Akamai

WHITE PAPER

Protect Your Business Against Advanced Attacks

As IT environments have grown in complexity, cyberattacks have evolved to take advantage of new points of fault. Applications, APIs, microservices, and components are constantly expanding and changing how you do business online. Unfortunately, those also create new vulnerabilities and threat surfaces for attackers to exploit. Cybersecurity solutions must address both the threats that exist on the inside (securing your own data) and the outside (blocking ransomware, DDoS, resource exhaustion, and other attacks).

We know this firsthand because Akamai researchers analyze, on average, 788 TB of data daily, and we continually innovate our products with the knowledge gained, protecting you and your users against the most dangerous attackers and advanced campaigns, even as attacks evolve.

What are the most dangerous attacks your company might face, and how can you be prepared for them?

Ransomware is on the rise

Loss of access to your — and your customers' — data is one of the biggest threats to your business. Between the first quarter of 2022 and the first quarter of 2023, the number of ransomware attacks increased 143% worldwide, with attackers taking advantage of zero-day and one-day vulnerabilities, according to Akamai's Ransomware on the Move report. You can decrease the likelihood and impact of advanced attacks through segmentation.

Whereas segmentation is an architectural approach that divides a network into smaller segments for the purposes of enhancing performance and security, microsegmentation is a security technique that enables you to logically divide a network into distinct security segments down to the individual workload level. Security controls and service delivery can then be defined for each unique segment.

Akamai Guardicore Segmentation, part of the Akamai Guardicore Platform for Zero Trust, acts to contain attacks on all your critical systems, preventing them from spreading across your assets — what's known as east-west travel — and then powering response and recovery. The result is protection against the reputational damage, loss of data, and loss of revenue that come with a successful breach.

Because it's an agentless solution for microsegmentation, the Akamai Guardicore Platform can be deployed quickly and easily, without having to make physical changes to your network or worrying about where your servers and devices are. It generates an interactive visual of all the connections in your network, helping you overcome one of the primary obstacles to deployment — a lack of visibility. In addition, Akamai has built active ways to address potential performance bottlenecks and compliance requirements, plus policy enforcement that can cover many different kinds of infrastructures. That means broad visibility and granular control, across environments, all in a single platform.

Akamai has unmatched visibility into online traffic across our massively distributed global network. The Akamai Guardicore Platform leverages that to provide deep visibility into your own environment, assets, access, and network flows. That's real-time information that will give you confidence that your business won't be disrupted.

Apps and APIs under assault

How many applications is your company using? It is almost certainly more than you're aware of. The average company uses more than 1,000 apps. The heavy reliance upon APIs for nearly all online transactions and the increasing adoption of microservices-based architectures also means apps are becoming more complex. Unfortunately, the pressure to grow fast through innovation often leads companies to release apps before they've been rigorously tested for potential security issues, introducing more risk to the entire application ecosystem.

Akamai's recent State of the Internet report found that 29% of global attacks targeted application programming interfaces (APIs), which are at the heart of most digital transformations. In the Europe, Middle East, and Africa region, the share was just over 47%. APIs are a common attack vector for cybercriminals using both traditional and API-specific techniques. Bots, distributed denial-of-service (DDoS) attacks, and multi-vector attacks must all be accounted for.

Protecting your web applications with Akamai App & API Protector will safeguard your workflow, your users, and your business from malicious activity and fraud. It provides configurable firewall protections that can absorb attacks aimed at the application layer, including those launched via APIs. With real-time visibility into bot traffic, you can investigate skewed web analytics, prevent origin overload, and customize permissions to allow access to third-party and partner bots without obstruction.

But, going back to the original question, what if you don't know all of your apps and APIs? Visibility is, again, the key — Akamai API Security will identify all of your APIs, assess their risk levels, and respond to attacks. This prevents attackers from accessing your data, loading malicious files onto servers, or overwhelming servers with bursts of traffic.

