LINK11

WE MAKE THE INTERNET A SAFER PLACE

LINK11 CLOUD SECURITY PLATFORM

A STRONG PARTNER

COMPANY

Long-term experience for your security.

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 CLOUD SECURITY PLATFORM

The patent-pending Link11 Cloud Security Platform is based on a worldwide unique technology. Via a two-level protection method all attacks are blocked and filtered.

The Link11 DDoS Protection is future-proof, cost-efficient and can be deployed via DNS Forwarding or BGP. The core of both solutions is the Link11 Scrubbing Technology. With this, Link11 customers are suited against every possible attack scenario.

Customers profit from a constantly evolving technology that makes an investment into new or further hardware obsolete. Additionally, Link11 always analyzes the development of DDoS attacks at any given time and strategically places new scrubbing centers where the DDoS traffic is intercepted close to its source.
The Link11 Cloud Security Platform includes further tools that boost your performance and helps you to deliver your content to customers more secure. You have access to a large-scale portfolio with secure DNS hosting and SSL, CDN (Content Delivery Network), a Web Application Firewall (WAF) and several optimization tools combined with the Link11 DDoS Protection.

ALL BENEFITS AT A GLANCE

High-Value Investment

Keep your focus on what is important. Further investments in extra hardware and staff training is obsolete. The Link11 Cloud Security Platform runs fully automated and is under constant development.

360° Protection

The self-learning technology is based on Artificial Intelligence (AI) and reliably blocks every form of attacks. Depending on the implementation, Link11 protects against DDoS attacks on layer 3 as well as 4-7 and is ready within a few minutes.

Scalability

Similar to your growth and need to expand your infrastructure your protection grows with you. Special packages fitted to your needs simplify the scaling of your IT security.

NEXT GENERATION DDOS PROTECTION

The Link11 DDoS Protection consists of an Artifical Intelligence with two individual cores that guarantee your security.

The Link11 Fingerprint Identification analyzes on a multi-level proofing system the attributes of every user and recognizes them so that regular customers can access your service without any anomalies.
To react quickly, the self-learning AI Shield activates automatically in the case of an attack and checks and compares the attack pattern with existing data. The DDoS traffic is then redirected to the nearest scrubbing center.

Cloud-Based DDoS Protection

While the protection by traditional appliances is executed automatically and quite inflexible, Link11 can protect the infrastructure dynamically. The DDoS Protection Cloud from Link11 has been developed to be reliable and future-proof.

During the first step, the incoming traffic is meticulously analyzed and every client receives a digital fingerprint. This fingerprint consists of hundreds of attributes like browser information, user behavior and network location and makes sure that the regular visitors can access the services even during an attack without noticing any disturbances. When the fingerprint identifies already known attack pattern, the client is blocked in the first request. Via a digital DNA Memory, every fingerprint is hashed anonymously and can be compared to new data at any time.

The user behavior is constantly analyzed and adjusted to existing data. The scoring model of the behavior identification equips every connection with a value according to the intelligent statistical model. When a connection does not comply with the norm, it can be treated by individual white- and blacklisting requirements.
The self-learning AI Shield from Link11 analyzes the incoming traffic and compares it with existing data from previous attacks that the system autonomously analyses and evaluates. When the AI Shield identifies an attack, it only directs the traffic of affected clients to one of the global scrubbing centers from Link11. Contrary to regular CDN solutions, the load is not just distributed. It is removed completely from the traffic so that regular users do not notice the filtering process.

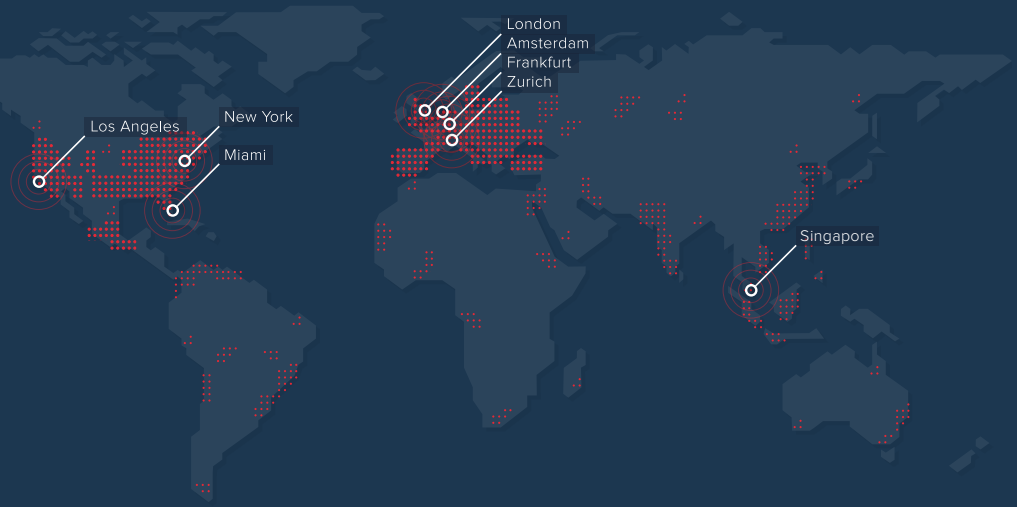
The protection is completely cloud-based and connected to the continuously growing global network from Link11. This way, Link11 can guarantee strong protection that adapts to the quickly changing IT landscape.

Global Filter Locations

By analyzing the incoming traffic, Link11 identifies the source countries where DDoS attacks occur and detects various botnets. Therefore, Link11 strategically picks its global filter locations to guarantee the best protection for its clients.

Link11 only works with selected partners that assure performance and reliability. Only high-security data centers with appropriate certifications are qualified for Link11.

The company is continuously expanding its network, connecting each node with fiber cables to ensure fast and stable bandwidth so that data and files can reach their destination in no time.



LINK11 WEB DDOS PROTECTION VIA DNS FORWARDING

The Link11 Web DDoS Protection is a cost-effective solution to protect a company‘s web-based applications.

