentation solutions enables the high level of granularity required to adapt network security to a resource-specific level by applying zero trust-based principles.

Broad Observability, Universal Coverage

Microsegmentation performs comprehensive discovery and inventory of applications and resources, addressing all assets, including Internet of Things (IoT) devices, by keeping up with modern application architectures. This practice ensures a strong security baseline, especially in large and complex retail environments. Advanced analytics are applied to further understand and map inter-application communications and dependencies. Profiling all devices and mapping communications between users, devices, assets, and resources provides an important detection layer for threats targeting legacy retail systems, infrastructure, and vulnerable protocols.

Threat Prevention and Detection

Continuous monitoring and continuous threat detection are key components of a zero trust strategy. Microsegmentation solutions do not simply enforce policy; they also aid in detecting threats. These solutions leverage advanced security analytics and automation to deliver dynamic, behavior-based detection and improve both mean time to detect (MTTD) and mean time to respond (MTTR). Time to mitigation is key, particularly in cases of ransomware attacks designed to evade defenses and spread rapidly to maximize havoc. Microsegmentation excels at mitigating ransomware damages through strong policy enforcement and threat detection capabilities. Even if adversaries gain an initial foothold, they are inhibited in their ability to propagate to enough of the network to where they can demand a ransom.

Enhanced Security Posture

The most sophisticated attackers utilize zero-day vulnerabilities and evasion tactics to gain persistent access to vulnerable systems. As with ransomware, once a foothold is established, attackers can move laterally at will to encrypt — and in some cases — steal data. The difference is these attacks aim to persist for long periods, during which time attackers can thoroughly search for and steal an organization's most sensitive data and IP for later sale, extortion, or harassment. Integration with SOAR enables correlation of threat signals to identify sophisticated attacks early in the kill chain. Microsegmentation provides a vital source of telemetry and signaling to detect threats, which can further improve SOAR detection. The benefit is bidirectional — SOAR orchestration capabilities can leverage microsegmentation to quarantine detected threats. Similarly, while EDR is a popular tool for protecting endpoints, these systems may still be vulnerable to zero-day exploits or sophisticated attacks that bypass EDR detections.

Business Benefits

Effective Security Requires Efficiency

IT buyers must shift beyond legacy approaches to segmentation such as firewalls and VLANs. In addition to waning security efficacy, legacy tools present performance bottlenecks and require extensive manual processes that become unwieldy for large or distributed organizations, thereby creating defensive gaps. Lacking profiling or automation capabilities, firewalls require manual management of rules and access control lists (ACLs) that are a drain on valuable — *and oftentimes scarce* — security resources. Policy changes are tedious processes for administrators, and firewall changes require Herculean efforts. Overall, firewalls and VLANs are simply not scalable or flexible, which is a particular challenge for large organizations. By comparison, microsegmentation uses automated profiling capabilities for rapid time to value and visibility into assets, data flows, applications and/or users.

Enhanced Value of Existing Investments

Microsegmentation leverages and enhances existing investments in security tools such as EDR and SOAR as control points for broader observability and added layers of defense. As a key component in a zero trust strategy, microsegmentation further complements the multifactor authentication (MFA) and ZTNA investments that businesses have already made. Microsegmentation provides "east-west" protection that complements ZTNA for a modernized, defense-in-depth security architecture. The combination allows organizations to take a stair-step approach to security transformation that supports the needs of various IT and line-of-business decision makers. Microsegmentation extends zero trust protections across the entire IT environment, allowing businesses to then focus on security modernization for specific use cases.

Enabling Digital Transformation

Security has a legacy as a hurdle or an afterthought in the process of adopting new technologies. Businesses have had to make difficult choices between improved productivity and business agility or reduced security posture. Ultimately, digital transformation has occurred regardless of the security implications. As a result, new threat vectors have emerged in recent years, thus requiring a modernized security architecture such as zero trust. However, security modernization and digital transformation can no longer be at loggerheads. When IDC asked retailers about their technology priorities over the next two years to ensure the long-term resilience and success of their business, 86% of respondents selected "digital trust" as a priority or top priority technology investment (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 6,* July 2021, n = 791).

