LINK11

WEB DDOS PROTECTION

APPLICATION PROTECTION VIA DNS FORWARDING

A STRONG PARTNER

COMPANY

Link11 - longstanding security experience

Link11 is a European IT security provider, headquartered in Frankfurt, Germany with operations in Europe, the US and Asia. Established in 2005, Link11 has been pioneering DDoS protection since the early days of attacks. Its **Cloud Security Platform** is focused on security-related services like **a Content Delivery Network (CDN), DDoS protection, Web Application Firewall (WAF), secure DNS hosting** and more.

The company's DDoS protection, a part of Link11's Cloud Security Platform, is entirely built using proprietary, patent-pending technology. **This state-of-the-art DDoS protection service for web applications and IT infrastructures uses Artificial Intelligence (AI)** and enables Link11 to protect mission-critical web applications, APIs and IT infrastructures against all types of DDoS attacks. This allows customers to focus on their core business.

With more than 11 years of experience in internet security and a clear security focus, Link11 has developed one of the most sophisticated DDoS protection services available. **Link11 protects some of Europe's largest media, financial, e-commerce and online organizations.** The company has won numerous awards and continues to innovate to ensure that Link11's IT security services are always one step ahead of the game.

Link11's global network is built to ensure resilience, performance and maximum availability for its customers' IT infrastructure. In recent years, Link11 has strengthened its network to offer the best possible protection, and the firm plans to further expand into Asia and the Middle East in the near future.

Link11's Strategic Points of Presence

What is DDoS?

A DDoS attack against a web application, web service or an API aims to exhaust the target's resources to make them unavailable to legitimate service users/clients. **DDoS attacks have become more and more complex over the years.** Attack tools are available for download – today, anyone can get them for free. New attack types have occurred in recent years, and experts expect to see additional attack vectors in the near future. **Cyber-criminals usually launch multiple attacks against the same target.** They combine different floods in combination with high-volume attacks using subtle and sophisticated attack and infiltration techniques. All these hammer against a single application, service or API at the same time. **Traditional security components like firewalls, IDS/IPS and others are not designed to detect or prevent such kinds of attacks.** On top of that, they are usually blind to whatever happens inside of encrypted tunnels (HTTPS traffic). Hackers have adopted their own evasion and attack techniques, and often use encrypted tunnels (HTTPS) to attack their targets.

Thousands of targets around the world are attacked every day, and enterprises across all verticals (e-commerce, financial, education, health care, industry and others) are affected.

Every enterprise needs to consider protecting their mission-critical web applications/services and APIs. **It is indispensable to be well prepared, as every enterprise is a potential target.**

LINK11 WEB DDOS PROTECTION

The Link11 Web DDoS Protection is a patent-pending, cloud-based DDoS protection service for web applications/services and APIs which provides state-of-the-art protection against layer 3 to layer 7 DDoS attacks of any kind. It is based on Link11 owned and operated scrubbing centers located all around the globe. They can handle terabits of traffic easily. A worldwide network of mitigation clusters works together in real-time to keep Link11 customers secured.

Link11's Web DDoS Protection is based on innovative detection and mitigation techniques that protect against all common types of DDoS attacks. Detection is based on multiple technologies working together.

Modern, globally distributed computers and big-data engines ensure detection of all common types of DDoS attacks in seconds. Patent-pending Artificial Intelligence ensures the detection of known, unknown and zero-day attacks. The Link11 Security Operation Center (SOC) and customers are informed immediately after an attack is detected. At the same time, mitigation mechanisms and engines are instantly activated to block any detected attack, globally.

Various leading mitigation techniques are used simultaneously to ensure the highest possible mitigation rates and the lowest possible false-positive rates.

