Akamai

7 MYTHS THAT TURN MINOR BREACHES INTO MULTI-MILLION DOLLAR DISASTERS

It may seem counterintuitive to think small when scaling big, but there are lots of misconceptions around modern microsegmentation solutions.

Think you'll encounter network downtime or difficulties operationalizing a software-defined deployment? Think again. Here's what's important when it comes to getting granular.

Myth 1

My EDR solution is enough to stop ransomware attacks

Endpoint detection and response (EDR) and segmentation both address ransomware attacks, but at different stages of the kill chain – and in different ways. EDR solutions aim to detect the presence of ransomware running or executing on devices or endpoints they are monitoring. If the EDR detects ransomware, it can kill the process, quarantine the device, and sometimes roll back any encryption that occurred. EDR and segmentation are complementary:

Should EDR not detect ransomware, segmentation solutions compartmentalize the network into siloed buckets to limit the lateral (east-west) movement of an attack. With ransomware, lateral movement must occur for attackers to be successful. Segmentation will ensure that attacks that have managed to advance beyond the endpoint will ultimately hit a roadblock, limiting the blast zone of an initial infection. Read more about the differences between EDR and segmentation.

1hr 42m

is the median time for a threat actor to begin moving laterally within the network once gaining an initial foothold

(Microsoft Digital Defense Report 2022)

Myth 2

I’m already doing segmentation

Segmentation is not a new concept – it’s just gotten more sophisticated. For decades, organizations have been using a patchwork of VLANs, internal firewalls, ACLs, and security groups to segment their environments. But these legacy methods haven’t evolved to meet the complex demands of modern hybrid and multicloud infrastructure, creating defensive gaps and blind spots through under-segmentation.

For example: Legacy firewalls do not map out or assess workflow dependencies, making it challenging to identify segmentations for applications, workloads, or users. Businesses are therefore forced to implement broad segmentation policies that are overly permissive and can easily – *and quickly* – result in dangerous misconfigurations that are difficult and cumbersome to troubleshoot.

With microsegmentation, organizations can segment and enforce up to Layer 7, far beyond what is possible with traditional segmentation tools.

$2.0M

cost avoidance of upgrading firewalls within three years

(Forrester TEI)

Myth 3

Microsegmentation is too difficult to operationalize

Modern microsegmentation is ready for enterprise prime time – now more than ever.

With Akamai Guardicore Segmentation, maximum operational efficiencies are achieved via the use of a single software-based solution for segmentation, visibility, policy creation, and enforcement across all environments – from the data center and cloud to container-based assets. Upon deployment, Akamai Guardicore Segmentation creates a dynamic visual map of the entire IT infrastructure that allows security teams to view activity down to the individual process level – on both a real-time and historical basis.

These detailed insights into application behavior can then be used to create granular microsegmentation policies quickly via an intuitive visual interface. Global deny rules, critical application ringfencing, and the ability to immediately segment large environments means rapid time to value – and reduced risk.

With legacy segmentation methods, you lack the visibility to even know where to start.

↓70%

Incident management effort reduced by 70% by Year 3

(Forrester TEI)

Myth 4

Microsegmentation means application and network downtime

With traditional approaches to segmentation, applications are often moved between subnets or VLANs, causing downtime and disrupting business continuity. Network engineers and firewall admins are left having to plan for scheduled downtime, change control, or maintenance windows, increasing the time to deploy new services or application updates. Even worse, these delays can result in increased risk due to asset exposure and vulnerability.

Software-defined segmentation, on the other hand, decouples security from the underlying infrastructure and operating systems so segmentation can be performed independently, without touching the network or application. If there is an event, instead of completely isolating affected machines, only the attack vector is blocked – limiting the negative impact to the business.

Microsegmentation can also be deployed in alerting mode to allow for testing policies in live production environments without the risk of downtime. The bottom line: Modern segmentation solutions shouldn't be a choice between better security and business agility.

Myth 5

Microsegmentation doesn’t cover my IoT or OT environment

Did you know that Zero Trust policies can be enforced for IoT and OT devices that are unable to run host-based security software?

Our agentless segmentation capabilities bridge the defensive gap between devices that can’t run agents to eliminate visibility blind spots – like air-gapped endpoints. This extended coverage is especially critical for healthcare, retail, and manufacturing environments with many network-connected (and vulnerable) IoT devices and legacy OT systems. Integrating agentless segmentation into your network infrastructure enables automatic discovery of new devices, fingerprinting, and policy enforcement to help mitigate risk while accelerating the enterprise-wide journey to Zero Trust.

Myth 6

A microsegmentation agent adds too much latency

One of the biggest misconceptions around microsegmentation is added latency.

In reality, using distributed, software-based segmentation policies instead of forcing all traffic through specific firewall chokepoints eliminates network bottlenecks. By design, the Akamai Guardicore agent is highly optimized to work with Linux, Unix, Windows OS, and MacOS, and does not consume substantial resources.

And because the agent is not in-line, it does not perform deep-packet inspection that can add to latency.

Instead, the Akamai Guardicore agent takes minimal information from the packet header to form a rich view of the customer environment. If you're looking for speed *and* performance, yes, you *can* have it all.

Myth 7

Microsegmentation means hiring impossible-to-find FTEs

With CISOs feeling the pressure to "do more with less," security solutions must lift the burden from defenders – not further consume scarce internal resources.

Traditional segmentation methods like managing firewalls and VLANs entail painful, multi-step processes involving many teams, separately responsible for switching, routing, firewall implementation, and security policy creation. A legacy firewall implementation can take 14 to 22 weeks on average. All of this adds to project timelines, subjecting the organization to significant labor costs and operational overhead.

In contrast, Akamai's software-defined solution takes on average two weeks to deploy – and only a single full-time employee. And by adding Akamai Hunt – our managed threat-hunting service – we'll save you time and resources by monitoring your environment for emerging attacks, lateral movement, and anomalous attack behavior.

These days, cyber talent is difficult to hire and even more difficult to retain. It's time that defenses work for – *and not against* – your organization.

Key Statistics

Proven ROI of up to ~ 152% within 12 months

(Forrester TEI)

How Akamai can help

Akamai Guardicore Segmentation is a software-based microsegmentation solution that provides the simplest, fastest, and most intuitive way to enforce Zero Trust principles. It enables you to prevent malicious lateral movement in your network through precise segmentation policies, visuals of activity within your IT environment, and network security alerts. Akamai Guardicore Segmentation works across your data centers, multicloud environments, and endpoints. It is faster to deploy than infrastructure segmentation approaches and provides you with unparalleled visibility and control of your network.

Learn how Akamai Guardicore Segmentation enables granular protection, deep visibility, and consistent enforcement of security policies at scale to keep your most sensitive data protected.