Akamai



# Segmentation and Zero Trust

## The Maturity Challenge

ISMG
INFORMATION SECURITY
MEDIA GROUP



**Michael Villar** used to be an Akamai customer. Now he's a director of field security technology. Akamai's approach to segmentation sold him on the company, and in this interview he discusses the maturity of segmentation solutions and how to maximize value.

**In this video interview with Information Security Media Group, Villar also discussed:**

- His background in segmentation technology;
- Whether maturity is a technology challenge;
- How to maintain momentum once value is created.

Villar joined Akamai as Director of Field Security Technology in the United States, previously Executive Director - Principal Engineer at Wells Fargo.

"When we talk about zero trust, there's no centralized way of enforcing end-to-end segmentation. We don't centralize the policy, we don't centralize the governance and we don't have a centralized audit trail. The telemetry is not shared, so there isn't a unified policy decision point."

## Segmentation Maturity and Zero Trust Gaps

**TOM FIELD:** In terms of the zero trust framework, how would you describe the maturity of segmentation today?

**MICHAEL VILLAR:** It's a mixed bag. Some areas are already very mature; for example, next generation firewalls, where we have a clear understanding and expectation of the role they play. There's a transition to move things closer to the endpoint. We have a lot more control there - and that's a newer type of technology. It's a new capability that we couldn't realize until we've had this much additional compute sitting on the workloads.

Because those things are new, they suffer from some maturity. It's a combination of organizations not truly understanding how that plays in and how that fits into their operating models and their existing security, risk and threat reduction efforts. But it's also a technology problem, and we've seen some players in the microsegmentation space fall off, and they're no longer operating because either the technology wasn't sound or there were some limitations that we didn't understand until we started deploying segmentation at scale.

There's some gaps with the technology in general, but for the most part, there are a few technologies that are bubbling up to the top as far as maturity is concerned; these technologies have addressed the underlying technology issues. The primary focus now is changing some of the perspectives on what a mature segmentation model looks like, what a zero-trust-aligned segmentation model looks like.

Ultimately, there's no centralized way of enforcing end-to-end segmentation. When we talk about all of the different tooling that might exist, whether it's zero trust network access solutions, the firewalls at the perimeter, zone-based design or microsegmentation, we don't centralize the policy, we don't centralize the governance and we don't have a centralized audit trail. The telemetry is not shared, so there isn't a unified policy decision point.

When we talk about zero trust, it is the foundational piece that's missing. How do we ensure that when an action is taken on one enforcement point or one area, how can we have parity of that action taken

someplace else? If I'm enforcing something at the perimeter, I want to see whether that can enforce something similar on the endpoint as well - not only from a defense perspective but also from a policy simplification perspective.

If I'm defining a single policy, I want that orchestrated across all of my different solutions without having to independently control them, and I don't want to independently control different orchestrators as well. This is the issue. Even if you had a best-in-breed solution across all of the different segmentation solutions that you have, you can't tie it all together, and that's the gap with zero trust right now.

## Technology Challenges in Zero Trust Segmentation

**FIELD:** Do you find zero trust to be a technology issue?

**VILLAR:** We've made strides on the technology piece, but it certainly is an issue. Enterprises are always looking to avoid vendor lock-in, so it goes back to the best-in-breed versus ecosystem kind of play, but they want a best-in-breed solution that operates as an ecosystem. API integrations don't cut it. You need to have just-in-time response on any type of enforcement point that is performing that type of function if it's a segmentation function.

The only way to do that requires the development of a custom abstraction layer where you can evaluate all the different signals and telemetry all at once, and then have a unified orchestrator for that, and have a way to do that at scale. When we particularly talk about enforcing microsegmentation, we are talking about granular rules applied directly to a host.

If you think of an organization that has 100,000 servers, that's effectively 100,000 firewalls that need to be operating in sync with any of the other traditional firewalls that have to be aligned with what you're doing on the ZTNA side. There is no technology that can make all the different layers work together. There are things that can make it easier, but that's the constraint of the technology side, and that's the technology aspect.

Considering the priorities for an organization from a segmentation perspective, there needs to be a better discussion on what a maturity model looks like in that space. We're not, as organizations, effectively taking the capabilities of microsegmentation solutions and layering it into the organization to provide the best value, so we measure things based on how many workloads have policies enforced on them.

