Protect againts online attacks yes

Optus Business and Akamai® Technologies Inc. are working together to help customers avoid data theft and downtime by extending the security perimeter to the edge of the network – to protect the web and data centre from attacks without loss of performance.

Highlights

The Akamai Intelligent Platform™ is monitoring Web conditions to help:

- Identify, absorb, and block security threats
- Make decisions based on comprehensive knowledge of network conditions
- Present business and technical insights

Distributed Denial of Service (DDoS) attacks are committed by cyber criminals who stealthily command unrelated PCs and servers, often in different geographical locations, to exhaust an enterprise's bandwidth or compute resources in order to overwhelm it. This can overload the enterprise's servers, networks, info-communications platforms and applications, and severely disrupts normal operations and causes financial losses.

Enterprises today deploy mission critical applications such as enterprise resource planning, e-commerce, cloud-based applications and Unified Communications across wide area networks and the internet. While these applications can help enterprises to be more productive, agile and cost efficient, they can also render enterprises more vulnerable to cyber attacks such as DDoS.

The Akamai advanced cloud-based cyber security solution leverages the massive scale and capacity of the globally distributed Akamai Intelligent Platform™ to help mitigate DDoS threats closest to the point of attack and keep networks and websites up during DDoS attacks. Using this solution, Optus Business can pre-emptively scrutinise, detect and block DDoS threats before they reach the targeted web services.

The Akamai Intelligent Platform™ provides extensive reach, coupled with reliability, security, visibility and expertise. Made up of a distributed network of servers and intelligent software, delivering over two trillion interactions daily, the platform provides the ubiquity to scale reliably and to quickly adapt to changes.

Extend your security perimeter

The partnership with Akamai enhances Optus Business' capabilities further to deal with DDoS attacks and provide a better customer experience through faster content delivery.

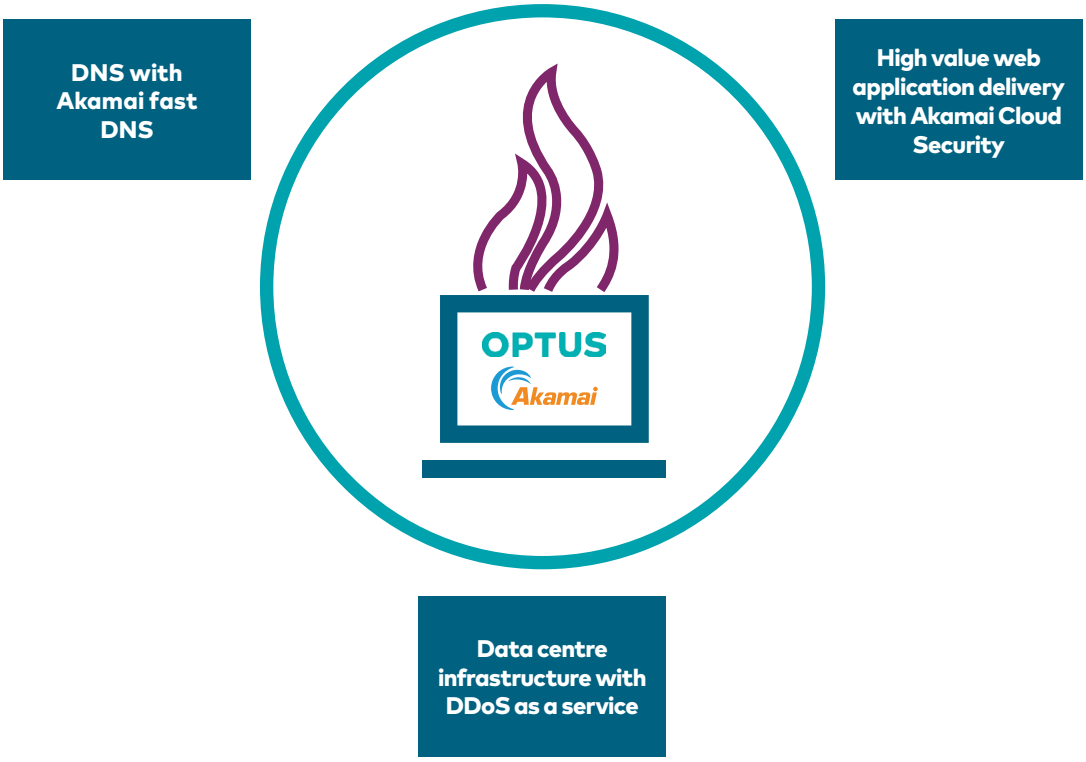
Our tiered DDoS Mitigation and Web Security framework powered by Akamai comprises the following service options:

