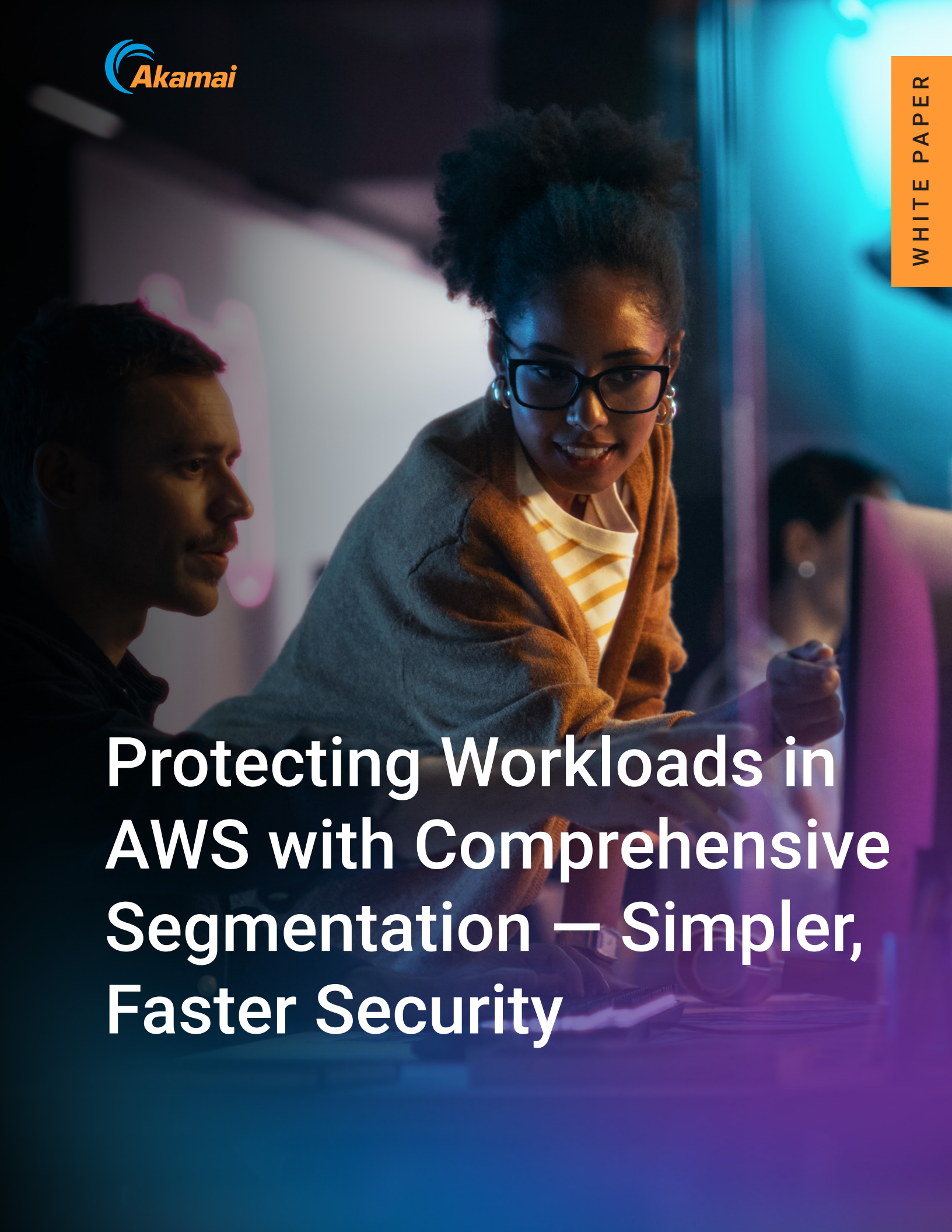


WHITE PAPER

Protecting Workloads in AWS with Comprehensive Segmentation — Simpler, Faster Security

Introduction

Don't let security concerns hold back cloud adoption. One solution can handle visibility, lateral movement prevention, and breach detection and response for assets and resources in AWS.

The benefits of using platform as a service (PaaS) resources in Amazon Web Services (AWS) and migrating critical workloads off-premises are clear: It takes infrastructure costs and maintenance off your hands; improves scalability and elasticity with almost limitless resources and power; and uses the latest innovations, such as machine learning and AI, to boost performance and analytics. However, security concerns are holding many enterprises back, especially since cloud resources are among the top targets for cyberattacks.

The challenge of security in AWS

When considering a whole new environment, it isn't surprising that you will need to revisit security from scratch. You may be a complete newcomer to the cloud — or you may be migrating from a different vendor, choosing a new hybrid solution, or adding AWS to your existing ecosystem. In any case, the cloud requires its own specific toolset to handle the unique challenges that this infrastructure presents. Some factors are common for all cloud vendors, while others will be unique to Microsoft Azure, Google Cloud Platform, or AWS. Here are some of the top concerns for businesses that use cloud or hybrid cloud that include AWS technology.