GLOBAL DELIVERY MODEL

- Globally distributed Link11 DDoS Filter Clusters in premium data centers
- 24/7 operations model via the Link11 Security Operation Center (LSOC)
- Self-built filter technology leveraging AI and machine learning
- Self-engineered software stack, running and orchestrating the Link11 Cloud Security Platform
- IP connection to Level3, Cogent, TeliaSonera, Deutsche Telekom and other major carriers
- Real-time access to the Link11 WebGUI
- Private peering relationships and links to the main Internet exchanges

FEATURES

- Automatically Generated and Adjusted Base
- Deep Packet Inspection
- Artificial Intelligence (AI)
- Big Data Engines
- Protocol Verification
- Session Analysis
- Challenging Mechanisms
- Address Rate Limiting
- Protocol Rate Limiting
- Anomaly Filters
- Signatures
- Reputation Databases
- GEO IP Blocking
- Dynamic Black-/Whitelists
- SYN Cookies
- Maximum Availability (According to Industry Standards)
- Minimal Time to Mitigate
- 24/7 support by the Link11 Security Operation Center (LSOC)
- Available Mitigation Capacity

BENEFITS

Self-Learning DDoS Protection Based on AI

Link11's patent-pending DDoS filter technology offers protection against non-volumetric and volumetric attacks. Protection is ensured from layer 3 to layer 7. Single-vector and multi-vector attacks get detected and mitigated. Sophisticated algorithms based on Artificial Intelligence ensure that even zero-day attacks are detected. The solution offers the ability to integrate on-premise/hybrid scenarios via a remote monitoring box (Link11 DDoS Sensor).

State-of-the-Art Reporting and Monitoring

The Link11 WebGUI enables customers to monitor and configure all services via one common interface. It provides access to real-time statistics and helps customers to understand ongoing threats. Customers can easily add further security services to increase their protection level.

24/7 Single Point of Contact

The Link11 Security Operation Center (LSOC) acts as a single point of contact at any time. Network and security experts are available whenever needed, around the clock. This ensures that no handover to any other group or vendor is required.