Did you know?

DDoS attacks increased by 50% between 2021 and 2023

More than 60% of the total DDoS attacks in 2023 had a DNS component

Defend against DDoS and resource exhaustion

If there is an elephant in the digital room, it's the distributed denial-of-service attack. As long as there's been an internet, there have been DDoS attacks — and their impact has scaled with everything else online. In recent years, DDoS attacks have grown larger in size, longer in duration, and highly sophisticated with multiple attack vectors and destinations. The number of highly volumetric DDoS attacks increased by 50% between 2021 and 2023. And more than 60% of the total DDoS attacks in 2023 had a DNS component.

Even the biggest companies can be taken down by these hostile botnets, disrupting service to millions of customers and bringing business to a crashing halt. Highly resourced cybercriminals, nation-state actors, and geopolitically motivated hacktivists leverage large and distributed botnets to not only take down the largest of companies, but also critical public institutions ranging from schools and hospitals to airports and utility providers. Devastating DDoS and resource exhaustion attacks are aimed at all layers, ports, protocols, and even the DNS of businesses and institutions.

Protecting your infrastructure from DDoS attacks requires real-time threat intelligence. The data we gather is used to fuel Prolexic, our DDoS attack protection and mitigation solution. Capable of protecting the underlying digital infrastructure that powers a company's digital applications and experiences, it stops attacks across all your ports and protocols — in the cloud, on-premises, or both — before they impact your business.

In recent years, there has been a significant resurgence in resource exhaustion attacks aimed at a business's DNS infrastructure. DNS is the foundational element of a company's online presence. If the DNS system goes down, the organization's online presence disappears. Akamai Edge DNS and Shield NS53 drop DNS resource exhaustion traffic at the edge and allow only legitimate DNS queries to reach a customer's origin.

DDoS protection has long been table stakes for online businesses, with the size of attacks doubling every two years and a concomitant increase in complexity. Securing all potential points of failure against them is necessary to keep from losing revenue and the trust of customers.

What happens when there's an attack?

It's safe to assume that if you have a digital presence, it's going to be targeted by an attack at some point. One purpose of a security strategy is to protect you before the attack — make you less of a target by protecting critical assets, providing visibility across your network so you can see what is happening, and detecting the attacks when they start.

But what if something happens like a zero-day attack? That's where the behavioral analysis that's central to solutions like Akamai App & API Protector comes in.

Akamai combines highly automated solutions and machine intelligence along with human intelligence from more than 225 frontline responders across our global Security Operations Command Center (SOCC) to defend customers' data, infrastructure, and their end users' digital experiences.

Akamai reviews more than 13 trillion Domain Name System (DNS) queries daily and defends more than 12 billion web application firewall (WAF) attacks each quarter. We see it all and we've experienced it through our customers, and translate our attack analysis into strength. Akamai uses that threat intelligence to make our solutions more responsive and more effective.

Even if you aren't using Akamai's security solutions yet, if you are under attack, you can contact us through our cyberthreat hotline. A security expert will call you with the next steps for mitigating current attacks.

Security everywhere your business meets the world

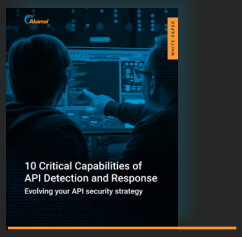
Like death and taxes, cyberattacks are one of the certainties of this world. But you can protect your organization and your customers with security solutions that use up-to-date threat intelligence, provide high visibility into your apps and networks, and evolve with the threat landscape.

Akamai protects your customer experience, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Leveraging the threat visibility of our global platform, our broad solution portfolio delivers industry-leading reliability, so you can stay ahead of threats and adapt quickly to the changing security landscape.

More resources

Learn the five steps you need to take to break the ransomware kill chain

Support your hybrid cloud strategy while defending from DDoS attacks



Defend the building blocks of your business with strong API security

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 06/24.