

Akamai Guardicore Access Unified ZTNA and Microsegmentation

A single console for visibility and control simplifies and accelerates Zero Trust

Organizations are rapidly adopting Zero Trust security to stop ransomware, meet compliance mandates, and secure their hybrid workforce and cloud infrastructure. Zero Trust Network Access (ZTNA) and microsegmentation are the two most critical solutions for enterprises that are moving to a Zero Trust architecture. Together, they help reduce the attack surface, contain breaches, and provide better access control with an improved user experience.

The power of unification

Akamai Guardicore Access combines segmentation and ZTNA; they are deployed with a single agent and managed with a single console. This innovative approach ensures comprehensive visibility from user to workload (north-south) and endpoint to endpoint or workload (east-west), enabling identity-based application access control and endpoint segmentation in one fell swoop. By combining these technologies, enterprises benefit from a robust security framework that fortifies network defenses, mitigates risks, and fosters a secure and compliant environment.

The Akamai Guardicore Platform is the first security platform to combine industry-leading microsegmentation and ZTNA to help security teams prevent ransomware, ensure compliance regulations, and protect both the hybrid workforce and cloud infrastructure.




For the first time ever, organizations can implement segmentation to minimize their attack surface while also easily managing access to their hybrid workforce from everywhere – with a single agent using a single console across all types of assets and infrastructures.

Key capabilities

End-to-end visibility

Gain full understanding of your network with end-to-end visibility, showing on both the map and the logs, and providing insights into end users' access patterns. This is made possible only by combining segmentation and ZTNA into a single product. See connection pathways, from endpoints to workloads, down to the process level. Near real-time and historical visibility makes forensic analysis easier and mitigation faster.

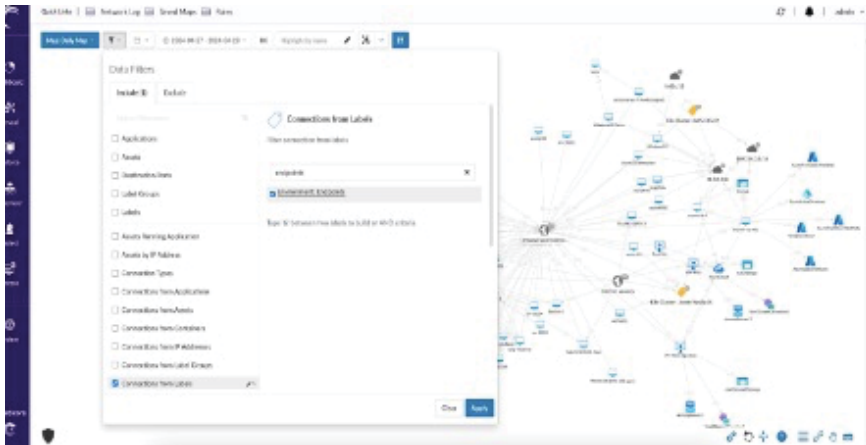
Benefits for your business

-  **Single console, single agent**
Implement segmentation to minimize the attack surface while also easily managing access to a hybrid workforce from everywhere – with a single agent using a single console
-  **Broad coverage**
Apply access controls everywhere and secure workforces remotely and in the office
-  **Unified policy**
Enforce policy for east-west traffic and north-south access, without changing syntax or consoles, for the simplest and most effective means of acting on Zero Trust



Application discovery

Reduce time to policy by quickly identifying the applications that need access permissions. Effortlessly discover your private applications and gain valuable insights into their use patterns, including user access and frequency.



Easily discover the applications for which access is required

Access and segmentation policy synchronization

Automatically sync access controls and segmentation rules to reduce cross-team dependencies and eliminate room for human error.

Primary use cases

Comprehensive ransomware protection: Reduce the likelihood and impact of ransomware and other malware attacks with identity-based and machine-to-machine policies. Ensure that endpoints access resources on a least-privilege basis while enforcing granular access controls.

- Protect high-value assets: Allow users to access critical assets based on secure access controls and block direct VPN traffic
- Restrict privileged users: Block VPN traffic to exploitable admin ports to provide secure access for admins

Workforce distribution: Support working from everywhere by enforcing strict access controls, ensuring that each device only connects to the resources it needs. This minimizes the attack surface and reduces lateral movement within the network.

Compliance: Implement endpoint segmentation policies so businesses can ensure that their endpoints comply with relevant industry standards and regulations, which reduces the risk of noncompliance penalties and strengthens their overall security posture.

Third-party access: Enable contractors and partners to connect to specific applications without installing an agent by routing and authenticating their access through a dedicated Akamai portal.

Visit [Akamai Zero Trust Security](#) to learn more