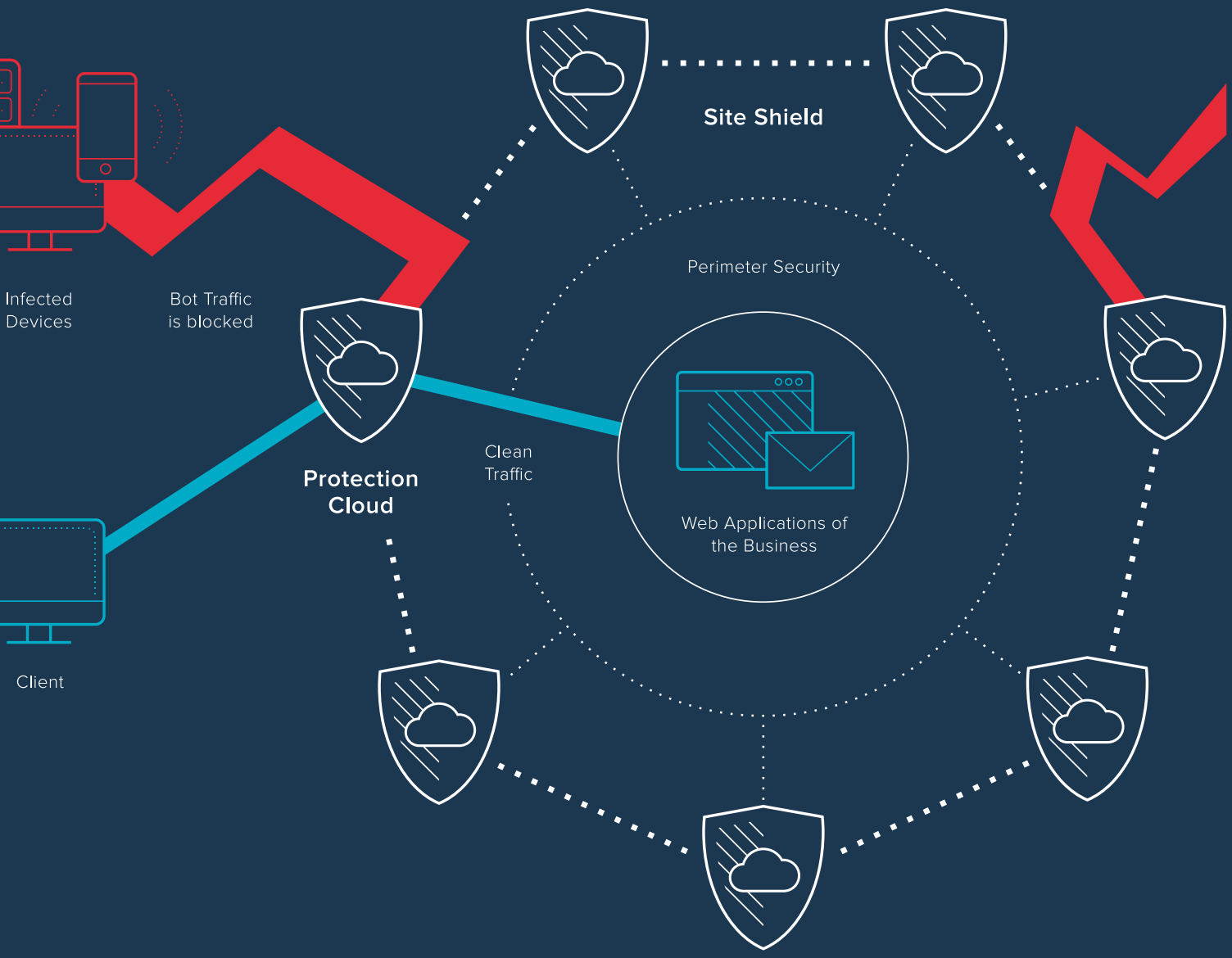
Link11's Web DDoS Protection via DNS Forwarding does not require an upgrade of the server infrastructure, additional bandwidth or new router technology. It is available already from one IP address and protects domain name based applications against DDoS attacks on layers 3–7. To this end, the DNS A record entries in the affected application are adapted to reroute the data transfer to the Link11 Scrubbing Center.

The Link11 Web DDoS Protection via DNS Forwarding mitigates in real-time and is active after the customer's DNS A records have been changed into Link11 owned public IPs.

Site Shield

To prevent culprits from directly attacking the server by using the original IP address, a site shield is established at the DNS protection.

The router/firewall configuration is adjusted in order to permit only access from the Link11 DDoS Filter.


Site Shield
Perimeter Security
Infected Devices
Bot Traffic is blocked
Protection Cloud
Clean Traffic
Web Applications of the Business
Client