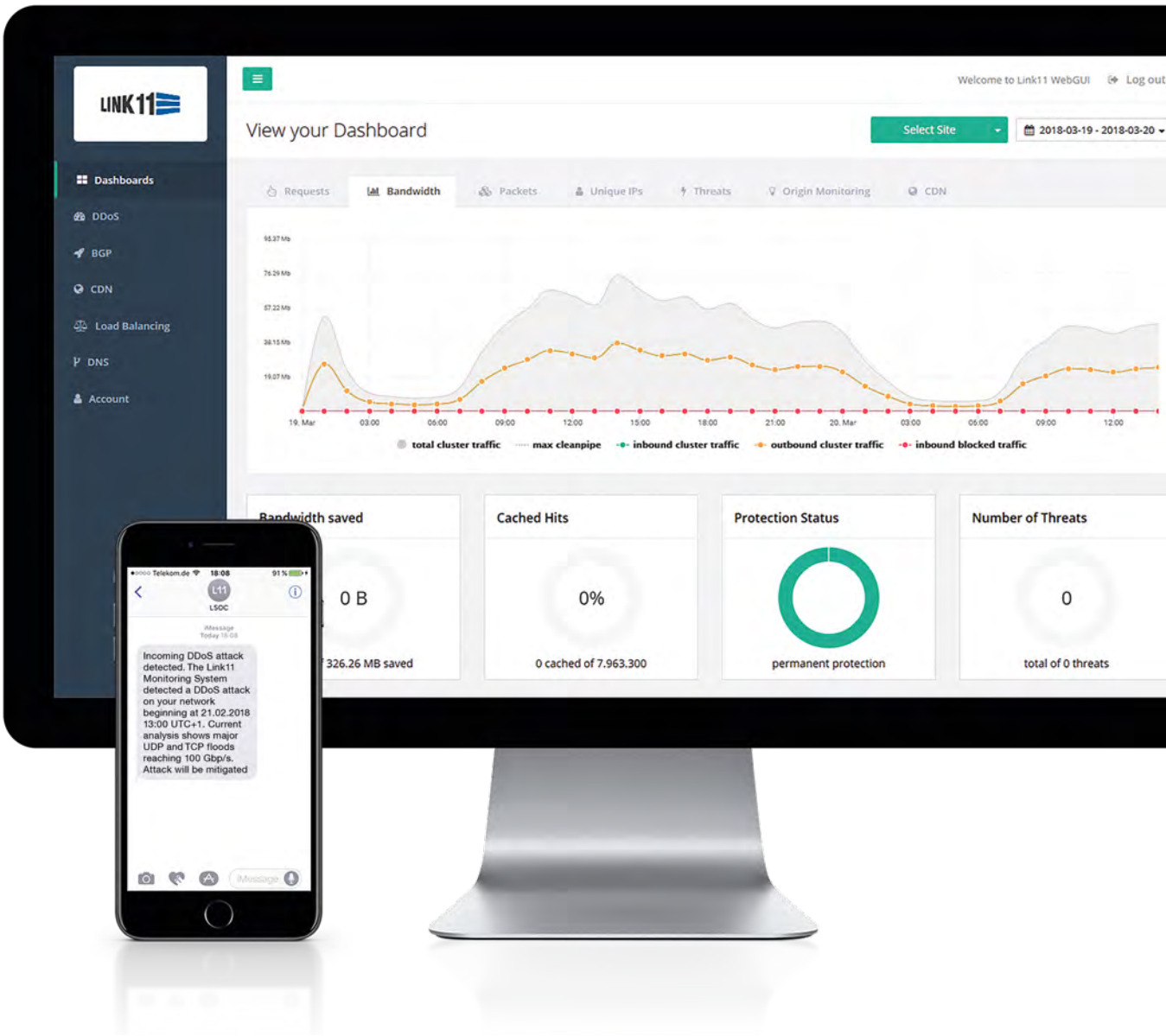
Lowest Possible Time to Mitigate

Link11's patent-pending DDoS detection and mitigation mechanisms detect abnormal activities and mitigate even unknown and future attack types and vectors automatically in real-time. This is how we ensure a market-leading time to mitigate.

LINK11 WEBGUI

Link11 operates several scrubbing centers around the globe. Attacks get mitigated as close to the source(s) of the attack as possible. Intelligent internal traffic steering ensures best possible usage of all available resources. All scrubbing centers are in sync at all times, thanks to real-time synchronization. Customers can count on Link11's global capacity of multi-terabits per second.

Customers get access to a state-of-the-art, web-based portal that provides visibility at all layers and 24/7 self-service. The Link11 WebGUI provides customers with real-time statistics (bandwidth, mitigation, attack details), role-based access control and attack reports.