Akamai Cloud Security – Cloud-based DDoS for mitigation of the largest attacks

Web Application Firewall (WAF) as a service – Web Application Firewall for application layer protection of your web assets

DDOS Mitigation as a service – Network clean-pipe solution for mitigating direct IP attacks and data centre protection

OPTUS | Akamai NETALLIANCE



Akamai cloud security

Multi-layered defence to protect websites against the increasing frequency, sophistication, and scale of attacks.

Akamai's Kona Site Defender is designed to improve your security posture and reduce the likelihood and impact of security events by mitigating attacks at the Akamai network edge. It includes configurable functionality designed to help protect your organisation by reducing the risk and impact of attacks at the network and application layers.

- Protect websites and web applications from DoS and DDoS attacks with the massive scale and capacity of Akamai's Intelligent Platform™
- Maintain website availability and performance during DDoS attacks through Akamai's globally-distributed architecture
- Reduce the risk of data breach with a highly scalable and high-performance web application firewall
- Reduce capital and operational costs associated with web security by leveraging Akamai's cloud security service
- Adapt to a changing threat landscape with security rules refined and updated by Akamai's Threat Intelligence Team

Kona Site Defender can thwart DDoS attacks by deflecting network-layer DDoS traffic and absorbing application-layer DDoS traffic at the network edge. Mitigation capabilities are implemented natively in-path to help protect against attacks in the cloud before they reach the customer origin.

Akamai's Managed Kona Site Defender Service is an optional Managed website security service for Kona Site Defender consisting of Management and Monitoring of the Akamai Kona Site Defender Service with support for DDoS and Application attacks.

With the Rules Update Service, organisations can also access one or more threat update review delivering a statistical analysis of your log files for WAF rules triggered.

The Fast DNS Service provides an outsourced primary and secondary DNS service via a distributed network of DNS servers deployed across multiple networks designed to improve DNS performance, security and scalability.

Web application firewall (WAF) as a service

Application-layer defence to protect against data theft through attacks like SQL injections and cross-site scripts.

Akamai's Kona Web Application Firewall provides always-on and highly-scalable protection against web application attacks including SQL injections, cross-site scripting, and remote file inclusion – while keeping application performance high. An embedded process within the Akamai Intelligent Platform, it inspects every HTTP and HTTPS request, helping to detect and block threats to web applications before they reach the data centre. Kona Web Application Firewall taps Akamai's cloud intelligence to refine web security rules for known website attacks and help to respond to new web security threats as they emerge.