LINK11 NETWORK DDOS PROTECTION VIA BGP ROUTING

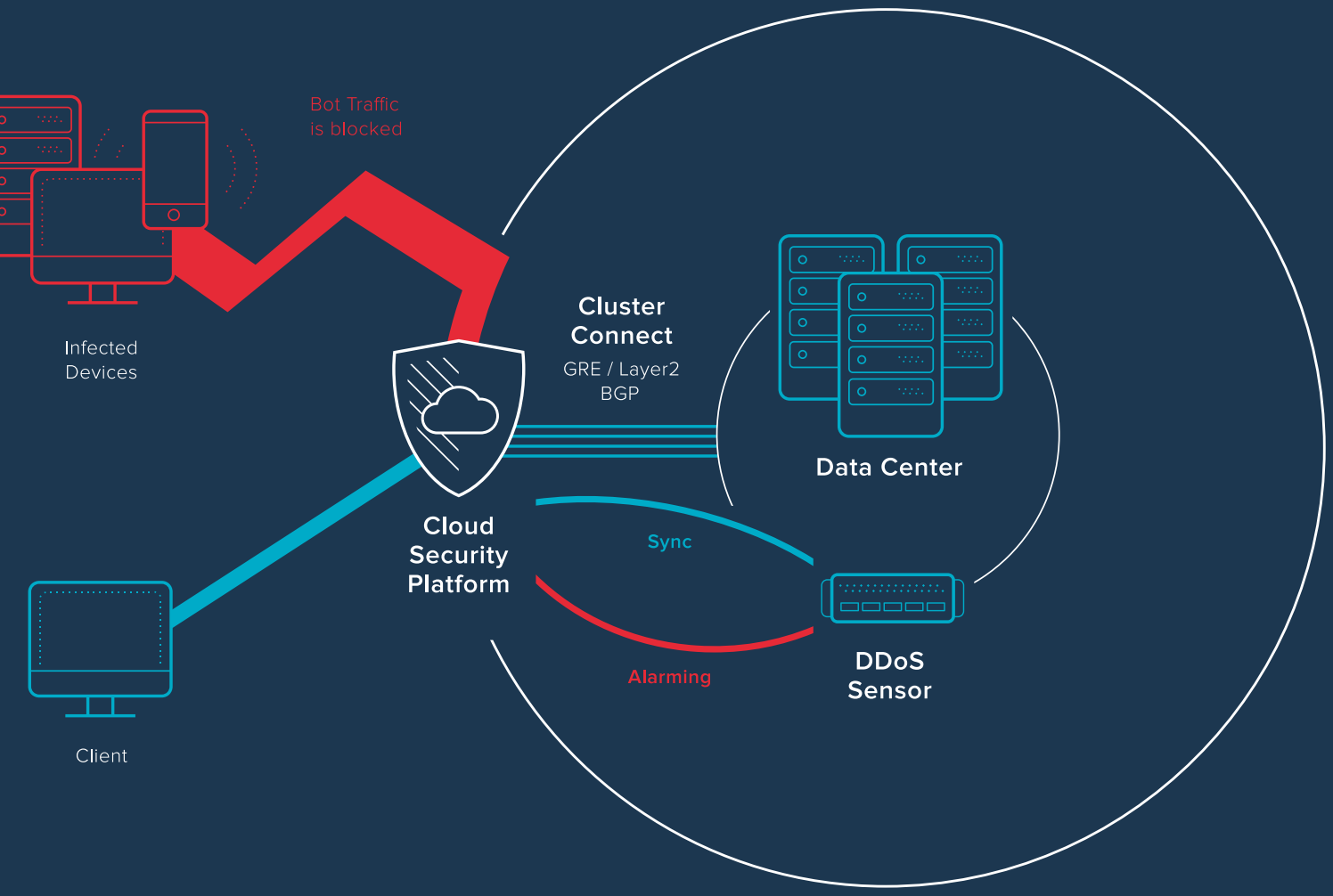
The Link11 Network DDoS Protection requires a /24 or larger IP network for the rerouting. The protection solution can be deployed as a permanent or standby service. In addition, it is also possible to transfer entire protocols on a customized basis. Within the standby integration, the customer as well as the Link11 Security Operation Center are able to announce the network in the event of an attack. By adding the Link11 DDoS Sensor, the flow data of the local routers are constantly analyzed to ensure that the protection is activated automatically in case of an attack.

Network Announcement

In the event of an attack, the network announcement reroutes the entire traffic via the Link11 DDoS Protection for analysis.

It is also possible to announce smaller parts of the network affected by the attack. For example announcing only a /24 network from an existing /16 network to be forwarded to the Link11 protection.

After a successfully blocked attack, the network is then rerouted directly back to the customer via a second announcement.


Bot Traffic
is blocked
Infected
Devices
Cluster
Connect
GRE / Layer2
BGP
Data Center
Cloud
Security
Platform
Sync
Alarming
DDoS
Sensor
Client

SELF-LEARNING AI SHIELD

Every attack mitigated by Link11 is saved within a sequence database. The self-learning AI of Link11's DDoS Protection analyzes each attack sequence and compares these with existing data. Companies protected by Link11 benefit from this technology, which is capable of reacting even faster when similar incidents reoccur.

Attack Sequencer

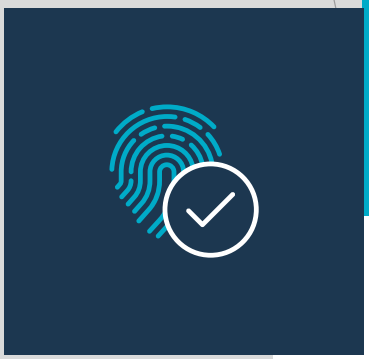
The Attack Sequencer is the core of the AI Shield. The incoming traffic on your infrastructure is compared to an integrated database. When anomalies occur, the data is shared between the AI shield and Fingerprint Identification so that the attack pattern is identified immediately and the protection is initiated within a few seconds.

Deep Machine Learning

The Artificial Intelligence is capable of analyzing the incoming traffic with Deep Machine Learning and comparing the information with the Attack Sequence Database. After the successful defense, every new attack that is identified by the protection as such is dismantled by the Link11 Security Operation Center (LSOC) and examined to identify new attack forms and vectors as soon as possible. This assures that the Link11 AI Shield is always prepared for new types of attacks on your infrastructure.

FINGERPRINT IDENTIFICATION

Every user leaves a digital fingerprint on the internet. This print is based on hundreds of traceable attributes. The Fingerprint Identification developed by Link11 analyzes the behavior of browsers and computers and creates an anonymous digital DNA that is temporarily saved for further reference within the database of the cloud protection. This assures that customers can safely reach their destination.



Digital DNA Memory

The digital fingerprint every user leaves is put together from hundreds of attributes. This fingerprint is saved anonymously within the digital DNA Memory so that clients can be recognized and blocked when needed. The deception-resistant system is linked to the AI Shield, can learn new attack patterns and compares these with the existing data. The data is hashed anonymously and dynamic IP addresses are not saved.

Behavior Identification

With the constant redirecting of traffic over the Link11 network, the behavior identification controls the behavior of every user. According to a scoring model every client is rated and directed through the filter. During this process, every request must pass various proofing levels. Suspicious behavior leads to CAPTCHAs and temporary bans. Clients from known botnets are blocked immediately while regular users access the services. At the same time, the individually defined white- and blacklisting requirements help to reach the target group and to keep unwanted packages like UDP and ICMP away from your network.

LINK11 WEBGUI

Link11 offers its customers a web-based, graphical user interface to monitor the servers protected by DNS Forwarding. The interface provides insight into the real-time traffic analysis, shows blocked DDoS attacks, server availability and provides metrics on current server response times. Graphical timelines can be displayed and analyzed. In addition, it presents the nature of attacks and respective places of origin. Furthermore, the Link11 WebGUI makes it possible to block entire countries by a geo-blocking function.

Diagnose Dashboard

The Diagnose Dashboard offers general DDoS information and hints on current threats. In addition, a DDoS warning system and DDoS traffic indicator offer a quick overview on the current security status. In the settings, the granularity of the intelligent DDoS prevention can be defined and customized blocking can be used to adjust settings for authorized and unauthorized access.

Whitelist

Whitelists can be used to set up permanent authorized access for systems that deviate too far from that of a normal user. Within the dashboard of the Link11 WebGUI automated scripts such as crawlers can be identified, ensuring compatibility with standard search engines, desirable advertising bots and administrators.

