IDC ANALYST CONNECTION

Sponsored by: Akamai

Despite some time in the limelight as an overused buzzword, zero trust, for many organizations, has emerged as a North Star for implementing modern security frameworks to reduce risk.

Microsegmentation for Commerce: Zero Trust Requires Lateral Defense

June 2022

Questions posed by: Akamai

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

Q. How should retailers think about successfully deploying a zero trust architecture, and why should microsegmentation be considered a critical component?

A. Despite the misnomer, "zero trust" is an important strategy for implementing security required to enable commerce, which has an overall effect of boosting trust between businesses and their customers. When IDC asked IT buyers about their organization's technology priorities over the next two years to ensure the long-term resilience and success of the business, 85.9% of respondents in retail/wholesale rated "digital trust" as a priority or top priority technology investment (IDC's *Future Enterprise Resiliency and Spending Survey,* June 2021, n = 800).

Zero trust is a security framework — a collection of principles, controls, and best practices designed to modernize security in response to new technologies and modern threats. As such, implementation will look different from industry to industry because security use cases are based on the types of users they must accommodate. In commercial settings, the focus is on protection that is low friction. Consider the following use cases:

- **Shoppers have high expectations.** Customers expect a user experience that is seamless and delightful. Any hurdle, such as slow page load or a confusing CAPTCHA challenge is an opportunity to lose a customer.
- **Employees have work to do.** Security is an accepted fact of life but ideally will be invisible, as much as possible. In the best-case scenario, an inconvenience will simply be a productivity waster. The worst outcome is that employees may look for shortcuts or workarounds that increase business risk.

Overall, segmentation is a foundational practice for erecting security boundaries that protect the business as well as its stakeholders, including customers, employees, and partners. But the results can vary drastically. A successful segmentation practice will be transparent for users. Poor execution can lead to user frustration and broken applications.

Q. Why is software-defined microsegmentation a more effective alternative to traditional firewalls and VLANs to keep sensitive credit card and customer PII protected — and out of the hands of cybercriminals?

A. For years, retailers have been required to segment networks to meet regulatory requirements such as PCI and GDPR. Firewalls are typically deployed at network perimeters and strategic network segments such as datacenter egress/ingress and so can provide a basic level of visibility into traffic passing across network segments. Similarly, VLANs provide a useful control point for logical segmentation. But the visibility and control offered by both firewalls and VLANs are too coarse-grained for the modern threat landscape.

A cybermiscreant who can evade perimeter defenses would then be able to move laterally at will to identify data to steal or systems to sabotage. Insider threats, account takeover, and social engineering are all examples of threats that can render perimeter-based security inert. In these situations, deep visibility and fine-grained controls are key to stopping threats from escalating to catastrophic proportions. Ransomware is one threat in particular where a few minutes of difference in time to detection can translate to millions of dollars of damages.

The digital transformation era requires a much more fine-grained level of control than is possible with traditional network security controls. The software-defined approach used by microsegmentation solutions enables the high level of granularity required to adapt network security to a workload level. Microsegmentation solutions use AI and other analytical models to help IT organizations map and understand which applications are communicating with other applications, users, and devices. This breadth and depth of visibility is a critical first step to understanding risk in the business environment and enables businesses to enforce policies and detect threats at the necessary application-specific level.

Q. Why should security leaders consider microsegmentation as a complementary — and necessary — security control in addition to any endpoint detection and response (EDR) solution that might already be in place?

A. Certainly, retail businesses are keenly aware of the importance of security and have made investments in EDR to protect against data theft and ransomware. IDC research shows that 72.1% of retail/wholesale businesses rated "security" as the top strategy overall for building trust with their customers (IDC's *Future Enterprise Resiliency and Spending Survey,* June 2021, n = 800).

Establishing security is not an easy proposition though. Retail IT environments are complex, spanning branch offices, warehouses, outlets, and storefronts as well as the main offices and datacenters necessary to support growing online businesses. In the digital transformation era, each office undoubtedly hosts a myriad of devices, including specialized retail systems and terminals, IoT devices such as cameras for security and analytics purposes, employee BYOD, and guest access for customer devices.

