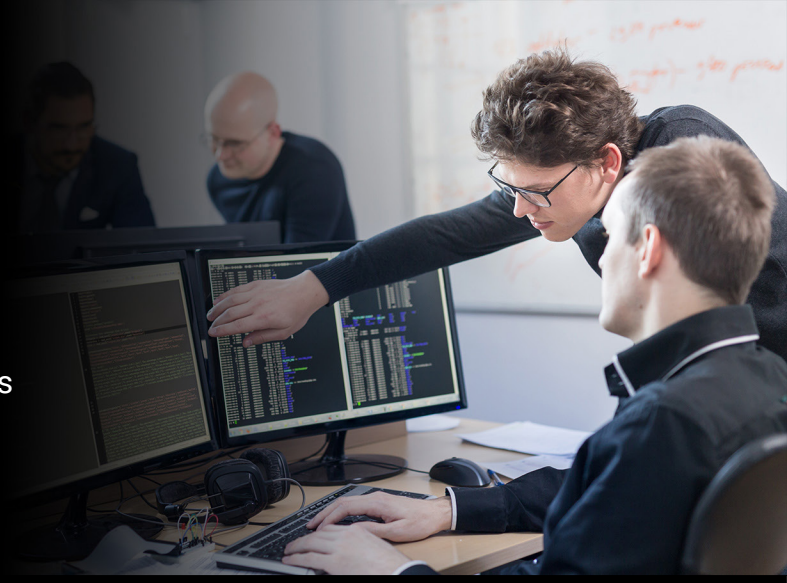
AKAMAI CUSTOMER STORY

At Summit Hosting, Security Comes First

Managed hosting provider stops malware in its tracks with Akamai Guardicore Segmentation



8,000
Virtual machines protected

5x
Faster implementation than other solutions

Stops spread of attacks

Keeping critical financial data safe

Managed cloud provider Summit Hosting has a passion for security that doesn't stop at the edge of the network. If malware makes its way onto servers, Summit wants to find out right away in order to wall it off from other servers. Summit found its solution in Akamai Guardicore Segmentation, which has successfully detected and averted ransomware and other malware attacks to keep its customers' financial data safe and secure.

Shielding customers from threats

Shannon Kaiser, Chief Technology Officer at Summit Hosting, experienced the misery of ransomware firsthand prior to joining Summit. One of his previous employers was hit by an attack that froze its hosts and most backups. "The loss of goodwill led to 30% customer attrition in the first month," Kaiser says. The burden of remediating two more ransomware attacks at subsequent employers has made him a true believer in multilayered security — the belt-and-suspenders approach.

"My experiences have shown that you can't count on a secure perimeter to keep out all of the bad guys," Kaiser says. "Realistically, some attacks will make it past even the best defenses, and once they're in the network it's crucial to limit their spread."

A security-first approach

Summit Hosting runs its customers' accounting software on dedicated, secure servers in the cloud. When it came time to update the IT platform, Kaiser focused on security before anything else. "Many hosting companies build their hosting infrastructure first and then add security, using freeware if they can," Kaiser says. "At Summit, we flipped that approach, building a secure environment first and then adding hosting services on top."

SUMMIT HOSTING
MANAGED CLOUD SOLUTIONS

Summit Hosting
Alpharetta, Georgia
www.summithosting.com

Industry
IT service provider

Solution
- Akamai Guardicore Segmentation

Akamai

Kaiser had in mind a modern, multilayered security architecture with three "crown jewels": a Zero Trust perimeter, endpoint security, and a segmentation solution to limit the reach of attacks.

"Segmentation prevents malware that makes it onto one server from spreading to others, which can be the most damaging type of attack," says Shane Barnard, Summit's Senior Network Engineer.

After evaluating several segmentation solutions, Kaiser and Barnard selected Akamai Guardicore Segmentation. "Akamai Guardicore Segmentation blew away all the other solutions we looked at because it's easy to implement at scale and gives us deep visibility into what's happening on our network," Barnard says. "The ability to search for any user to see where they've been and what they're doing right now is extremely valuable for ransomware defense."

