ENTERPRISE DEFENDER

Zero Trust Security at the Edge

The defensible network perimeter no longer exists. At least not in any recognizable form. Utilizing a security and access approach that made sense 20 years ago in today's environment is at best misaligned and at worst perilous. And this isn't just theory. This is evident in the number and scale of data breaches we've seen in the past five years, the vast majority of which happened as a result of trust being abused inside of the perimeter. It's time to adopt Zero Trust security, where trust in the corporate network is no longer inherent, and security and access decisions are dynamically enforced based on identity, device, and user context.

ENTERPRISE DEFENDER

Built on the Akamai Intelligent Edge Platform, Enterprise Defender combines malware prevention with adaptive application access, security, and acceleration in a simple-to-consume security service at the Edge. Enterprise Defender enables organizations to move toward a Zero Trust security posture without hardware or appliances. Simply subscribe to Enterprise Defender to reduce risk and complexity while improving user experience.

HOW IT WORKS

Enterprise Defender leverages the Akamai Intelligent Edge Platform to secure all enterprise applications and users, delivering optimal security and reducing complexity while improving performance. It enables you to ensure secure access to applications you control, while mitigating risks associated with your users accessing applications you don't control on the Internet.

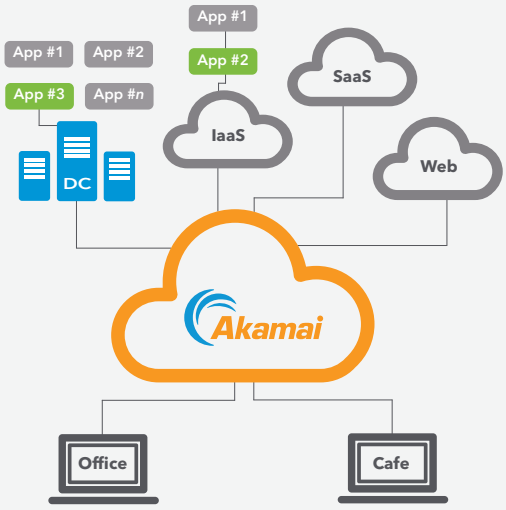
Enterprise Defender includes the following capabilities in an easy-to-consume per-user, per-month subscription service:

Malware Prevention: Akamai proactively identifies, blocks, and mitigates targeted threats such as malware, ransomware, phishing, DNS data exfiltration, and advanced zero-day attacks. Akamai offers a Secure Internet Gateway (SIG) that enables security teams to ensure that users and devices can safely connect to applications you don't control on the Internet, regardless of where users are connecting from, without the complexity associated with legacy approaches.

Zero Trust Access: Akamai ensures that only authorized users and devices have access to the internal applications they need, and not the entire corporate network. All access decisions are dynamically enforced based on identity, device, and user context. No one can access applications directly because they are hidden from the Internet and public exposure. Enterprise Defender integrates data path protection, single sign-on, identity, application access, and management visibility and control into a single service.

Web Application Firewall (WAF): Akamai provides broad protection for critical web applications against the largest and most sophisticated DDoS and web application attacks. Our WAF includes robust security protections for websites, updated by the industry's best threat research team, to help organizations keep up with ever-evolving security threats.

Application Acceleration: Akamai enables enterprises to deliver applications that are fast, reliable, and secure in a cost-effective manner. This empowers enterprises to overcome the challenges related to delivering business applications over the Internet by placing application delivery capabilities within the Akamai Intelligent Edge Platform very close to users, the cloud, and on-premises workloads – anywhere in the world.



- Application access, acceleration, and security controls at the edge
- Keep users off of the corporate network
- Single sign-on and multi-factor authentication for enterprise applications
- Block access to malicious domains, URLs, and content – everywhere

ENTERPRISE DEFENDER

BUSINESS BENEFITS

- **Stop malware propagation and lateral movement**
  In traditional perimeter-based networks, malware typically penetrates deeply due to a lack of segmentation and poor network visibility. With Enterprise Defender, the combination of more granular access controls for specific applications combined with proactive threat prevention makes it much harder for malware to propagate or for an attacker to gain access to other workloads.

- **Reduce complexity and streamline operations**
  Cloud-based security such as Enterprise Defender enables teams to replace costly-to-manage and -maintain virtual or hardware appliances with a simple security service at the Edge.

- **Reduce both CapEx and OpEx for security**
  Improving security is invariably associated with increased cost. With Enterprise Defender, this is typically not the case; to the contrary, improved security combined with cloud-based simplicity enables CISOs and security teams to consolidate multiple, disparate security controls and reduce management costs.

- **Increase visibility and reduce time-to-breach detection**
  Quotes associated with breaches often include "malicious actors were undetected for *n* number of months" and "once past the perimeter, malicious actors were able to move around the network unfettered." With Enterprise Defender, the combination of more granular application access logging combined with DNS-based security controls provides more visibility and accelerates breach detection.

- **Stop exfiltration of internal data**
  Allowing data to get into the hands of malicious actors can have serious business consequences, whether it's fines for not taking sufficient care of personal data, or loss of revenue caused by the theft of intellectual property or strategic plans. With Enterprise Defender, stop exfiltration of internal data with "least privilege"–based adaptive access controls and DNS-based visibility and security.

- **Enable digital business transformation**
  The IT and security team can become a partner in digital transformation. With perimeter-based security, teams earned a reputation as paranoid custodians; once they allowed access into the corporate perimeter in support of a new cloud service, partner, or customer model, they were opening a door or connection to the entire corporate network. With Enterprise Defender, this is not the case as access is only granted to a limited number of applications, based on identity and security context, without ever granting access to the full network. In addition, enable a modern, "work anywhere" corporate culture by blocking access to malicious domains, URLs, and content – whether your users are in the office or a local coffee shop.

AVAILABLE EDITIONS

	Standard	Premier
Malware Prevention	√	√
Zero Trust Access	√	√
Web Application Firewall		√
Application Acceleration		√