19
21
23
18
20
22
24
19
21
23


17

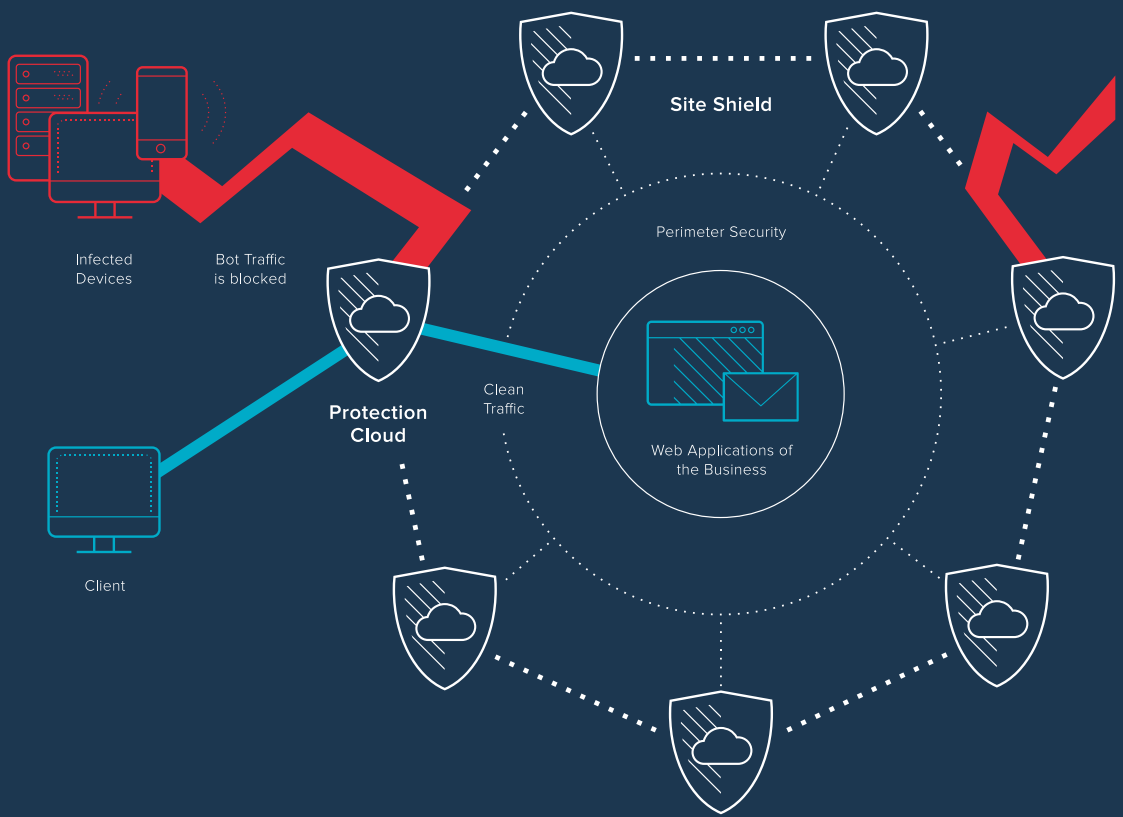
IMPLEMENTATION

The Link11 Web DDoS Protection requires the customer's application, service or API traffic to pass through Link11's Cloud Security Platform at all time. All traffic is forced to flow via Link11 using DNS record changes. Link11 will provide public IPs and DNS record changes to ensure traffic reaches Link11 first. If necessary, our DDoS protection proxies will handle all incoming traffic and pass it through various detection engines and mitigation engines. Attack traffic is filtered out, and the remaining legitimate traffic is forwarded to the original application, service or API IP addresses via the public internet.

The customer can optionally choose to handle SSL/TLS traffic at Layer 7 inside Link11's DDoS protection proxies. Using customer-provided valid certificate/key pairs, they are able to terminate SSL/TLS following the latest standards. This ensures visibility at layer 7 for maximum security. Traffic is re-encrypted again when it passes through all detection and mitigation mechanisms.

Our Site Shield/Protector ensures that the original backend IPs are not directly attackable, as attackers might try to bypass the Link11 Web DDoS Protection by accessing the origin servers directly.

Link11 Web DDoS Protection



TRAFFIC FORWARDING VIA DNS

The Link11 Web DDoS Protection Proxies need to analyze inbound and outbound traffic for all protected applications. They act as proxies – inbound traffic is forwarded to Link11 using DNS A record changes.