Unfortunately, complexity is the enemy of security. Retail IT organizations typically lack the tools and time required to keep up with all the varied devices, use cases, and users on the network, leading to security blind spots and undiscovered vulnerabilities. Even the largest retail businesses with sophisticated security practices can be breached if they lack appropriate visibility. Systems that are thought to be protected by "air gaps" (not connected to the internet), forgotten, or owned by third parties have proven to be especially vulnerable over the years because they are often outside the scope of protection offered by legacy network security tools.

Investments in advanced security tools, including EDR, XDR, SIEM, and SOAR, are more effective when the tools provide more visibility. The combination of endpoint security and network security represents a particularly powerful security strategy. EDR provides deep, process-level visibility that is critical for detecting threats and assessing risk. Microsegmentation offers the comprehensive visibility possible only through a network vantage point. Thus, while least privilege access is a key value proposition for microsegmentation, the broad visibility into communications patterns and high-fidelity telemetry provided can be combined with EDR insights to reduce time to detection — an especially important survival factor in the face of a ransomware attack.

Q. How does microsegmentation enable scalable security for containerized applications and/or multicloud environments without slowing down retail innovation?

A. With COVID as a spark, retailers have been accelerating the migration of applications and workloads to the cloud, many of which deploy microservices architecture via Kubernetes to maximize speed, improve operational efficiency, and optimize DevOps-friendly workflows. Cloud computing has a particular allure for retail organizations because it offers on-demand scalability to accommodate traffic surges associated with seasonality trends. Similarly, utilization-based pricing makes perfect business sense, allowing retailers to grow their computing costs as their business grows.

Unfortunately, the race to the cloud has been fraught with the following complexity and challenges:

- Workloads now exist in a variety of locations, from on-premises offices and datacenters to multiple public cloud IaaS environments.
- IaaS environments may include optional firewall functionality, but with varying levels of control from vendor to vendor.
- Workloads may be ephemeral or may relocate with short notice or no notice, depending on developers and their plans as well as the processes employed by IT leadership.

As a result, IT organizations have been challenged to apply consistent protections or policies to workloads. Basic inventory, monitoring, and mapping efforts represent a Sisyphean task with a constantly moving target, and the complexity is only increasing. Microservices architecture is growing in popularity and coincides with growing adoption of new containerized environments to protect. These new cloud-native technologies, computing environments, and business practices are stimulating a massively complex level of communications that firewalls cannot control or even see.

Given the complexity of workloads and computing environments today, a zero trust practice is possible only using dynamic, AI-driven protections offered by microsegmentation solutions. Notably, in IDC's *Future of Trust Survey* (February 2021, n = 500), when respondents were asked to identify the areas in which their organization had invested or planned to invest to improve organizational trust, the leading response (44.3%) was "leveraging AI and analytics in cybersecurity processes."

Q. Why is it important for retailers — or any organization for that matter — to adopt a "post-breach" state of mind when thinking about their security posture, and how does microsegmentation help stop the spread of malware once attackers are beyond the front door?

A. We know that highly motivated attackers will find a way to penetrate defenses, especially when dealing with advanced or nation-state threat actors. Zero trust principles were developed after years of pernicious cybercrime, espionage, and sabotage campaigns by advanced persistent threats (APTs). Traditional APTs were able to evade perimeter protections and persist in victims' network environments with impunity, conducting extended data theft and surveillance campaigns. On the other hand, ransomware attacks are intentionally noisy, operating quickly to maximize damage and using high-pressure tactics to extort victims. Both threats remain a problem today, and with devastating effect for unlucky victims each year. Time to detection can mean the difference between millions of dollars in damages, loss of intellectual property, penalties and fines, and loss of trust.

Microsegmentation plays a foundational role in a zero trust strategy, providing "east-west" protection that complements zero trust network access (ZTNA) for a modernized, defense-in-depth security architecture. For example, while ZTNA provides access to specific resources under well-defined, controlled conditions, microsegmentation provides always-on protection to prevent insider threats, stolen accounts, or zero-day exploits from accessing applications. These solutions work hand in glove to enable key zero trust principles such as least privilege access, continuous monitoring, and "assumed breach" posture.

The reality of the retail environment is extreme complexity and lack of control over a sizable portion of devices and users, all overshadowed by a need for automated, frictionless security. Microsegmentation fills these needs through broad visibility, strong boundaries, automated detection, and lateral threat protection.

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

About Akamai Segmentation

Akamai 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 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
- 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

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