AKAMAI SOLUTION BRIEF

Akamai Guardicore Segmentation for Endpoint Protection

When considering microsegmentation, most security teams think of protecting the assets that reside squarely within the corporate network, such as critical applications and servers. However, microsegmentation should also extend well beyond data centers and workloads to include endpoint devices. Endpoints are often the initial point of infection, and though XDR and NGAV are designed to detect threats on end-user devices, they are often bypassed by the likes of phishing, social engineering, and other tactics. Applying microsegmentation to endpoints is an effective way to prevent both the initial infection from the internet as well as lateral movement to other parts of the network.

From small annoyance to big problem

Cyberthreats continue to become more intrusive and more debilitating than in the past, and while their target is usually in the data center, their initial point of infection is typically an end-user device where they can capitalize on human error. A holistic security strategy to protect against these kinds of threats, including ransomware, requires multiple layers of protection and should be guided by a comprehensive framework such as Zero Trust. What is inevitable, however, is the appearance and exploitation of gaps in any security strategy.

One commonly exploited gap is the use of phishing or brute-forcing a built-in service such as RDP to gain access to a single endpoint, and then moving laterally to infect as many endpoints as possible until finding a machine with high-level or admin privileges. Although an initial infection can be remediated with minor impact, it must be done before lateral movement can occur. If screenshot capturing, information stealing, and encryption begins, what could have been a small containable breach becomes a veritable nightmare for security professionals and their organizations.

Fill in the gaps

Though machine learning and other new technologies have enabled significant progress to be made in anti-malware and EDR or XDR solutions, breaches continue to occur. Endpoint security solutions simply cannot catch all malware, and even when they do alert to malware, the time gap between infection and detection gives threat actors a chance to scan for open ports and hijack built-in OS services to hop from machine to machine, looking for the best way to access sensitive business-critical assets.

To ensure the best position for combating security threats today, it's important to adopt a post-breach mindset, starting with the assumption that not all infections will be detected and blocked. Therefore, security teams should make sure that these inevitable infections cannot make it past the first compromised endpoint. XDR or NGAV can provide helpful telemetry and should detect most breaches, but the best way to supplement these detection-centric tools and contain the potential blast radius is to microsegment your endpoints.

Benefits

Enable Zero Trust
Microsegmentation is required for achieving Zero Trust

Extend your coverage
Windows and Mac laptops and devices are supported

Prevent initial infections
Protect your endpoints without having to rely on detection

Reduce reaction time
Block suspicious lateral communication in one click

In a 2021 study conducted by Vanson Bourne and commissioned by Guardicore, 92% of security professionals surveyed attested that comprehensive segmentation has prevented cyberattacks on their organization from doing significant damage or stealing substantial amounts of data. But only 2% are extending segmentation beyond the network to protect all their critical assets — including endpoints. This wide gulf shows just how few security teams are leveraging techniques like segmentation to protect all their assets, leaving gaps in their security strategies that potential attackers are counting on to gain network access.

Securing endpoints with Akamai Guardicore Segmentation

Akamai Guardicore Segmentation, formerly Guardicore Centra, provides one single platform to monitor and control communications between endpoints and network assets, supporting Linux, Windows, and now Mac machines. Our agent-based approach enables you to gain visibility into connections down to individual processes and services, and our own driver allows for enforcement of granular security policies that limit communications, regardless of the underlying OS.

In one instance, a customer installed our agents on their endpoints and built policies that prevented unnecessary communications between those endpoints. Though this kind of lateral movement protection is the point of microsegmentation, we've historically seen it applied to assets within the data center, not to the endpoints. In this specific case, because our customer microsegmented their endpoints and not just their servers and apps, they were able to prevent the initial lateral move caused by malware, breaking the kill chain at its first link.

Having learned that the threat actors were using RDP brute-force techniques to infect laptops accessing the internet, the customer added a new policy that blocked inbound RDP from the internet to all end-user devices. In just a few clicks, they created and enforced a new segmentation policy that would stop future attackers from being able to infect machines with this technique in the first place. During postmortem analysis, the security team quickly realized that all indicators pointed to a major and well-known ransomware threat actor. If the campaign had been successful, the attackers would likely have attempted to proceed with their usual tactics, encrypting anything in reach before issuing a ransom note. This would have come with significant added disruption and downtime if business-critical assets, such as the ERP system, had been compromised.

As threats become more advanced, new security strategies are needed to combat these threats. While XDR and NGAV aren't going away any time soon, leveraging microsegmentation to protect your endpoints as well as your data center assets is the best way to limit the blast radius of an inevitable breach. Akamai Guardicore Segmentation can ensure that unauthorized or unnecessary lateral movement among endpoints is rendered impossible. By leveraging microsegmentation to supplement existing endpoint security, disruptive and costly security events can more easily be avoided; when used as part of a holistic security suite, it enables you to make the next big step on your journey to a state of Zero Trust.

> “
>
> Akamai Guardicore Segmentation limits the spread of attacks that could disrupt our business.
>
> **CISO**
>
> leading life insurance company

For more information on securing your endpoints with microsegmentation, preventing ransomware, and moving toward Zero Trust, visit akamai.com or contact your Akamai sales team.