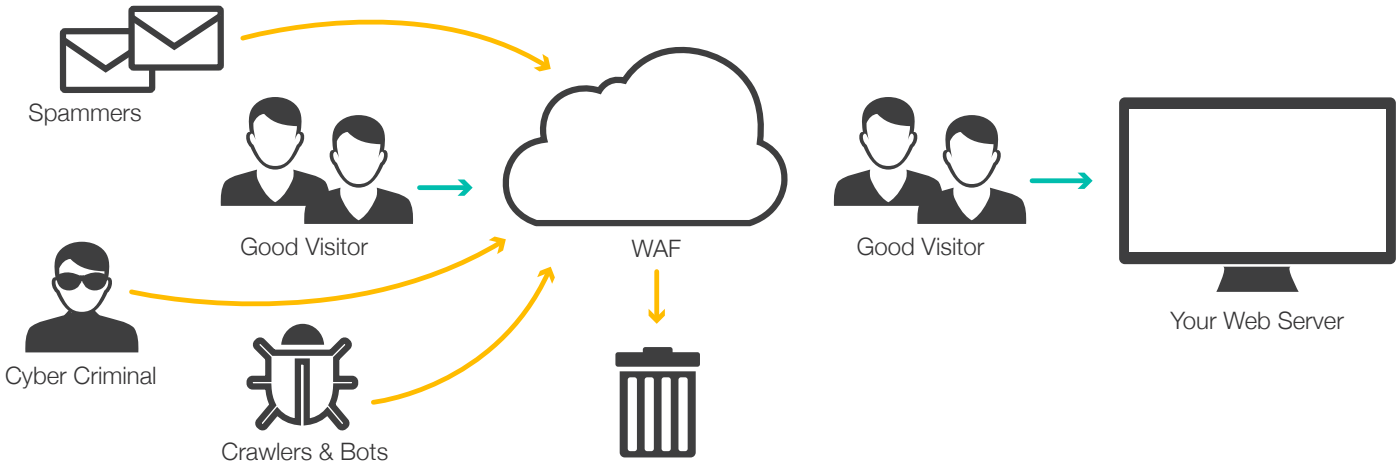
SECURITY SERVICES AG

CLUE

MANAGED APPLICATION PROTECTION

Today, modern web applications are exposed to a multitude of attacks from the Internet. To protect you from these threats, we use Web Application Firewalls (WAFs). This protection mechanism is placed between web applications themselves and the Internet. This prevents direct access to systems and controls any interaction taking place within web app.



PROTECTION FROM A TO Z

Whether web shop or news portal: Web applications are becoming more and more the target of attacks from the Internet. Due to insecure and faulty programming, or system components that are no longer supported, confidential and sensitive information is being exposed to countless attack possibilities. Hackers use automated tools to steal data, resell it or blackmail affected companies. The tendency is that these vulnerabilities are being totally missed or not sufficiently flagged by classic IT security systems, such as network firewalls or IDS/IPS systems – again, we have you covered.

EFFICIENT PROTECTION

A protective wall at the application level between the business function and its interaction on the Web is situated directly in the data center. As a result, web applications themselves are no longer directly accessible and the systems and databases behind them can no longer be attacked. More to the point, every access by users and all responses from web applications are checked and blocked if necessary.

FAST PROTECTION

It is true that with structured and security-oriented development methods, many weak points can already be avoided during the development of software or through the release of software updates. However, this simply cannot be guaranteed 100 percent. It is all too often the case that updates are a little late in closing problematic gaps or that released software is not always as secure as hoped for.
So, when protecting web applications, a combination of secure development and an upstream mechanism, that covers the entire attack surface, should always be used. For dev ops scenarios, the Web Application Firewall (WAF) integrates into such a process and can be seamlessly addressed and configured through the full API interface.

APPLICATION PROTECTION FEATURES

APPLICATION PROTECTION
Robust security mechanisms protect against targeted and automated attacks. Attacks documented in OWASP Top 10, such as SQL Injection and Cross Site Scripting (XSS), are automatically detected and logged. Granular rules can be implemented to manipulate, forward, block, or perform other actions.

IDENTITY MANAGEMENT
The first hurdle for unauthorized access is already created by upstream authentication. SAMLv2 and web-based single sign-on as well as LDAP, Radius and Azure AD compatibility simplify implementation and offer flexible user authentication.

REST-APIS
Many business applications also offer APIs for machine communication. These are often forgotten or neglected during security checks. Clue Application Protection fully secures mobile applications, JSON-based RESTful APIs and XML APIs.

COMPLIANCE
Clue Application Protection helps you to successfully meet compliance requirements based on PCI-DSS, HIPPA, FISMA or SOX guidelines. The mechanisms for the protection of web applications mentioned in PCI-DSS chapter 6.6 can be implemented according to required (legal) rules and regulations.

VULNERABILITY SCANNER INTEGRATION
It is a common practice to check web applications with a vulnerability scanner before and after implementation as well as during a penetration test. Clue Application Protection supports the automatic import of scan results to prevent detected problems from being directly in the policy.

MULTI FACTOR AUTHENTICATION
For strong user authentication, both Clue Multi Factor Authentication and other two-factor authentication services or certificates can be included.

REPORTING
Powerful reports help you assess the security level of protected applications and identify and address security incidents. These can also provide information on attack types, geolocation, and web traffic for SIEM systems.

DEPLOYMENT
Dedicated protection for your applications can be provided physically, virtually, and in private and public clouds.

APPLICATION PROTECTION SERVICE

Clue Application Protection combines the operation of a web application firewall with the complex protection of your web applications. Our security experts create a tailor-made policy based on your requirements, advise you on the optimisation of the software code and take over the operation of the required web application firewall. This includes regular back-ups, software release and lifecycle management as well as the monitoring of health and security events. Clue Application Protection can be used flexibly on all platforms and is supported and monitored by specialists with many years of experience in the field of application security.

CLUE-LESS?

Bolster your team with Clue Managed Services. Our security experts are a welcome addition to your business. Proven products, tailor-made features and your very own personal support - we meet your requirements at a low TCO. The monthly service fee eliminates high investments and training costs, enabling you to use our services in a modular way.

WHAT'S NEXT?

Do you use web applications such as web shops, customer portals, remote access portals or other critical applications in your company and want to protect them and know their current security level? Talk to us about an Application Security Assessment and the Application Protection Service. We would be pleased to advise you in the area of Application Security Assessment and Application Protection Service and to show you secure implementation adapted to your requirements.