AKAMAI SOLUTION BRIEF

Deloitte Bolsters Incident Response and Ransomware Mitigation Offerings by Leveraging Akamai Guardicore Segmentation

Client challenges

Firmly established security product categories promise increasing levels of protection against the latest threats to enterprise networks. However, few solutions have been able to offer a comprehensive, single-solution method of reducing the attack surface by securing against malicious lateral movement — whether that movement is to or from on-prem hardware, workloads hosted in the cloud, end-user devices, or containers. Furthermore, initial Zero Trust segmentation initiatives have historically taken months, if not years, for enterprise clients to complete, due to the technological constraints and limited human expertise to execute projects that aim to stop attacks if they bypass established security products like legacy firewalls, EDRs, and more.

When approaching segmentation projects, enterprise clients typically face the following challenges:

- Lack of visibility into all assets, network flows, users, and connections across all environments
- Limited security controls over disparate technologies and infrastructure, such as hybrid cloud infrastructure, legacy operating systems, and OT/IoT
- The need to ensure business continuity by avoiding downtime that often comes hand in hand with traditional segmentation techniques
- Shortage of security resources and talent to build, deploy, and manage initiatives that support Zero Trust

Solution highlights

Akamai Guardicore Segmentation is a host-based microsegmentation solution that provides the simplest, fastest, and most intuitive way to enforce Zero Trust principles in the network. Using a mix of agent-based sensors, network-based data collectors, and virtual private cloud flow logs to map your network, Akamai Guardicore Segmentation is designed to deliver a single visual of all of your assets and infrastructure — including legacy and modern operating systems, operational technology, and IoT devices. From there, you can easily create and enforce policies that will limit unwanted communications, reducing your attack surface and ensuring business continuity.

Leading use cases

- **East-west traffic controls**
  Separate environments, applications, users, and infrastructure that do not need to communicate
- **Ransomware mitigation**
  Deploy policy templates with AI/ML to block attack paths known to be used by various types of ransomware attacks
- **Application ringfencing**
  Focus on the specific dependencies of your business-critical applications to create tight security controls

- **User-based segmentation**
  Block users from accessing applications, environments, and devices that are not essential to their work
- **Infected device isolation**
  Contain the spread of a breach if one or more devices are compromised
- **Compliance**
  Be ready to demonstrate compliance at a moment's notice with deep contextual understanding of your network, devices, and potential attack paths

Client benefits

- Solve visibility challenges with single-pane visibility into your entire network and connections, including servers, endpoints, clouds, containers, users, and more
- Enforce Zero Trust policies to mitigate the possibility of a successful ransomware attack
- Reduce incident response time using threat intelligence and comprehensive breach detection and deception capabilities
- Simplify network forensics and compliance projects using both real-time and historical features

Deloitte expertise

1. **Advisory**
   Deloitte's experience in impactful cybersecurity decision support, security gap analysis, and implementation roadmap creation ensure that enterprise clients are making sound decisions during breaches and when planning for the future
2. **Professional services**
   Experience fully managed implementation services as well as customized integrations into your existing security, ITSM, and cloud solutions
3. **Incident response managed services**
   Receive instant white-glove assistance from Deloitte's incident response tacticians to contain the breach and help prevent future incidents
4. **License subscriptions**
   Deloitte can offer a wide range of license subscriptions to be purchased

Customer case study — How Akamai and Deloitte Solve Client Ransomware Challenges

Major ransomware events have caused clients to seek consultation and solutions that can help immediately at a critical time. The combined capabilities of Deloitte's incident response and security teams — leveraging the network visibility, breach forensics, and subsequent measures for significant attack surface reduction provided by Akamai Guardicore Segmentation — have produced a winning combo for these clients in need.

Background

In the case of one enterprise organization, the customer was experiencing a significant ransomware event that took down their core business operations, and did not know how to begin addressing it. Their entire data center, consisting of thousands of servers, had been taken over, and the breach needed to be contained immediately in a safe manner. Trusting in the guidance of Deloitte, the client called and asked what to do next. With the Deloitte team already prepared to offer and deploy Akamai Guardicore Segmentation, the client was able to quickly gain visibility into the scale of the attack, understand which assets and applications had been affected, and see what all the related application dependencies were.

Solution

By mapping the client's entire environment down to the individual process level, Akamai Guardicore Segmentation was able to reveal all the potential routes the malware may have taken from the infrastructure that was compromised, allowing the Deloitte team to focus on specific parts of the network for additional forensic analysis. This ensured that once the client had restored business operations and access to their data center, there would not be any remaining compromised devices.

Outcome

With the ransomware attack resolved, the data center back online, and business operations resumed, measures were taken to reduce the chance of such an attack happening again. Like many enterprise clients, this client uses a layered security approach with multiple leading solutions in place to protect devices, applications, users, and more. However, because something as simple as a phishing email can be the gateway for an attacker, these solutions were not enough to stop the attack. With full visibility into the network, application dependencies, and the users that have access to the data center, the client was able to implement precise microsegmentation controls to greatly reduce the routes that a future ransomware breach could take.

Once the client was able to experience the value of the solution and their trust of Deloitte's expertise was reinforced, they decided to keep the solution in place to continue providing Zero Trust segmentation, and requested that Deloitte manage the technology for them on a day-to-day basis.

In summary

Deloitte's deep technical expertise and experience executing Zero Trust projects for clients makes them an ideal partner for deploying and managing Akamai Guardicore Segmentation for clients. Clients can depend on Deloitte to use this technology for any security initiative that includes attack surface reduction, lateral movement controls, application ringfencing, or ransomware mitigation.

About Deloitte

Deloitte provides industry-leading audit, consulting, tax, and advisory services to many of the world's most admired brands, including nearly 90% of the Fortune 500® and more than 7,000 private companies. Our people come together for the greater good and work across the industry sectors that drive and shape today's marketplace — delivering measurable and lasting results that help reinforce public trust in our capital markets, inspire clients to see challenges as opportunities to transform and thrive, and help lead the way toward a stronger economy and a healthier society. Deloitte is proud to be part of the largest global professional services network serving our clients in the markets that are most important to them. Building on more than 175 years of service, our network of member firms spans more than 150 countries and territories. Learn how Deloitte's approximately 415,000 people worldwide connect for impact at deloitte.com.

Contact

Ola Sergatchov
Head of Global Strategic Alliances, Akamai
osergatc@akamai.com