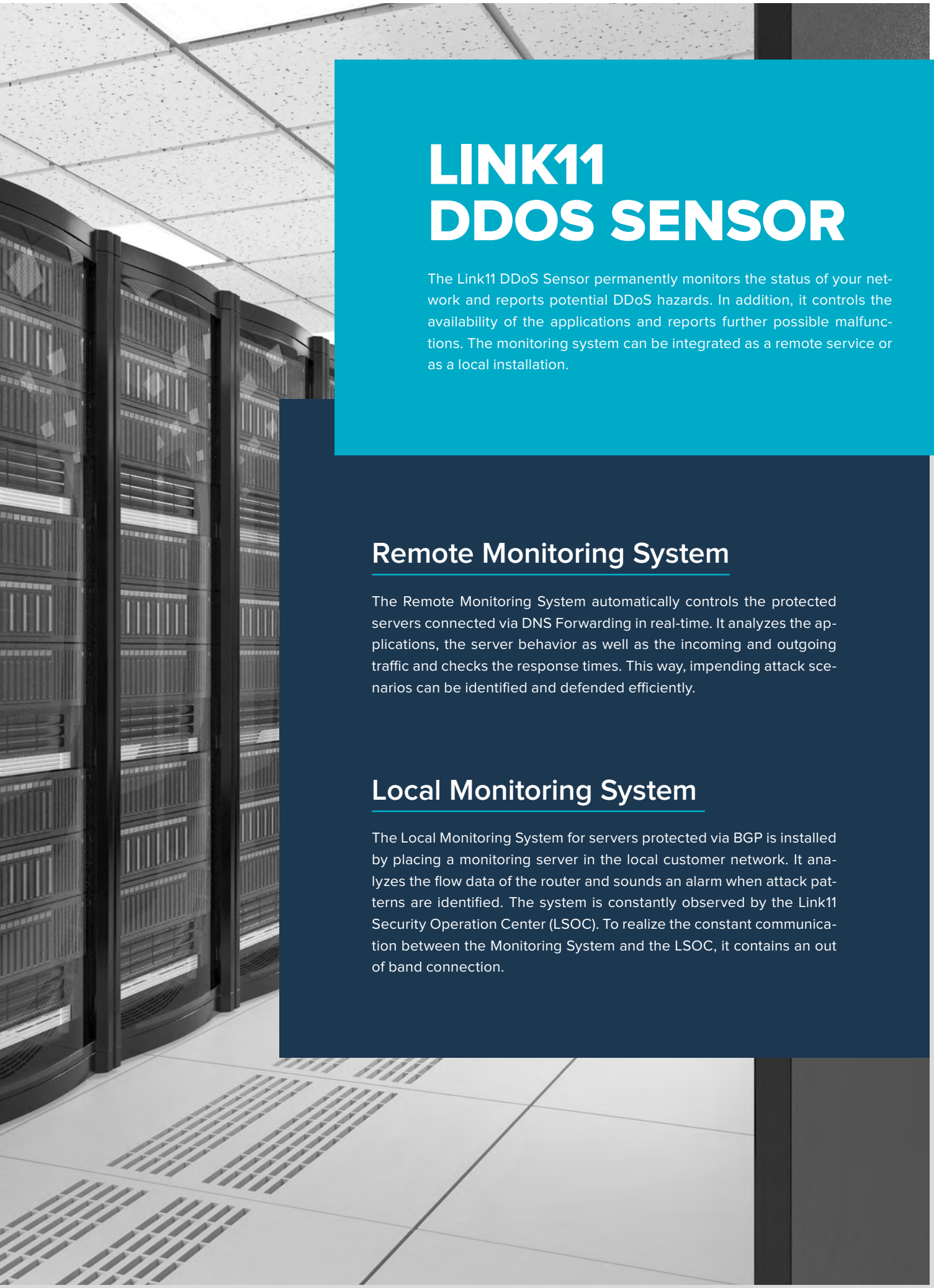
Alert Function

An alert function is able to send SMS alerts about current threats. The prevention list states the reason for each blocked connection, the origin and the duration of the connection. The blocked connections can also be authorized to access the server on their next attempt.

Reporting

Individual reports make it possible to generate and routine reports in a management overview. The reports can be transmitted on a regular and automatic basis. Any settings made by administrators in the user interface can be traced and edited ad hoc.


LINK11
Welcome to Link11 WebGUI
Log out
View your Dashboard
Select Site
2018-03-14 - 2018-03-20
Dashboards
DDoS
BGP
CDN
Load Balancing
DNS
Account
Requests
Bandwidth
Packets
Unique IPs
Threats
Origin Monitoring
CDN
total cluster traffic
mux cleanpipe
inbound cluster traffic
outbound cluster traffic
inbound blocked traffic
Bandwidth saved
0 B
0 B of 0 B saved
Cached Hits
0%
0 cached of 0
Protection Status
Number of Threats
0
total of 0 threats
Blocked IP
Search
Date
Attacker IP
Country
Attacker ISP
Reason
Top Talkers
Search
Date
IP
Country
ISP
Hits