We don't talk about how effective the policy is, we don't talk about the amount of risk reduced, and we are aiming to increase our time to market with enforcement rather than building a framework that allows us to implement our enforcement design across the entire organization. The automation gets ignored, which we've seen in security time and time again. Automation comes as an afterthought.

"Microsegmentation is an outcome of visibility. There are many other outcomes that exist as well. Organizations spend all this time and effort trying to deploy deep-packet inspection across as many environments as possible, and that's too much data, it doesn't scale, and it's extremely expensive."

But when you're dealing with 100,000 firewalls, it can't be an afterthought. There are entire organizations that are dedicated to managing and maintaining 500 to 1000 enterprise firewalls. Why does a team of microsegmentation get three guys? There's no way to scale that up from an operational perspective.

The criteria for success is not well-defined in alignment to what this product and the solutions offer, so we need to take a step back and think about how do we bring ourselves into that state where in three years, we want to see this type of adoption, and in five years, we want to see this type of improvement. Where does automation fit in that message? How can we improve visibility and enhancements to areas around security?

It ends up resulting in false starts. If you implement a policy for a subset of servers and you don't have telemetry or visibility on the other because you fast tracked the deployment and you don't have an agent on the other servers for whatever reason, you can build a policy, and it will work, and it's going to work fine.

But then when you're trying to make modifications to it - enhance it, improve it, incorporate a new use case - a regulator says you need to start doing environment segmentation now. How do we change that policy now? We can't. We have to start over and rebuild it. How do we handle novel applications? There's no way to continually improve the models, and that's the area where there is a gap with the segmentation - specifically zero trust segmentation.

## Maximizing Value From Segmentation Solutions

**FIELD:** What is the best way to get the most value from segmentation solutions?

**VILLAR:** This is probably an unpopular position to take because I found that in almost every single deployment that I've done, it's completely counterintuitive and it creates a lot of pushback. When organizations buy a segmentation solution, they're buying a microsegmentation solution, not a visibility solution. But practically speaking, it's the visibility you get. You're getting a level of visibility that can scale. You prune off the unnecessary data and payloads and things like that, and you enrich it

with data from the workload itself. That data is so incredibly valuable.

Organizations spend all this time and effort trying to deploy deep-packet inspection across as many environments as possible, and that's too much data, it doesn't scale, and it's extremely expensive. But what if we had something that can provide a similar level of value from a visibility perspective without all of that additional operational, technology and cost overhead?

That's what these microsegmentation solutions do. Microsegmentation is an outcome of visibility. There are many other outcomes that exist as well. There has been circumstances where I've sat in the room where we're going over matters requiring attention, and these are pretty significant directives, and it had to do with cyber resiliency.

Cyber resiliency could not understand the dependencies for the infrastructure that exists in a bank. When you look at mission-critical business services and the dependent solutions and technologies for them, if one of the servers were to be compromised or outright disappear, how long will it take to get it online again? And how do we know which systems are dependencies? This is a core function of microsegmentation. You need to understand how things communicate so that you can secure them.

If I understand how they communicate and understand what the outliers are and what we can expect and not expect, and I overlay that with the information from data sources like CMDBs, I can cross-reference the traffic patterns that we have to know how our organization actually operates compared to our expectation of how it should operate. We should be seeing critical infrastructure operating a certain way, but if I see inbound connections from the internet that we weren't anticipating, that's a red flag, and that's easy to detect. It stands out, it sticks out. It's very easy to identify.

There are so many use cases, which I observed during these implementations, that have come up because we now understand where to place focus and where to place emphasis. And the original use cases that we had, they fall by the wayside. They seem much less important when you realize there's potentially. If we have an active



attacker which we didn't even know existed, we can now see it with microsegmentation. How prevalent is this attack vector for us?

When you dig into the visibility piece, you start looking at who you can partner with in your organization and who can get value out of this data. Before you've even entered the enforcement space, you've already started to provide value. You haven't even turned on enforcement yet, and you've already closed out findings. You've cleared matters requiring attention. You've enabled the business to operate better. They understand how their platform works, they understand what deviations could look like.

All of these things align with that, and it makes the entire organization operate better when you know what you're doing. And that serves as a jumping-off point to enter the segmentation space to start reducing risk.