Understanding shared responsibility: When you shift your workloads to AWS, or when leveraging its built-in PaaS resources, you need to recognize that you still hold a lot of responsibility. You will need to secure customer data, applications, and platforms. The lack of understanding around the shared responsibility model is why Gartner predicts that 99% of cloud security failures will be the customer's fault through 2025.

Lack of visibility: You can't control what you can't see. In the cloud, visibility is a lot more complicated, especially when it comes to protecting and visualizing network traffic that moves east-west as well as north-south. Looking at flows alone is not enough. Your critical assets may be spread across multiple AWS accounts, containers, or network security groups — and without contextualizing all of this, it can be impossible to accurately get a sense of flows and interdependencies.

Limited control for policy creation: If your business is used to having insight at Layer 7 on-premises, you aren't going to want to take a step back to just Layer 4 visibility, losing that granular insight and control now that your workloads are in the cloud. Amazon Security Groups support controlling traffic to Layer 4. But with Layer 7 visibility and control, no matter the underlying infrastructure, you can do more than rely on ports and IPs alone, which are largely insufficient for breach detection or troubleshooting.

Container security: AWS uses Amazon Security Groups to apply policy for container security, but this is limited to clusters rather than individual pods. For full insight into communications, you need a solution that can recognize the context of an overlay network running on top, and can drill down in a granular way to the pod level. This gets more complex when you want to create network policies that include both virtual machines (VMs) and containers, and can often result in organizations handling two sets of security controls.

PaaS adoption: There is a significant trend toward adopting PaaS resources in addition to migrating critical workloads to the cloud, reflecting the evolving needs of cloud-centric organizations. These PaaS resources cannot support agents, however, so most agent-based security solutions are too limited to extend full protection over PaaS resources. This can lead to fragmented cloud security policy, creating additional overhead for your teams and potentially leaving security gaps that can be exploited by threat actors.

Combating these issues with an all-in-one security platform

Amazon provides certain built-in tools, such as Amazon Security Groups, that work to combat some of the challenges of migrating your infrastructure to the cloud. We encourage organizations to get the most out of AWS identity and access management (IAM) by using groups to assign permissions, rotating credentials regularly, and using IAM groups to ensure simplicity. However, these tools alone are just a starting point in today's dynamic public cloud, especially when you consider a hybrid environment that covers anything from legacy infrastructure to container technology, and PaaS resources that are being employed in different public cloud environments.

A sophisticated security solution will allow you to complement what AWS provides with a technology that removes blind spots and works seamlessly with the rest of your security stack, even in a hybrid environment. Here's what Akamai offers.

Full visibility of AWS instances

The more complex your IT infrastructure becomes, the more important it is to have deep, automated visibility. Manual moves, adds, changes, and deletes are not just unreliable and prone to gaps and errors, they are a slowdown, and therefore a barrier to cloud adoption. In contrast, enhanced and automated visibility will discover all applications and flows, adding visibility to your instances all the way to the individual process level.

Akamai Guardicore Segmentation, the core offering of the Akamai Guardicore Platform for Zero Trust, includes a powerful AWS API that pulls in orchestration data along with a dedicated component for collecting asset, flow, and tag information, giving you valuable context that you can use for labeling and application mapping. As you baseline your infrastructure, you have the details you need to fully understand how your applications communicate with one another, where the interdependencies are, and how policy should be created to enable fluidity and agility. Rather than having a separate security solution for each cloud vendor or environment, users can visualize native-cloud information and AWS-specific data all on the same dashboard. Our solution works across platforms, infrastructures, and clouds, so you can be guaranteed to have zero blind spots.