Emerging Technology Trends and the Concomitant Need for Security Adaptation

Microsegmentation is one of many security solutions available in the marketplace at a time when security tooling and practices are being adapted to the modern digitally transformed enterprise.

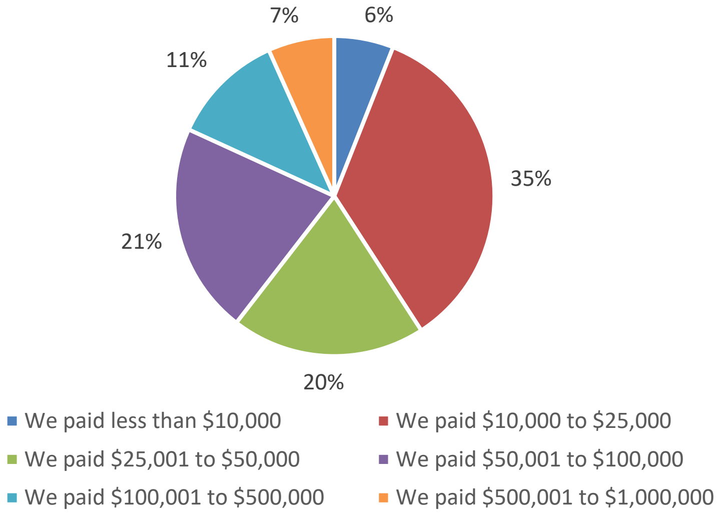
Advanced Threats Surge

In 2022, cybersecurity threats has surged once again. In IDC's *Future of Trust Survey* (February 2021, n = 507), the majority of respondents (30.9%) identified "increasingly sophisticated cybersecurity attacks" as the greatest challenge to establishing organizational trust. Ongoing high-profile data breaches and sophisticated attacks exacerbate concerns. For example, large international technology companies and security specialists have been the targets of sensitive data theft, including intellectual property and extortion.

Furthermore, security researchers noted that familiar botnets such as Emotet have returned to spread ransomware. IDC research shows that 44% of organizations experienced a ransomware attack in 2021 (IDC's *Future Enterprise Resiliency and Spending Survey, Wave 11,* December 2021, n = 858); 94% of retail/wholesale organizations that paid the ransom paid at least $10,000, and 18% of that group paid $100,000 or more (see Figure 1).