## Maintaining Momentum Through Visibility and Automation

**FIELD:** Once value is created, how does one maintain the momentum?

**VILLAR:** The momentum of these solutions is still predicated based on visibility and automation. What I found is that I can implement these solutions, and if I work closely with the business, I can also create value with them while securing things. The end goal is how do I provide a high degree of security and reduce a lot of risk without impacting the business? And if I can, how do I enable the business?

What I've come to realize is that we can simplify how our policy structure is in the security organizations. Let's look at defining our guardrails. Let's define our security policy and stay high level with it. Let's simplify what our security policy looks like as an organization and decouple the elements that are specific to the business application owners. If I understand how organizations should function at a minimum from a security perspective, I can place the rest of the capabilities onto the application owner.

If I give them an engine to serve themselves real time, the risk is low. They're making changes on individual workloads, and that is a low-risk change. They're not going to impact a large set of network devices like you would in a firewall. We're not changing network segments.

We're changing the function of individual hosts or a small subset of individual hosts. We're operating guardrails, so we know that our risk is never going to exceed our risk appetite, and in the event that there's something that could create friction where something is blocked where it shouldn't, we're self-serving that. Let them request that and have it implemented in real time so that they can stay innovative and keep moving. The business understands what they're doing, and they don't feel that they are breaking policy intentionally or unintentionally as they progress.

They're in a position where they feel confident to innovate, they feel confident that what they're building is going to be okay. They feel they don't need to go back and rework it and re-architect it; it's already operating within their guardrails, and it's like a self-service model and a software secure by design model.

## Akamai's Approach to Segmentation

**FIELD:** In terms of Akamai's approach to segmentation and as a former client and now a director, what makes the difference?

**VILLAR:** There are three things that stuck out to me when I worked with Guardicore, which is the flexibility of the platform. You're going to need every different lever you can pull when you're doing an implementation. You're going to need to have different capabilities across different types of environments, and you have to design your policy for the common denominator across them. If you have a capability that only works for Windows and doesn't work for Linux, then that capability is effectively useless because I can't apply it across my entire estate.

Akamai abstracted the firewall component and optimized the firewall component, which means that there are no interdependencies, there's no contention with other tools that might interact with that underlying component, and I have more options available to me to do that type of enforcement. There was no limitation ever, which is no substantial limitation or anything to that extent with labeling. I was always able to incorporate all of the data that I need. It's able to collect all the telemetry. I don't have to decide if I need to ignore a subset of traffic because the system can't scale.

And those types of things - from a technology perspective - enable us to move the needle forward. It lets me build policy for circumstances for that last 10% that is difficult to create a policy for. It's difficult to cover. I see that as the main technology aspect, but there was another piece to it.

Every time that I work with the Guardicore team, they've done things to enable Akamai and its teams that are doing the segmentation, which I have never seen any other vendor do in my career. We've had circumstances where we've had issues, and I had an entire team fully available to me either remotely or in person or in both for as long as it took to get it resolved.

If there was an issue that required an enhancement and it made sense for them as an organization to do, I had a commitment for these things. They operate as an organization that is looking for your success. And that was different from what I experienced even at large enterprises where I've submitted enhancements to a lot of the big organizations out there that we partner with.

It took five years to get an enhancement in place, and that's the kind of stuff that it creates a huge strain on the technical teams. It creates a huge strain on our project. We have to build around that, architect around that and build strategy around the fact that there's a capability that we need that we don't have.

I don't like being upsold on things that don't work, and I like commitments. And I don't expect perfection in technology, but if people are willing to partner, they're willing to build the stuff that we need and they're willing to do the right thing, that makes all the difference. That's where I found some of the most value from the technology teams.

## Where to Learn More About Segmentation

**FIELD:** Where can our audience go to learn more about segmentation?

**VILLAR:** They can go to https://www.akamai.com/security or https://www.akamai.com/products/akamai-guardicore-segmentation. There's tons of information that dig into the different security offerings that we have. Specifically within the Akamai-Guardicore segmentation component use cases, there are plenty case studies as well, and videos and demonstrations that tie into it.

A lot of this information can answer a lot of the questions. But if not, feel free to reach out to me directly, and I'll see if I can set up some time to have a conversation.



## About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY® CAREERS INFO SECURITY® Data Breach TODAY Prevention. Response. Notification. CyberEd.io

ISMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io