Original DNS Entry

```
www.customer-example.com. 60 IN A a.b.c.d
```

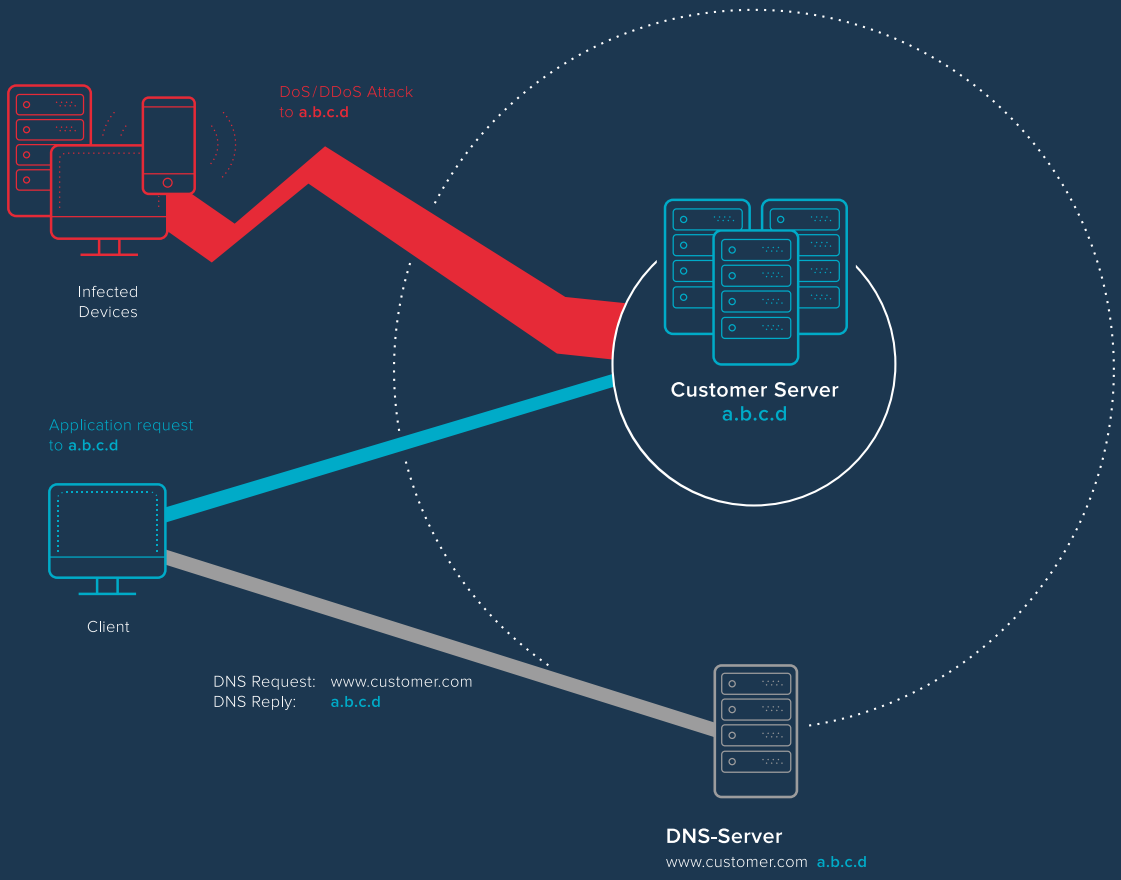
The fully qualified domain name (FQDN) www.customer-example.com is pointing to a customer-owned public IP “a.b.c.d”. Implementing Link11 Web DDoS Protection for www.customer-example.com requires the customer to change this DNS entry, as it needs to point to a Link11 owned public IP.