LINK11 DDOS SENSOR

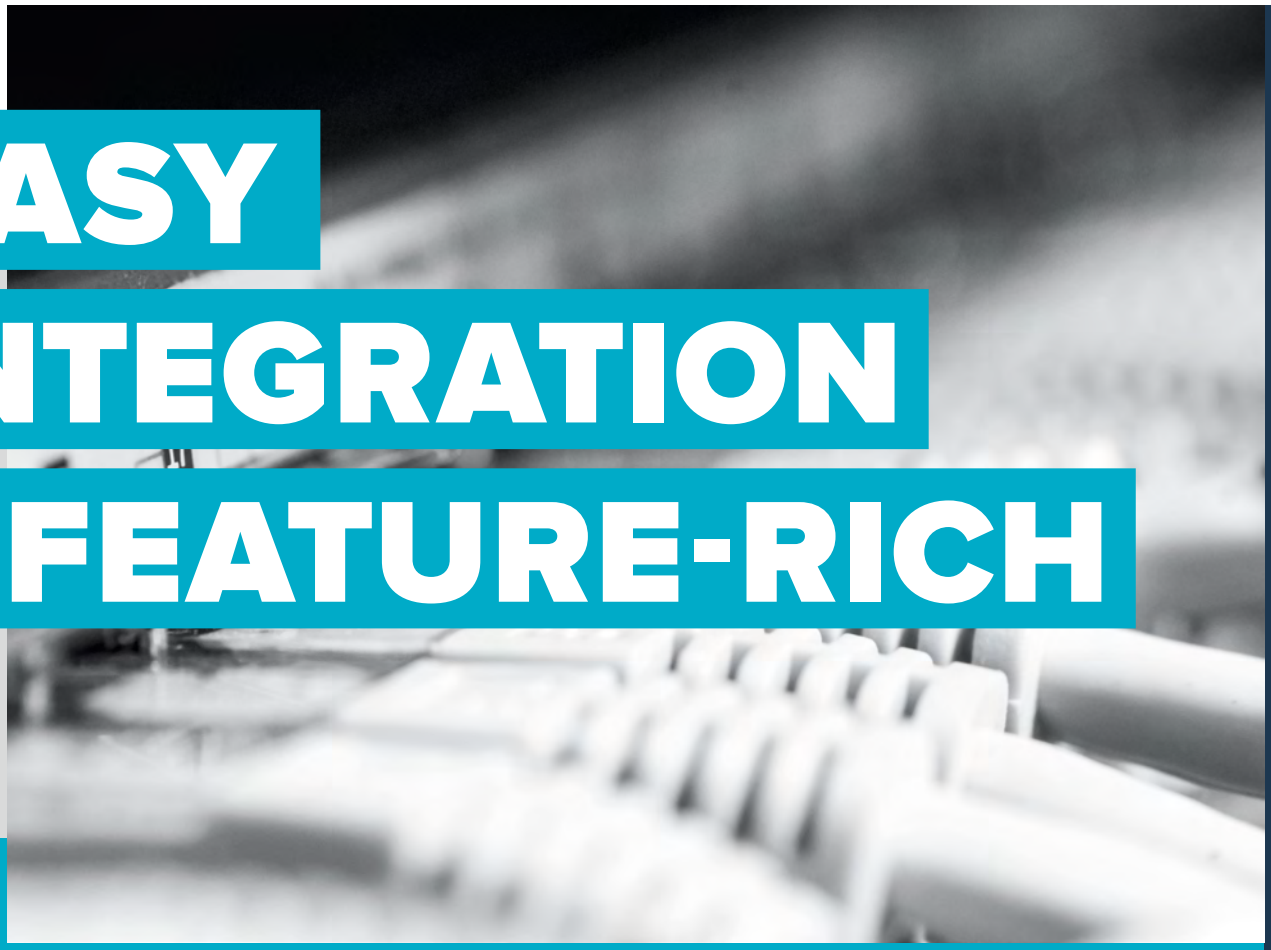
The Link11 DDoS Sensor permanently monitors the status of your network and reports potential DDoS hazards. In addition, it controls the availability of the applications and reports further possible malfunctions. The monitoring system can be integrated as a remote service or as a local installation.

Remote Monitoring System

The Remote Monitoring System automatically controls the protected servers connected via DNS Forwarding in real-time. It analyzes the applications, the server behavior as well as the incoming and outgoing traffic and checks the response times. This way, impending attack scenarios can be identified and defended efficiently.

Local Monitoring System

The Local Monitoring System for servers protected via BGP is installed by placing a monitoring server in the local customer network. It analyzes the flow data of the router and sounds an alarm when attack patterns are identified. The system is constantly observed by the Link11 Security Operation Center (LSOC). To realize the constant communication between the Monitoring System and the LSOC, it contains an out of band connection.



EASY INTEGRATION & FEATURE-RICH

Hybrid DDoS Protection

Nowadays, the capacity of DDoS mitigation hardware is not enough to deal with large and complex DDoS attacks. Link11 has developed a hybrid solution that offers protection against combined attacks on application and network layer.

The hybrid solution protects on both sides: The hardware installed in the business infrastructure protects against application attacks. The external scrubbing centers from Link11 protect against bandwidth-heavy, volumetric attacks and is the ideal addition to your existing hardware. The appliance oversees traffic and blocks DDoS attacks on Layer 3-7. When the amount of DDoS packages on network layer exceed a certain value, Link11 is alarmed, offers counter-measures immediately and takes over the mitigation via BGP.

DDoS Protection for Hosting Providers

By connecting the data center (or the shared internet access platform) with the Link11 network, all customers using this connection can be protected against volumetric and protocol-based attacks when desired. The customers receive an IP address within the network range (≥ /24) that is solely connected with Link11. When this IP address is attacked, the traffic is immediately and automatically routed over the Link11 Scrubbing Centers. All other IP addresses within the protected range still receive their traffic over the regular Link11 IP access without having to go through the DDoS filtering process. This way, they are not affected by the incoming DDoS attack.

FEATURES

DNS Forwarding / BGP Announcement
The service can be implemented via DNS Forwarding, or the data transfer is guided and filtered in the event of an attack via BGP. This makes the Link11 DDoS Protection independent of the client server location.

User / IP Filtering
Link11 observes the behavior of the individual user and has granular user prevention capabilities.

Multi Ten Gigabit Aggregation
Several 10GE Tier 1 provider uplinks to the individual scrubbing centers.

IP Reputation Filtering
There is a constant comparison with the Link11 database that contains IP addresses which are part of a botnet or otherwise misbehaving.

Statistical Application Protocol Inspection
Analysis of application protocols (e.g. HTTP) with several statistical models and filtering of malicious requests.

Crawler Detection / Identification
Identification of authorized or unauthorized internet crawlers. Compatible with standard search engines.

Flooding Attack Mitigation
Detection and prevention of volumetric attacks on websites (HTTP, SYN, UDP, etc.).

IP Rate limiting
Individual limitation of the data rate to the customer.

GEO Blocking
Exclusion of users from certain regions (country-specific).

SSL Encryption
Optional termination of the SSL connections directly at the Link11 DDoS Filter.

Web Application Firewall Filtering
Customers have the option to add a WAF for applying individual firewall rules to protect applications.

Caching
Static HTTP client content is cached in the Link11 network.

SSL Handling
Optional termination of SSL connections directly at the Link11 DDoS Filter.

DDoS Mitigation on Layer 3 and 4
DDoS protection on protocol layers 3 and 4.

DDoS Mitigation on Layer 7
Application-specific protection on application level.

Suspicious User Behavior Recognition
Statistical procedure for individual detection of suspicious behavior on the website.

Whitelisting / Blacklisting
Customers are able to maintain their own black- and whitelists.

Suspicious User Blocking
Conspicuous users are blocked based on a defined threshold value. These users have the option to enable their access via a CAPTCHA page.