Segmentation and enforcement — one policy that follows the workload

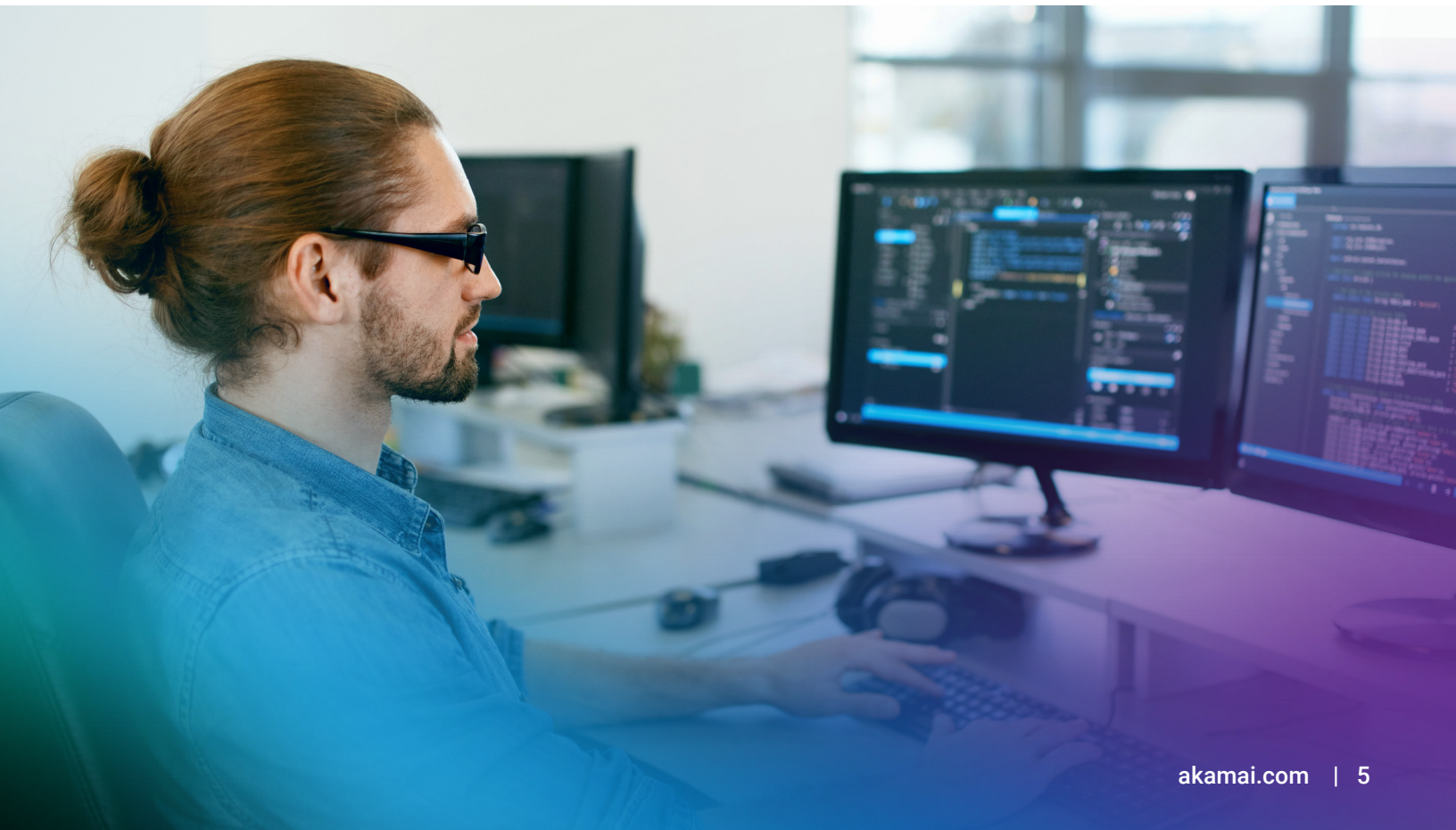
Once you've achieved this "single pane of glass" view across all your environments, you can begin to design and deploy security policy. Application-aware policy goes further than Amazon Security Groups alone can achieve, providing Layer 7 (as opposed to Layer 4) granularity. While some organizations are attempting to use next-generation firewalls on-premises to limit lateral movement, this only supports coarse segmentation of east-west traffic. It is prohibitively difficult as a solution for granular segmentation controls because of the need for massive infrastructure and networking changes to reroute traffic through the firewall. Even if it was an option on-premises, it also leaves organizations with the problem of retaining this level of control on the cloud.

Layer 7 microsegmentation is the answer, with policy built for dynamic workloads, without the need for changing the underlying network infrastructure at all. As the policy follows the workload itself, we've removed the need for manual changes and enhanced your organization's ability to embrace agility and fast-moving DevOps processes. One microsegmentation policy can simplify a hybrid environment by enforcing rules across regions, VPCs, containers, VMs, and on-premises, all with one consistent policy expression. Starting with the visibility we provide, you can define and apply segmentation policies in mere minutes. Your policy creation process is also enhanced by automatic policy recommendations that provide best-in-class security protocols on the public cloud.

Breach detection and incident response on the AWS Cloud

With Akamai, you can take your AWS security further than segmentation or visibility alone. Detecting policy violations is an important part of breach detection, allowing you to respond to a potential cyberthreat in real time with application-level detail. We offer multiple breach detection methods that can immediately alert you to malicious intent in a hybrid cloud environment.

- **Reputation analysis:** Automatically detect suspicious information within flows, from domain names and IP addresses to file hashes and command lines
- **Dynamic deception:** Engage the attackers without their knowledge, diverting them to a high-interaction honeypot environment where you can safely learn from their behavior
- **Tools to speed incident response:** Integrate with AWS to allow any policy violations or security incidents to be sent in real time to the AWS Security Hub
- **Custom threat hunting:** Capitalize on the infrastructure and massive global threat intelligence of Akamai to stop the most evasive threats in your hybrid cloud environment with our Akamai Hunt service



Bringing it all together for enhanced security on AWS and beyond

Reaping the benefits of the public cloud doesn't have to mean settling for lesser security, visibility, or control than your organization enjoys on-premises. With Akamai, you can gain complete visibility of your AWS assets and resources alongside your entire infrastructure. Using this foundational map, policy creation is seamless and enhances existing security measures to provide granular control without the need for manual support. The complements of breach detection and incident response give you a single end-to-end security solution that covers all your bases on the AWS cloud and beyond.

Please visit akamai.com/guardicore for more information.

About Akamai Security

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. 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. Published 11/24.