Fast implementation on existing virtual servers

Getting Akamai Guardicore Segmentation up and running was as simple as installing the software agent on virtual servers and writing rules about which servers were allowed to communicate with one another. "Working with Akamai's team, we implemented Akamai Guardicore Segmentation on 8,000 Microsoft Hyper-V virtual servers in three data centers in just six months, about two years faster than we could have done it with any other solution I've seen," Barnard says. "Other solutions would have required a complete overhaul of our virtual servers, including rebuilding some of them from scratch."

To create rules that control communications between servers, Barnard first used Akamai Guardicore Segmentation to create a map of normal traffic flows — for instance, among a single customer's servers. Then, referring to the map, Barnard needed only a few days to write a small set of rules to allow legitimate server-to-server traffic. "Akamai Guardicore Segmentation blocks all file sharing that we don't explicitly allow, which saved months spent writing thousands of rules," Barnard says.

Visibility into all network activity and who's doing it

Now Summit Hosting can immediately spot unusual traffic patterns in any data center, a telltale sign of ransomware. "The most shocking part of the ransomware attacks I've seen was realizing that the bad actors had been poking around inside the networks for several weeks before they attacked," Kaiser says. "Our existing tools alerted us when attackers were trying to get onto the network, but not when they were already in. Akamai Guardicore Segmentation fills that gap."

Barnard likes that the solution shows how ransomware got onto the network, helping him continually strengthen defenses. "We can quickly see what's happening on the network, who is doing it, where they are, what they're targeting, how long they've been at it, and what else they're doing," he says.

With the newfound visibility, Summit plans to expand to verticals with stringent compliance requirements like the Healthcare Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA). The visibility also helps the IT team prepare for acquisitions. "Before integrating acquired environments, we install the Akamai Guardicore Segmentation agent on a few of the company's servers, which gives us a deeper understanding of their network than we can typically get from their engineers," Barnard says.

> Our existing tools alerted us when attackers were trying to get onto the network, but not when they were already in. Akamai Guardicore Segmentation fills that gap.
>
> **Shannon Kaiser**
> Chief Technology Officer,
> Summit Hosting

Peace of mind for customers and the IT team

Companies considering Summit's hosting services ask more questions about security than they did even a few years ago. "They're smart to care, given that the average cost of a ransomware attack to an individual company is now over $750,000, including loss of productivity and goodwill, brand damage, and fines for exposing personal information," Kaiser says. "By helping us detect attacks and limit their spread, Akamai Guardicore Segmentation has become a competitive advantage for Summit Hosting."

Quality of life for the IT team has also improved. "Remediating large-scale breaches is enormously time-consuming, and Akamai has already saved us from that stress many times over," Kaiser says. "We wouldn't have this peace of mind with any other vendor. Since implementing Akamai Guardicore Segmentation, I've had 180 consecutive full nights of sleep. You can't put a price on that."

> Akamai Guardicore Segmentation blew away all the other solutions we looked at because it's easy to implement at scale and gives us deep visibility into what's happening inside our network. The ability to search for any user to see where they've been and what they're doing now is extremely valuable for ransomware defense.
>
> **Shane Barnard**
> Senior Network Engineer,
> Summit Hosting

SUMMIT HOSTING
MANAGED CLOUD SOLUTIONS

With more than 30,000 customers in the U.S. and Canada, Summit Hosting is one of the largest providers of cloud-based hosting for QuickBooks, SAP Business One, Sage, and other accounting software. The company hosts these mission-critical applications and software on secure dedicated servers that customers can access from anywhere, on any device. Summit also provides a multi-lingual 24/7 server support team and a top-tier security suite with every server. Its services are designed to make customers' lives easier, save them time, and minimize their IT and hardware costs. https://www.summithosting.com/.