Link11 WebGUI / DDoS Sensor
Graphical user interface, which permits real-time analysis of the data traffic from the website, provides information on the form of attacks and serves as an administrative interface.

Reporting
Individual reports that can be transmitted to defined users.

DNS Anycast Protection
To mitigate DDoS attacks on the DNS infrastructure, Link11 offers a DNS Anycast compound system.

LINK11 WEB APPLICATION FIREWALL

Link11's cloud-based Web Application Firewall (WAF) service is an add-on to the Link11 Web DDoS Protection. It protects applications and APIs against all common web application threats, including the Open Web Application Security Project's Top10 (OWASP Top10). Mission critical applications can get complete protection against all common web application threats and attacks with a single solution.

BENEFITS

- Protects critical web applications, APIs and services
- One-click deployment on top of Link11 Web DDoS Protection
- Global coverage using Link11 Cloud Security Platform
- Single point of contact for 24/7 support and emergencies
- Real-time access to Link11 WebGUI
- Attack reports
- State-of-the-art encryption (SSL/TLS)
- Specific front-end SSL/TLS settings
- Specific back-end SSL/TLS settings (reencryption)
- OWASP Top10 coverage out-of-the-box
- DoS/DDoS protection

Self-Learning DDoS Protection Based on AI

Link11's patent-pending DDoS proxy 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. Web application threats are detected and blocked. OWASP Top10 coverage out-of-the box.

State-of-the-Art Reporting and Monitoring

The Link11 WebGUI enables customers to monitor and configure all services via one common interface. It offers a consolidated view across all security modules from layer 3 to layer 7 and across all protected applications.

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.

WE PROTECT YOUR BUSINESS

A cloud-based scrubbing service is a must-have today. DDoS attacks can easily take your internet facing applications offline in seconds. But enterprises need to take care of more than just DDoS – web applications and APIs also need protection against additional web application threats. A WAF is essential to ensure 360° application security. The Link11 WAF complements the Link11 Web DDoS Protection to cover today's most common web application security threats, known as the OWASP Top10. The solution is based on the OWASP ModSecurity Core Rule Set (CRS) to guarantee the best possible coverage. The rules are manageable and well documented.

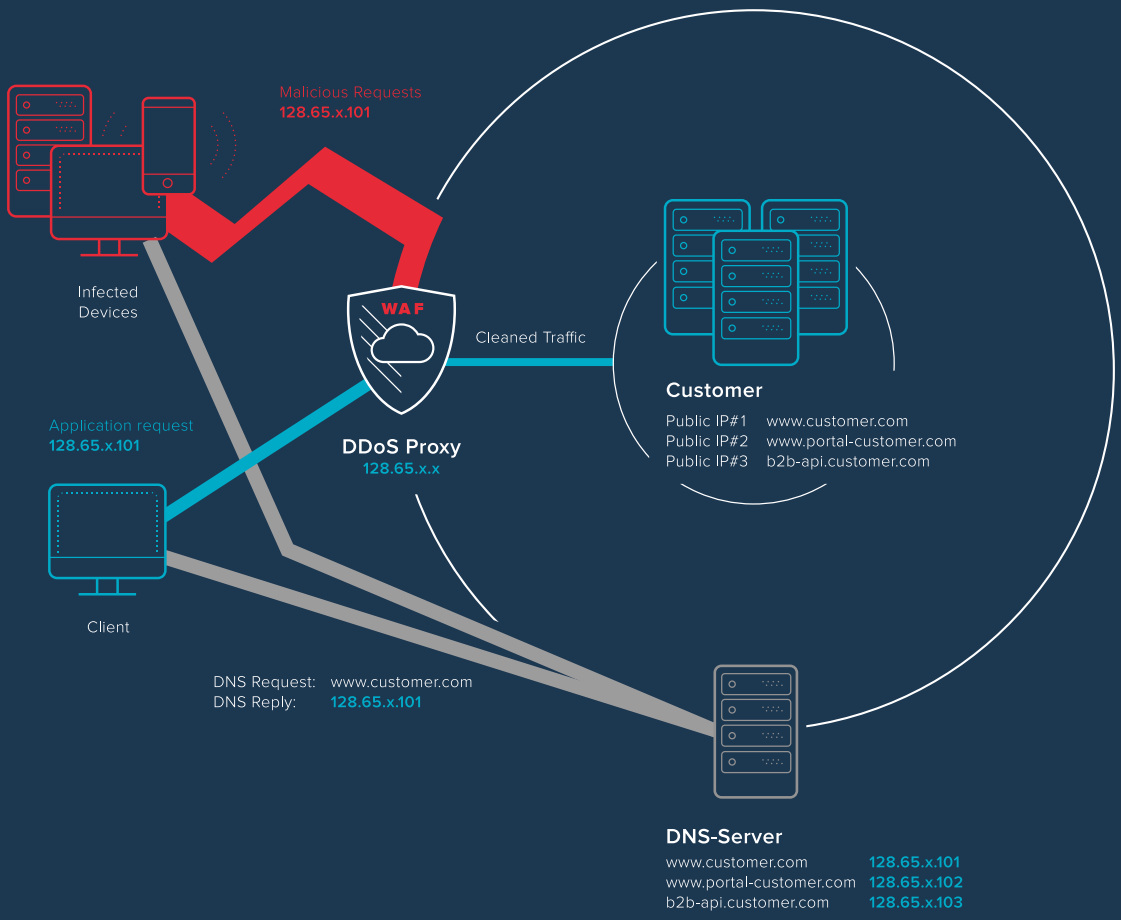
THE RULE SET PROVIDES PROTECTION AGAINST COMMON WEB ATTACKS AND HACKS LIKE:

- SQL Injections
- Cross-Site Scripting
- Local File Inclusion
- Remote File Inclusion
- Remote Code Execution
- Metadata/Error Leakages
- Scanner Detection
- Session Fixation
- Shellshock
- HTTProxy
- GeoIP Country Blocking

Together with Web Application Firewalling, Link11 Web DDoS Protection provides full coverage against attacks and threats at all layers. Protection of SSL/TLS encrypted services is also possible. Due to the solution's always-on deployment, customers get immediate protection against any type of DoS, DDoS attack or application threat that strikes their services.

Traffic is cleaned in Link11's Cloud Security Platform, and the cleaned traffic is sent back to the customer via the public internet. The protection services act as a proxy between clients/attacks and the customer. SSL/TLS Termination is possible and includes the ability to reencrypt traffic back towards the origin server. Implementation is fast and simple.