FIGURE 1: ***Ransomware Impacts the Bottom Line***

Q. *If your organization paid a ransom in the past 12 months to regain access to systems or data, how much was paid?*



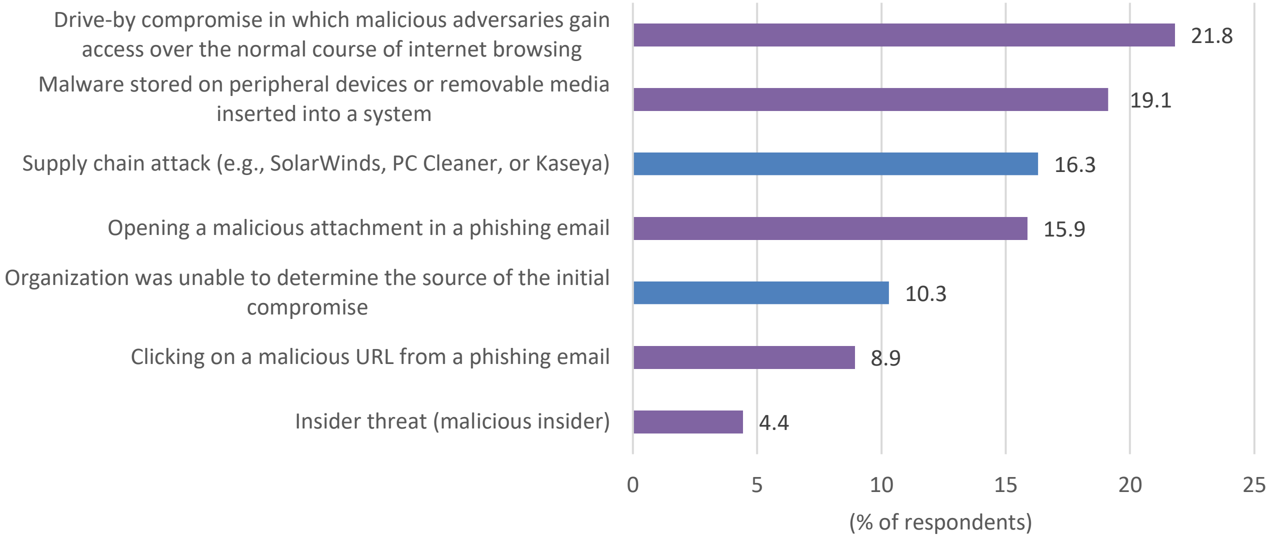
n = 100 retail/wholesale respondents

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2021

Insider threats can also be devastating and are traditionally difficult to detect as the insider has privileges granted by the organization. For example, Microsoft reported that LAPSUS$ gained access to sensitive Microsoft files including source code by bribing employees for illicit access. The LAPSUS$ group openly recruits on its Telegram channel for employees to provide credentials, answer MFA prompts, or install remote management software such as AnyDesk. Unwilling employees are targeted as well, including hacking of personal email account credentials or resetting account credentials through support systems. Users, whether intentionally or unintentionally, are often the key to enabling a ransomware attack (see Figure 2).

FIGURE 2: ***User Interaction, Whether Intentional or Unintentional, Enables Ransomware to Gain a Foothold***

Q ***For your most recent ransomware incident that blocked access to systems or data, what was the most significant source of the initial compromise?***



n = 444

Base = respondents who indicated their organization has experienced ransomware attacks/breaches

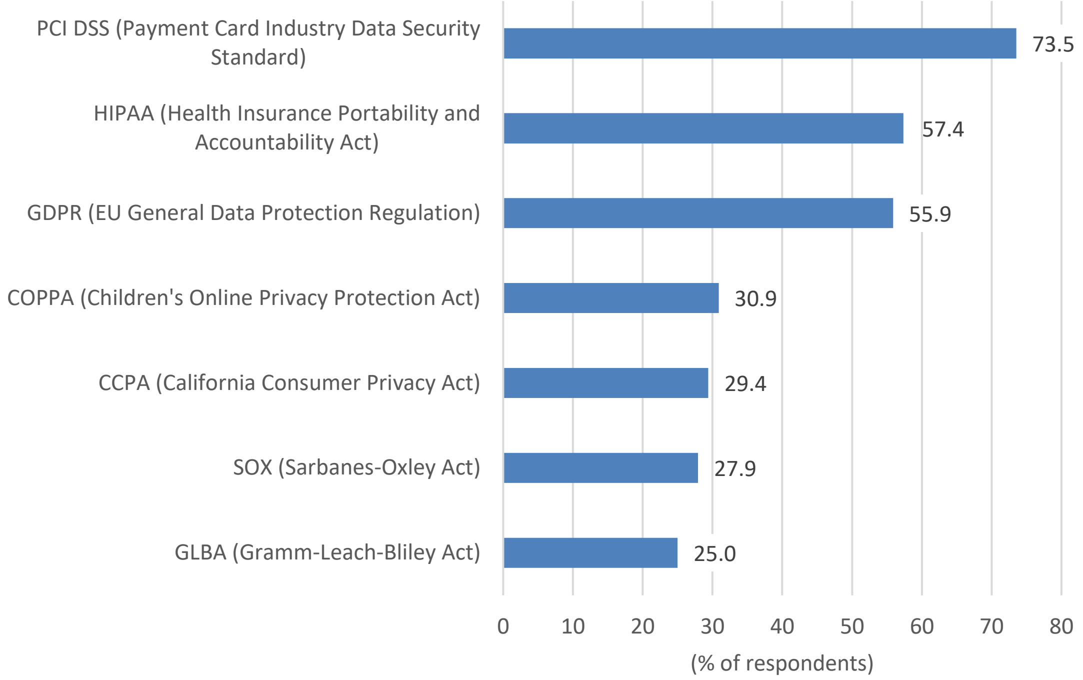
Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2021

