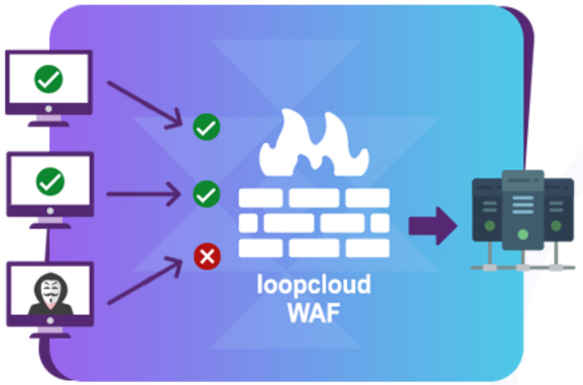
Web Application Firewall

The highest demands on IT security



WAF Highlights

- Filtering (Attack blocking)
- Fraud detection
- Threat Intelligence
- Rapid deployment – DevSecOps
- Reporting & monitoring
- SIEM integration
- Virtual patching
- Load balancing
- Learning Mode for easier administration
- MS applications

Filtering of Application-based Attacks

Our WAF analyses traffic between users and services. Attempted attacks on applications are blocked before they can reach the in-house systems. It provides comprehensive protection against the OWASP Top 10 vulnerabilities and enables centralized management of security policies. Thanks to these innovative security functions, you can always stay ahead of attackers.

Security Dashboards

Thanks to built-in dynamic reporting, decision makers have an overview of attempted attacks at all times. Operational problems such as performance bottlenecks or back-end problems are also displayed. Interactive drill-down from the dashboards, along with the display of the log lines causing the issue, facilitate the in-depth analysis of every attempted attack. In addition, we are a CEF certified, which enables integration with common SIEM solutions. For Splunk there is even an in-house Splunk App available.

LOOPCLOUD

Web Application Firewall

Policy Enforcement Point

Working in conjunction with our IAM, the WAF serves as a policy enforcement point for security guidelines, allowing only filtered, authenticated and authorized access. This combination of access management and content filtering guarantees security, with no compromises.

Reverse proxy and high availability

A reverse proxy makes it possible to virtualize in-house services and applications for external access. The integrated load balancer also ensures the high availability of applications and services. Even complex issues such as the configuration of TLS security and certificate management can be dealt with upstream on the central proxy. Thanks to integrated Let's Encrypt support, certificate renewals can even be completely automated.

DevSecOps

Comprehensive REST API, WAF is easy to integrate into modern DevOps pipelines and can be supplied as hardware, virtual appliance or cloud image. Early integration of the security in application development cycles, including the new Docker- and Kubernetes-philosophies, allows WAF to offer flexible security.

Central Hub

A host of interfaces with peripheral systems such as SIEM systems, virus scanners, fraud-prevention systems and HSMs. Thanks to its integrated threat intelligence feed, WAF reacts immediately to real-time threat situations on the Internet, protecting systems from new and potentially harmful hazards. Additional components can be integrated via the high-availability capable ICAP interface.

All-Round Flexible

Efficient and powerful configuration options allow full adaptability without customization and future updates become easy. A flexible licensing model, customer-specific requirements can be met.

LOOPCLOUD