Link11 Web DDoS Protection with Web Application Firewall



LINK11 SECURE DNS

Customers, employees and partners – they all expect instant, secure, and reliable access to your website, no matter where they are or which device they use. The Domain Name System (DNS) is responsible for the translation of human-readable domain names into numerical IP addresses. This critical process assures a faster web experience for your website visitors and application users.
Despite the importance, many organizations are reluctant to deploy a sufficient DNS infrastructure and only rely on two or three DNS servers. As a result, they leave their services vulnerable to data center outages and DDoS attacks.

The domain name resolution service Secure DNS provided by Link11 resolves your DNS request through the global network consisting of redundant servers. Other than the DNS servers provided by your ISPs, you are capable of providing a much faster and reliable customer experience that does not require any hardware or software installation.

The Secure DNS server infrastructure is more reliable as it spans over many locations distributed around the world. This way, Link11 can offer one of the most reliable and fully redundant DNS services within Europe. Each node is deployed with multiple servers that are connected via several Tier 1 carriers to the internet. The complete infrastructure is realized with strong partners that guarantee 100% availability by SLAs.

To be faster than others, Link11 uses strategically placed nodes where the important intersections of the internet are located. DNS requests are always answered by the closest server and content is reached by users faster than ever before.

Built-In Security

You get access to comprehensive DNS protection against DDoS attacks based on DNS. Our self-developed platform is resilient to hijacking and other cybercriminal attempts. Additionally, Secure DNS helps stopping phishing and the name server segmentation keeps you protected.

DNS Shielding

The DNS Shielding minimizes the security risk of DDoS attacks and provides low latency and a better response rate.

High Performance

The globally distributed BGP and IP anycast network responds accurately and manages over millions of queries per day. You gain access to far-reaching control and flexibility with the advanced management features. Secure DNS includes a management dashboard with failover options that provide an additional level of redundancy.

SSL

With the SSL functions of Link11 you can lift your website security to a new level. The SSL from Link11 is integrated in the DDoS Protection Platform and defends your clients from unwanted access. At the same time, your web performance is increased as well as your opportunities to gain more awareness.

SSL Management

Link11 takes care of the complete SSL Management and can provide you with all information on your protocols and their expiration date at any time.

SSL Offloading

With SSL Offloading the web server is relieved and does not have to handle the encryption and decryption of SSL. Link11 takes care of your SSL Acceleration and SSL Termination.

Perfect Forward Secrecy

Especially governmental institutions have to rely on their security and none of their confidential files being compromised. With Perfect Forward Secrecy keys are renewed after every session and cannot be recreated from a long-term session key.

SSL Updates

Link11 manages the actualization of your SSL/TSL protocols. This service assures you to be always up to date.

Better SSL Ranking

With the right SSL protocols your website is optimized for search engines (SEO). Link11 choses the right protocols for you and helps you to become more visible.

Integration

No matter if you are making a new setup or just updating an existing system, just a few clicks and Link11 sets everything up for you.

Link11 Certificates

The SSL Certificates from Link11 strengthen the trust in your infrastructure and let you know that your security comes from one single source.

LINK11 CDN

Nowadays, content and applications have to reach customers and businesses faster than ever before. The global Link11 Content Delivery Network (CDN) was developed to connect users and businesses in a minimum of time.

A network of locally distributed servers takes care of Link11's worldwide availability. The servers are connected to the most important Internet exchange points of every country that assure the global availability and fast loading of videos and images.

Intelligent Distribution

The Link11 CDN supports Anycast to make your files available everywhere. By sharing one IP address for all nodes the data can be requested even faster as the closest available node will receive the request. The redundancy of multiple servers makes sure that the next server can be addressed when one has gone down without users noticing.

Fast by Technology

The CDN from Link11 increases your website performance by an average of 50%. State-of-the-art SSD flash disks double the loading speed of files. This saves bandwidth and costs.

Set your Data Privacy

In the Link11 WebGUI you have various settings. Thanks to white- and blacklisting functions you have full control over who can see your website and from which nodes they will receive the data.

CORS Header

So far the Same-Origin Policy (SOP) was the standard to guarantee domain security. But now Cross-Origin Resource Sharing (CORS) is gaining popularity as it allows full access of domains without borders. The headers permit browsers and servers to communicate and to define which requests are allowed. The Link11 Content Delivery Network offers full settings of CORS and guarantees secure communication between various domains.

Add DDoS Protection

The Link11 Content Delivery Network is the ideal addition to the Link11 DDoS Protection and secures your files where they are needed.

Handpicked Nodes

Link11 chooses CDN network partners wisely. With local reliable data centers your files can be spread fast, secure and globally.


Center

OPTIMIZATION

Performance, security and reliability.

With more than 11 years of experience as a network provider, Link11 stands for high efficiency. With Link11 you gain access to an efficient optimization technology that not just accelerates your web performance. It gives you security as well.

Caching

The availability of your files and the performance of your website is increased by caching your files on preset servers. The origin server is relieved and users from other regions do not have long waiting times to access files like images and videos.

Backup Website

During maintenance, Link11 supplies your customers with a backup website where users can see all the useful information on the current situation. Provided with the right facts every user knows when the services will be fully available again.

Load Balancing

The Link11 Load Balancer assures the availability of all critical services even when there is much traffic. The dynamic load balancing guarantees a high availability and redundancy of the servers.

Geo Routing

The Geo Routing supports you in making an adjusted range of supply and helps you to bring your services to the place where they will reach the desired target groups best.

GLOBAL LOAD BALANCING

The Link11 Load Balancer is an ideal tool to preserve the availability of all critical services even when there is much traffic. The dynamic load balancing guarantees a high availability and redundancy of the servers.