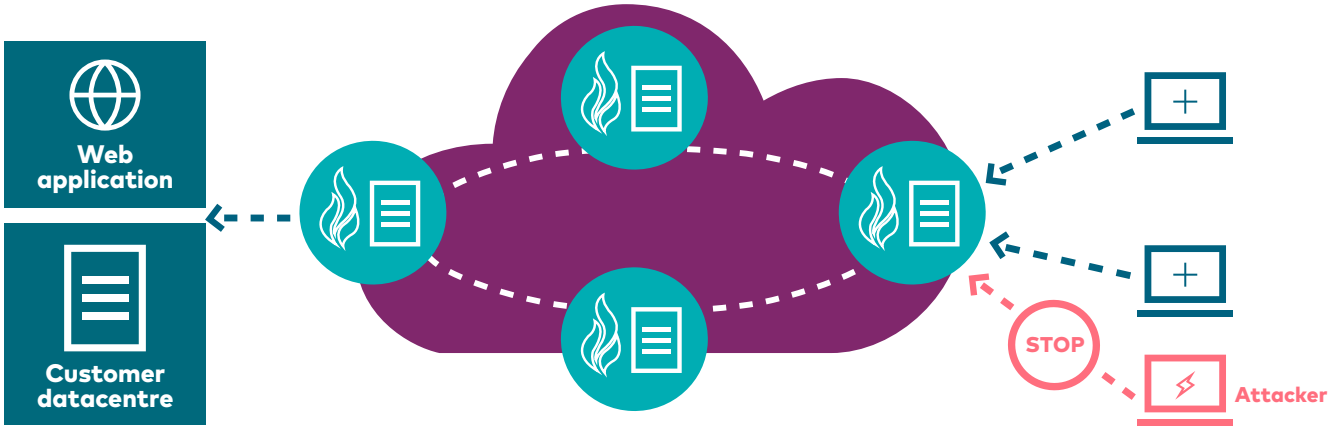
- Reduce the risk of data breach with a highly-scalable and globally-distributed web application firewall
- Innovate faster by protecting in front of the application with a cloud-based web security solution
- Simplify web security with pre-defined application-layer controls that are easily configurable
- Adapt to a changing threat landscape with security rules continuously refined and updated by Akamai's Threat Intelligence Team
- Reduce capital and operational costs associated with web security by leveraging Akamai's cloud security service

DDOS as a service

DDoS defence for protecting network and data centre infrastructures.

Prolexic, now part of Akamai, helps to defend data centres on all ports and protocols against complex DoS and DDoS attacks. Prolexic DDoS protection solutions leverage proprietary DDoS filtering techniques and Akamai's DDoS mitigation network, employing advanced DDoS protection routing and anti-DDoS devices to help protect your organisation from DoS and DDoS denial of service attacks.

But what does that really mean when your Internet-facing infrastructure is under DDoS attack? It means minimised financial loss for business – Prolexic can help protect your business from DDoS attacks quickly after traffic starts flowing through Prolexic's scrubbing centres.



Web and application security delivered via an intelligent platform with 170,000 servers in 102 countries

Minutes count, which is why Prolexic stands behind a time-to-mitigate service level agreement (SLA). Simply put, massive DDoS traffic flows that overwhelm others – even the largest multi-gigabit-per-second distributed denial of service (DDoS) attacks – usually end at Prolexic.

- Prolexic security engineers have extensive DDoS mitigation experience backed up by a large, global mitigation network to protect organisations from the biggest DDOS denial of service attacks
- Stops an extensive number of distributed denial of service (DDoS) attacks each year
- Classifies and identifies more than 100 different types of DDoS attacks and offers DDoS protection services capable of mitigating a large number of them – even new variants that may have just emerged
- Proprietary hardware protects your encryption keys and confidential information while providing a secure way for Prolexic to monitor and stop HTTPS attacks
- Security operations centre for DDoS protection monitors DDoS attacks 24/7/365, compiles anti-DDoS intelligence on thousands of botnets, and informs customers immediately when Prolexic detects a DDoS attack that could affect your network

A range of DDoS protection service levels and options are available to meet the needs of your business.

Prolexic Routed leverages the Border Gateway Protocol (BGP) to route all of an organisation's network traffic through Akamai's globally distributed scrubbing centres. Within each scrubbing centre, Akamai security operations centre staff then inspect the network traffic for potential DDoS attack vectors, drops detected attack traffic and forwards only clean traffic to the application origin.
Built on a global network with close to 4 Tbps of dedicated capacity today, Prolexic Routed protects some of the largest Internet-facing organisations from the largest known and most sophisticated DDoS attacks.

Better together: Optus business and Akamai

As a telecommunications provider, security is in Optus' DNA. We provide protection from the network through to your content and endpoints, including mobile devices. Partnering with Akamai and embedding their expertise and technology allows us to extend your security perimeter to deliver a more comprehensive defence for our customers against the latest security threats.

Optus can manage your security related incident and response management 24 x 7 and is able to provide you with visibility across your entire managed network system and components.

GMO_N 0396 0816MZ