Regulatory Requirements Proliferate

According to IDC's *Future of Trust Survey* (February 2021, n = 507), 27.5% of respondents identified "increasing and complex regulatory requirements" as the greatest challenge to establishing organizational trust, second only to "sophisticated cybersecurity attacks." Retailers face a number of regulatory requirements, with 50% or more of businesses beholden to PCI DSS, HIPAA, and GDPR (see Figure 3).

FIGURE 3: ***Retailers Face Regulatory Complexity***

Q *Which of the following data protection- or privacy-related regulations is your organization required to comply with?*



n = 68 retail/wholesale respondents

Source: IDC's Data Security Survey, January 2020

These regulations address consumer concerns regarding privacy and protection of sensitive data. Regulations such as PCI DSS have required retailers to segment networks for years because the practice protects the business as well as its stakeholders, including customers, employees, and partners alike. PCI DSS has continued to evolve in accordance with technology trends. The latest version of PCI DSS permits different methods of zone enforcement beyond firewalls. The change is welcomed as manual methods of compliance and reporting consume the time and attention of scarce internal security resources and budgets. The move to automated security such as microsegmentation will help lessen the burden of PCI attestation for retail security teams.

Digital Transformation Requires Security Modernization

Digital transformation enables retail organizations to improve productivity, reach broader audiences, and provide excellent user experiences that deepen brand loyalty. For example, cloud computing provides on-demand scalability to accommodate traffic surges — a major advantage for retail organizations adapting to seasonal sales trends. Cloud also offers utilization-based pricing that allows retailers to scale their computing costs as their business grows.

Unfortunately, cloud environments increase security complexity. Workloads may exist across different environments, each with varying degrees of security visibility or control available. With the rise in microservices architecture and containerization, legacy security tools are unable to adapt to workloads that are ephemeral and transient. Put simply: Legacy security tools are ill suited for the needs of digital transformation. The digital transformation era requires a much more fine-grained level of control than is possible with traditional network security controls.

While digital transformation has empowered businesses, it has also exacerbated standing security challenges, particularly in the areas of visibility and complexity. Retail IT environments were already complex and diverse, including IoT and operational technology (OT) systems for security and analytics, specialized systems for payment, order management and inventory, point-of-sale systems, terminals, and scanners. Over the years, systems that were thought to be protected by "air-gapped security" (not connected to the internet) no longer are. Some systems are owned by third parties or were simply forgotten. These devices vary in terms of sensitivity or ability to support an endpoint agent. Without an appropriate level of visibility, these systems are extremely vulnerable for even the largest retail businesses with sophisticated security practices.

Considering Akamai Guardicore Segmentation for a Holistic Security Strategy

Zero Trust and Security Enablement

Akamai Guardicore Segmentation provides a vital layer of visibility and control, which is an important foundation for a security modernization strategy. The solution enables key zero trust principles of least privilege access, strong authentication per session, continuous monitoring, and an "assumed breach" defensive mindset across the entirety of the IT environment. It provides granular visibility into the assets, data flows, applications, or users to enforce policies without sacrificing productivity.

As part of Akamai's zero trust portfolio, Akamai Guardicore Segmentation provides "east-west" protection, including behavioral analysis capabilities to prevent the lateral movement that ransomware and insider threats require to spread and cause damage. This is an ideal complement to ZTNA solutions that control "north-south" (ingress/egress) access such as enterprise application access (Akamai EAA) and MFA solutions (Akamai MFA). Akamai Guardicore Segmentation provides a complete breadth of security visibility and control across applications and workflows; EAA and MFA can then be rolled out to specific applications. In addition, Akamai SIA addresses a key zero trust requirement for threat detection by protecting users accessing the internet.