Changed DNS Entry

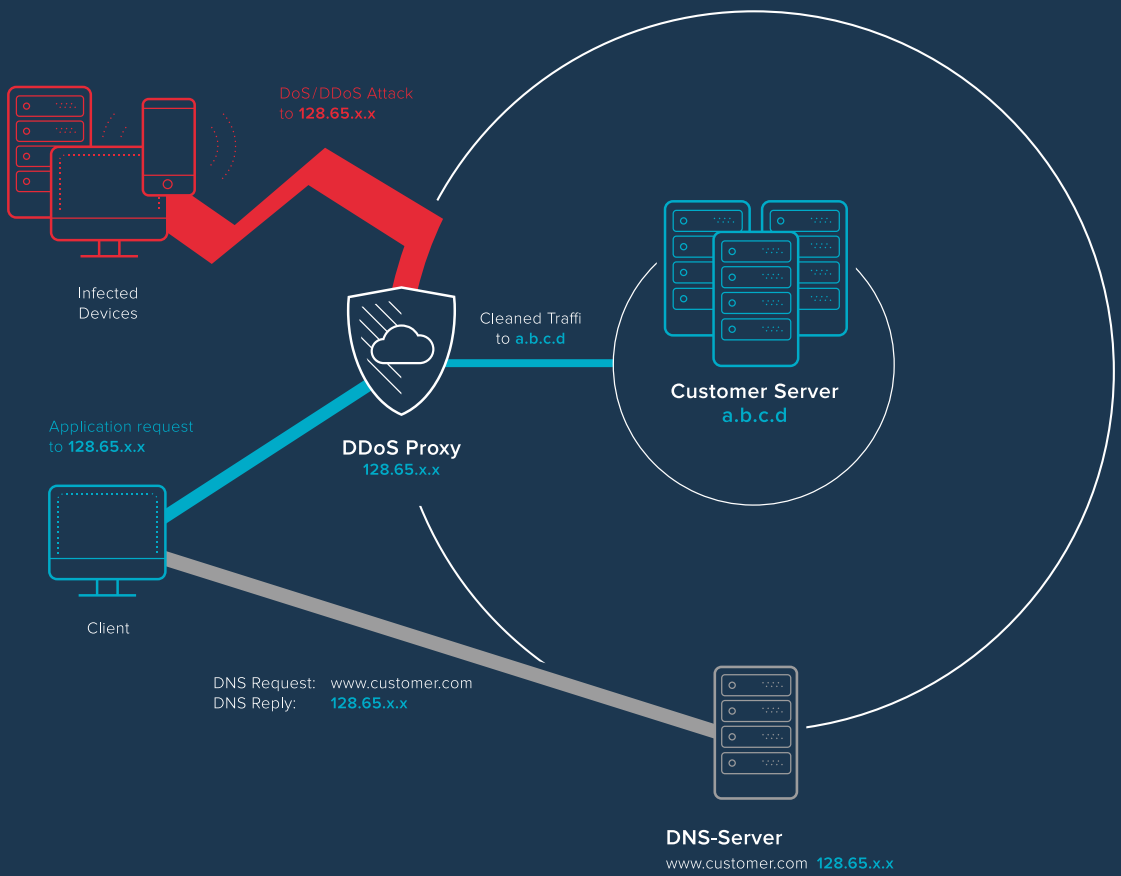
```
www.customer-example.com. 60 IN A 128.65.x.x
```

Client DNS queries will now resolve www.customer-example.com to 128.65.x.x, which forces them to connect to Link11 Web DDoS Protection Proxies instead of the original customer-owned public IP.

Traffic Flow without Link11 Web DDoS Protection



Traffic Flow with Link11 Web DDoS Protection



MITIGATED ATTACKS

The patent-pending DDoS detection and mitigation mechanisms of the Link11 Web DDoS Protection detect abnormal activities and mitigate known, unknown and zero-day attacks and vectors automatically in real-time.

Abstract of Attacks Detected & Mitigated

- IP Fragmentation
- ICMP Floods
- IGMP Floods
- UDP Floods
- TCP Floods
- SYN Floods
- TSUNAMI SYN Floods
- DNS Query Floods
- NTP Floods
- Packet Anomalies
- SSL Renegotiation Floods
- SIP Floods
- NTP Reflection
- SSDP Reflection
- DNS Reflection
- CHARGEN Reflection
- SNMP Reflection
- CLDAP Reflection
- Protocol Anomalies
- HTTP Floods
- Encrypted HTTP Floods
- Low & Slow Attacks

CONTACT OUR EXPERTS

Do not lose the race! The attack landscape is changing rapidly, and attackers find new ways to take down their targets on a daily basis. Ransom DDoS has become more and more popular – who knows who will be hit next?

DDoS protection is a mandatory pillar of any security strategy. Get in touch with the experts from Link11 to gain access to the world's leading DDoS protection for web applications, services and APIs.

link11.com

+49 (0) 69 264 929 777

sales@link11.com

GROUP HEADQUARTERS: LINDLEYSTR. 12, 60314 FRANKFURT, GERMANY