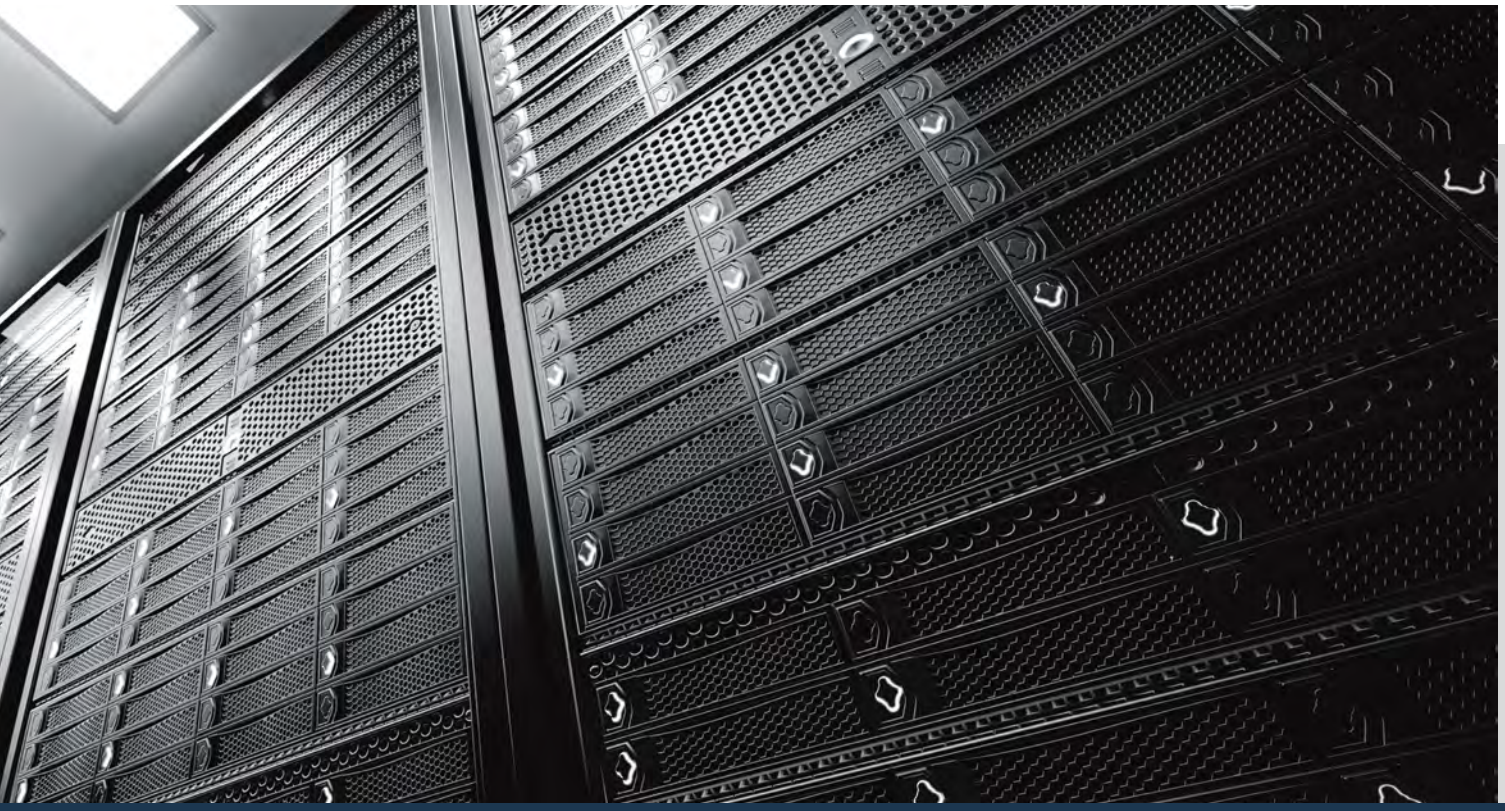
Optimize Your Performance

The Link11 Global Load Balancer offers all the foundation for management technology such as IP control, email notifications and interface control. It provides advanced application health checking to ensure that unavailable services or data centers are not visible to clients. Health checking can occur at the service level or even the site level, allowing flexible decisions on when traffic should be diverted per Fully Qualified Domain Name (FQDN).

The Global Load Balancer from Link11 offers “Round Robin” load balancing for all active data centers, which includes support for weights and a chained failover option for disaster recovery. It offers “Real Server Load” load balancing, in which the Link11 Global Load Balancer uses local data center metrics allowing clients to connect to the least busy data center.

Added to this is the location awareness of your clients which results in your clients being redirected to the most appropriate data center based on their location. The Link11 Global Load Balancer is deployed in a distributed (Active/Active) high availability configuration with secure synchronizing.

Information is compared with the cloud and guarantee redundancy. Implementing the Link11 Global Load Balancer in your existing Authoritative Domain Name Services (DNS) requires minimal integration work, allowing you to fully leverage your existing DNS investment. The Link11 Global Load Balancer can be set up and managed simply. Network management is made easy, administrators can deploy new servers and take individual servers offline for routine maintenance without disrupting services to end-users.



esting clients

est the IP addresses
tomers' servers

Link11 Global Load Balancer

The Link11 Global Load Balancer sends the traffic to the most suitable available customer data center

Customer Data Centers

CONVINCING ARGUMENTS

Link11 as a strong security partner.

- 360° cloud-based DDoS Protection
- Patent-pending AI Filter Technology
- Protects against all types of DDoS attacks
- European data privacy is respected
- Local 24/7 support, short distances
- No investments in hardware and infrastructure needed
- Link11 DDoS Protection is attractive for companies of all sizes
- Link11 Cloud Security Platform combines performance and sercurity services (Secure DNS, CDN, WAF and DDoS Protection)

AWARDS & PARTNERS

Allianz für Cyber-Sicherheit Partner

bevh PREFERRED BUSINESS PARTNER

DEUTSCHER RECHENZENTRUMSPREIS 2016 1. PLATZ KATEGORIE 2: RZ-SOFTWARE

DEUTSCHER RECHENZENTRUMSPREIS 2014 1. PLATZ KATEGORIE 5: RZ-SICHERHEIT

SecurITy made in Germany TeleTrusT Quality Seal www.teletrust.de/itsmig

G4C German Competence Centre against Cyber Crime e.V

eco

HOSTING & SERVICEPROVIDER Award 2014

MEMBER OF BITKOM

50 Technology Fast 50 2017 Deloitte.

CONTACT OUR EXPERTS

Nowadays, a reliable and secure high-performance IT infrastructure is decisive for the success of a digital business. This is why cybersecurity is more crucial than ever. The Link11 Cloud Security Platform is constantly evolving and is adapted to the needs of the current situation.

Make an appointment today to talk to one of our experts in order to find out which of our services is the most appropriate for for your business.

Please visit our website to find more information on the Link11 Cloud Security Platform and and have a look on our quarterly published DDoS report for Central Europe.

link11.com

+49 (0) 69 264 929 777

sales@link11.com

GROUP HEADQUARTERS: LINDLEYSTR. 12, 60314 FRANKFURT, GERMANY