AKAMAI SOLUTION BRIEF

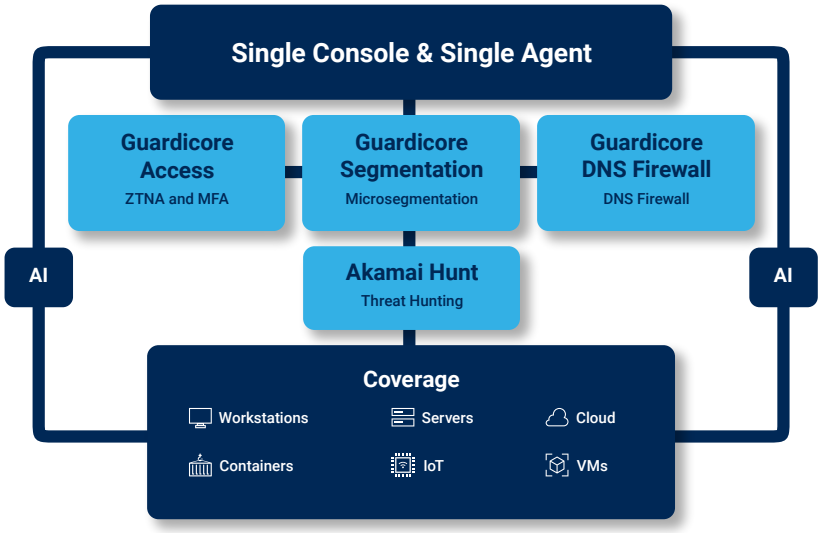
The Akamai Guardicore Platform: Zero Trust Security

Implementing Zero Trust is prohibitively complex and expensive for most businesses, especially when those protections must cover assets on-prem and in the cloud, and a workforce that is remote or in the office. This is why the Akamai Guardicore Platform is built to efficiently address all facets of Zero Trust with one console and a single agent.

As cyberthreats become increasingly sophisticated and regulatory requirements continue to tighten, organizations face immense pressure to secure their networks while maintaining operational efficiency. The Akamai Guardicore Platform offers a comprehensive Zero Trust solution to address these challenges by providing organizations with the tools and capabilities needed to implement a robust Zero Trust security model effectively.

The Akamai Guardicore Platform is built to enable Zero Trust projects by combining best-in-class microsegmentation, Zero Trust Network Access (ZTNA), DNS firewall, and threat hunting into one platform. Together, these components streamline Zero Trust efforts to significantly reduce the attack surface and strengthen security posture across the entire enterprise.

The Akamai Guardicore Platform



Microsegmentation

One of the key components of the Akamai Guardicore Platform is microsegmentation. Traditionally, network security has relied on perimeter-based defenses that focus on securing the outer boundaries of the network. However, as cyberthreats evolve, it has become increasingly clear that perimeter defenses are no longer sufficient to protect against sophisticated attacks.

Benefits

Consolidated infrastructure
Deploy quickly and scale effortlessly with minimal impact on performance.

Broad and rich visibilty
Gain comprehensive insights into network assets and communications.

Unified policy engine
Simplify policy enforcement across diverse environments from a single UI.

Modular flexibility
Leverage modular components tailored to your business requirements.

Complete coverage
Protect all of your assets on-prem and in the cloud, and users at home and in the office.

Best-in-class solutions
Combine industry-leading microsegmentation and ZTNA for enhanced security posture.

Akamai

Microsegmentation takes a different approach by dividing the network into smaller, more manageable segments and applying security policies to each segment based on the principle of least privilege. This granular approach to security ensures that even if one segment is compromised, the rest of the network remains protected. With Akamai Guardicore Segmentation, every asset is protected, including on-prem data centers, cloud instances, legacy OSes, IoT devices, Kubernetes clusters, and more — without ever having to change consoles.

Zero Trust Network Access

In addition to microsegmentation, the Akamai Guardicore Platform also offers Zero Trust Network Access (ZTNA) capabilities. ZTNA is a security model that assumes Zero Trust, meaning that no user or device should be trusted by default, even if they are inside the corporate network. Instead, access to resources is granted based on strict verification of identity, device posture, and other contextual factors. This approach minimizes the risk of unauthorized access and helps organizations prevent data breaches and insider threats.

DNS firewall

Another critical component of the Akamai Guardicore Platform is the DNS firewall. DNS (Domain Name System) is a fundamental component of the internet that translates human-readable domain names into IP addresses. However, it is also a common target for cyberattacks, as many malware variants rely on DNS to communicate with command and control servers or to exfiltrate data. By deploying a DNS firewall, organizations can block malicious DNS queries and prevent malware from communicating with malicious domains, thereby reducing the risk of data breaches and other cyberthreats.

Threat hunting

Finally, the Akamai Guardicore Platform includes an adaptive segmentation service that enables organizations to proactively identify and mitigate security threats before they escalate into full-blown incidents. Threat hunting involves actively searching for signs of compromise within the network, such as anomalous behavior or indicators of compromise (IOCs). By leveraging threat hunting tools and techniques, organizations can stay one step ahead of cyber adversaries and protect their valuable assets from harm.

In addition to its core capabilities, the Akamai Guardicore Platform also offers several key benefits that set it apart from other security solutions on the market. The platform provides a lightweight and consolidated infrastructure that minimizes agent bloat and console fatigue, allowing organizations to deploy and manage their security stack more efficiently. Furthermore, the platform offers broad and rich visibility into network assets and communications, enabling security professionals to gain comprehensive insights into their network environment, and respond to threats quickly and effectively.

> Gartner suggests implementing microsegmentation and/or ZTNA to move toward a Zero Trust Networking (ZTN) posture.
>
> **– Gartner®, Quick Answer: What Is Zero Trust Networking? Andrew Lerner, John Watts, 13 September 2023***

*GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.