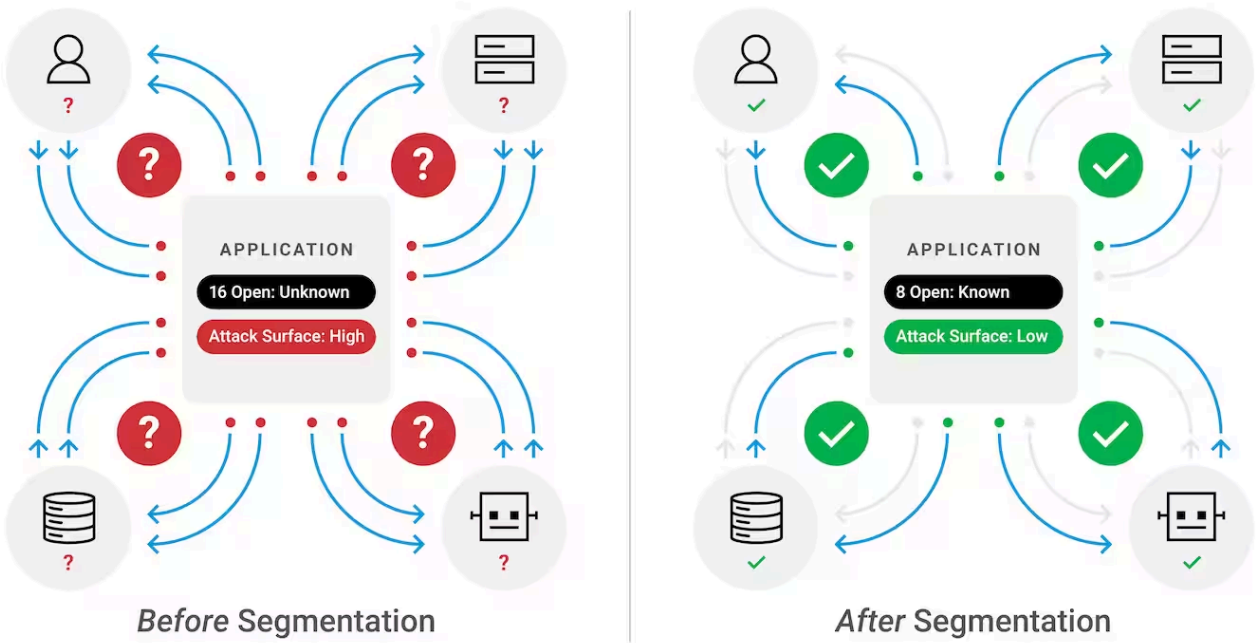
What Is Software-Defined Microsegmentation?



Software-defined microsegmentation is a network security technique that splits or segments a network into extremely granular areas, allowing individual workloads, applications, and virtual

Diagram illustrating network segmentation.

machines (VMs) to be protected by narrowly defined security controls. In contrast to traditional network segmentation, which primarily uses hardware and protects traffic flowing in and out of the network (north-south traffic), microsegmentation is managed with software and protects traffic that flows between applications and assets within the network (east-west traffic). By isolating application workloads and controlling communications with precise security controls, administrators can contain any security breach by blocking lateral movement while supporting a Zero Trust security model, reducing the attack surface, and improving regulatory compliance.

Why is software-defined microsegmentation important?

With digital transformation— including the rise of cloud computing, hybrid cloud networks, and remote workforces — the traditional security perimeter has essentially disappeared. Organizations can no longer secure their organizations from cyberthreats by simply focusing on a secure network perimeter. Attackers are constantly finding ways to bypass cybersecurity defenses, breaching one part of a network and moving laterally through it to access high-value targets. Microsegmentation enables security teams to adopt a Zero Trust approach that focuses on placing security controls around individual workloads. As a result, attackers who have breached one part of a network can be stopped before they can access additional assets.

What IT assets can be protected with microsegmentation?

Microsegmentation techniques can protect applications, servers, VMs, containers, microservices, and individual workloads — essentially, any code or application that uses memory and CPU. In this way, microsegmentation provides more granular protection than techniques that simply isolate entire applications, devices, or networks.

How does software-defined microsegmentation work?

Microsegmentation is applied using software-based technology that enables administrators to set and manage security policies from one location, rather than configuring routers, switches, firewalls, and other network equipment. Microsegmentation solutions enable administrators to perform several critical steps as they segment important IT assets.

- **Visualize activity at the application layer.** To implement microsegmentation effectively, IT administrators need visibility into application dependencies, including the ways that

applications communicate with each other and how traffic typically flows between them.

- **Define granular security policies.** Once dependencies and traffic flow between applications is clear, administrators can set granular policy controls that permit legitimate network traffic while blocking or flagging anomalous and suspicious activity. Policies can be customized for each workload or type of workload. An example of this would be setting stricter guidelines to access business-critical workloads while allowing broader access to less important assets.

- **Continuously monitor the environment.** Administrators must keep a close eye on the restrictiveness of policies to make sure there are no impediments for legitimate traffic, and on the security of the network, identifying and investigating any anomalous or suspicious activity.

Where is software-defined microsegmentation applied?

IT administrators can use software-defined microsegmentation to protect workloads in both on-premises data centers and cloud environments. Leading microsegmentation solutions should provide the same visibility and policy controls provisioned in on-premises environments to those in the cloud, and those capabilities should also be able to be extended to legacy machines, devices, and containerized workloads.

How does software-defined microsegmentation improve network security?

Microsegmentation improves an organization's security posture by addressing two areas of concern for security teams.