Security That Makes Business Sense

For retailers, blocking ransomware spread has a quantifiable benefit by preventing costly ransomware payouts. Akamai Guardicore Segmentation mitigates ransomware through strong zero trust policy enforcement and threat detection. Similarly, the solution helps prevent loss of data, reputational damage, and erosion of customer trust that impact the bottom line through fines, penalties, and lost future business. IDC also notes the following advantages of the Akamai Guardicore Segmentation solution:

- **Confidence in segmentation.** Previous methods of internal network segmentation, such as internal firewalls and VLANs, have failed and led to mistrust in the concept. Akamai Guardicore Segmentation was designed to eliminate those challenges and makes it achievable more efficiently for more businesses.
- **Security architecture support.** Retailers invest heavily in security but note diminishing returns when these tools operate in silos. Akamai Guardicore Segmentation complements and extends existing investments such as ZTNA, MFA, XDR, and SOAR.

- **Secure digital transformation.** More and more retailers are embracing microservices to rapidly deploy new workloads and applications to the cloud. Akamai Guardicore Segmentation enables mapping and control of workloads, communications, policies, and policy enforcement across complex heterogeneous cloud and hybrid environments. This insight helps enable and support innovation and agility via security controls that accelerate the process and don't slow the retailer down; there is also coverage for bare metal, virtual machines (VMs), containers, and agentless devices including IoT and unmanaged end-user devices. Control is provided per asset categories across critical applications, public-facing applications, domain controllers, endpoints, servers, and business-critical assets/data.
- **Security efficiency.** Akamai Guardicore Segmentation advanced automation and analytics capabilities provide efficiency and timeliness across multiple functions:
    - **Observability:** Comprehensive visibility, coverage for IoT-laden retail environments
    - **Regulatory:** Reporting, compliance by default (e.g., PCI, GDPR)
    - **Operational:** Flexible labeling and tagging assets, abstraction of networking technical details to simplify policy creation
    - **Timely, complete protection:** Defenses that offer features and functionality that go beyond Layer 4 separation and rules; broad coverage for legacy operating systems
    - **Optimization:** Incident response and management efforts that are designed to streamline threat remediation

Challenges

IDC notes some key challenges for Akamai Guardicore Segmentation. Microsegmentation has generally taken a back seat to high-priority, obvious control points such as MFA and ZTNA. Continued market education efforts will help emphasize the value of a holistic approach to zero trust adoption. While Akamai now offers both ZTNA and microsegmentation, integration is a necessary next step to deliver customer value. Cross-pollination between products is necessary to operationalize zero trust practices in large, complex retail organizations.

Conclusion

Microsegmentation has entered the security lexicon as a key technology for enabling zero trust principles. However, retail organizations have historically approached security as a steady march of emerging individual security solutions that end up in silos. Microsegmentation is a foundational security platform for business enablement and risk reduction. The value of microsegmentation is particularly pronounced for complex, business-critical retail IT environments.

The value of microsegmentation is particularly pronounced for complex, business-critical retail IT environments.

About the Analyst

Christopher Rodriguez, *Research Director, Security and Trust*

Christopher Rodriguez is a Research Director in IDC's Security and Trust research practice focused on the products designed to protect critical enterprise applications and network infrastructure.

MESSAGE FROM THE SPONSOR

Akamai Guardicore Segmentation (previously Guardicore Centra) helps detect and stop the spread of ransomware to limit the blast zone of an initial infection - before it becomes a business-impacting event. By applying principles of least privilege, microsegmentation enables granular protection and deep visibility into east/west dataflows of applications to stop the lateral movement of bad actors —keeping your most sensitive data protected.

With Akamai Guardicore Segmentation, retailers can also:

- More efficiently meet compliance and attestation requirements (i.e., PCI, GDPR, etc.)
- Scale and enforce consistent security policies across complex retail environments – with confidence
- Provide segmentation coverage for microservices-style architectures
- Adopt and deploy new cloud services without compromising security
- Modernize infrastructure while reducing both CapEx and OpEx for security

To learn more Akamai Zero Trust solutions for stopping the propagation of ransomware click here

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.