- **Lateral movement.** A network protected by microsegmentation may have dozens of separate, secure zones. When attackers exploit a vulnerability to access one part of the network, microsegmentation prevents them from easily moving laterally to other parts of the network as they attempt to access workloads, escalate privileges, and steal valuable or sensitive data. At the same time, any unauthorized attempts to move laterally will create incident alerts that can help a security team quickly mitigate the attack.

- **Insider threats.** In a microsegmented data center, a user who has access to one part of the network cannot access other assets without receiving explicit authorization. This

reduces the risk of privilege escalation and insider threats in which users knowingly or inadvertently compromise confidential data.

What is software-defined microsegmentation vs. Zero Trust security?

Zero Trust is an approach to network security that works in concert with software-defined microsegmentation to protect networks and IT assets more effectively. Zero Trust assumes that nothing inside or outside the network can be inherently trusted. This means that every user, device, and application must be authenticated and validated before being permitted to access IT assets or workloads. Permissions are granted with the principle of least privilege, only granting access to the systems and data that are needed to perform a task in a given moment.

What are the benefits of microsegmentation?

- **Reduced attack surface.** Narrowly defining security controls around individual workloads and IT assets significantly minimizes the potential attack surface across different workload types and environments.

- **Limited blast radius.** When workloads and assets are protected with microsegmentation, a breach in one part of a network cannot spread easily to other assets or network segments. This neutralizes a class of cyberattacks that seek to gain access to one part of an IT environment before moving laterally throughout the network to compromise additional assets and launch further attacks. With microsegmentation, security teams can also uncover and remediate attacks more quickly by receiving incident alerts of any suspicious attempts to access protected workloads and assets.

- **Improved regulatory compliance efforts.** Microsegmentation allows security and network teams to comply more easily with ever-evolving regulatory requirements. The granular visibility and control provided by leading microsegmentation solutions make it easy to establish levels of protection for individual assets, and to document proper data separation and compliance efforts related to protecting sensitive information and preventing a data breach.

- **Protection for hybrid environments.** Microsegmentation can secure workloads across dynamic environments and hybrid networks, protecting assets on-premises, in the cloud, and in different network configurations.

- **Cost savings.** The expense and effort of implementing a software-defined microsegmentation solution is far less than attempting to protect a network by

provisioning, configuring, maintaining, and updating multiple firewalls and VLANs.

- **Similar security management.** Adopting a leading software-defined microsegmentation solution will enable administrators to manage network security more easily, setting microsegmentation policies for all assets and environments from a single pane of glass.

FAQs

What does software-defined mean?

What is a workload?

What is a container?

What is a serverless framework?

Why customers choose Akamai

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence.

Related Products

Akamai Guardicore Segmentation

Visualize, protect, and segment on-premises, cloud, and hybrid environments.

Learn more ›

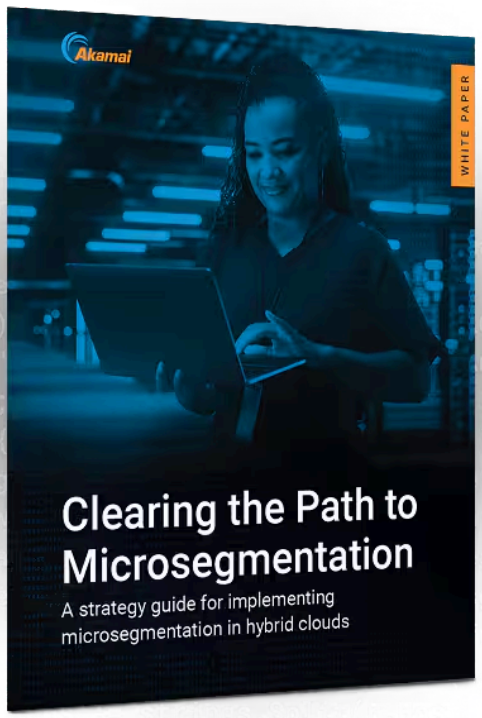
Zero Trust Security

Comprehensive cybersecurity coverage combined with deep visibility and granular control.

Learn more ›

Additional Resources

Clearing the Path to Microsegmentation: A strategy guide



White paper with a suggested strategy for implementing microsegmentation in hybrid clouds.

Learn more ›

Software-Based Segmentation: An inside-out approach to achieving security confidence

Learn why software-based segmentation offers better cyber defenses than legacy firewalls and how it can help you achieve Zero Trust security.

Learn more ›

Related Pages

Learn more about related topics and technologies on the pages listed below.

What Is Microsegmentation? ›

What Is Application Control? ›

What Is Lateral Movement? ›

What Is Network Segmentation? ›

What Is a Segmented Network? ›

What Is Software-defined Segmentation? ›

Take me there

PRODUCTS

Cloud Computing

Security

Content Delivery

All Products and Trials

Global Services

COMPANY

About Us

History

Leadership

Facts and Figures

Awards

Board of Directors

Investor Relations

Corporate Responsibility

Ethics

Locations

Vulnerability Reporting

CAREERS

Careers

Working at Akamai

Students and Recent Grads

Workplace Diversity

Search Jobs

Culture Blog

NEWSROOM

Newsroom

Press Releases

In the News

Media Resources

LEGAL & COMPLIANCE

Legal

Information Security Compliance

Privacy Trust Center

Cookie Settings

EU Digital Services Act (DSA)

GLOSSARY

What Is API Security?

What Is a CDN?

What Is Cloud Computing?

What Is Cybersecurity?

What Is a DDoS attack?

What Is Microsegmentation?

What Is WAAP?

What Is Zero Trust?

See all