cWatch

cWatch is a comprehensive website security solution developed by Comodo, designed to protect, monitor, and optimize online presence against various cyber threats. It integrates advanced technologies with human expertise to provide a robust security framework for businesses of all sizes.

1. **Web Application Firewall (WAF):** cWatch includes a fully managed WAF that filters incoming HTTP/HTTPS requests, blocking malicious traffic and protecting against threats such as DDoS attacks, SQL injection, and cross-site scripting (XSS).
2. **Malware Scanning and Removal:** The platform employs state-of-the-art malware scanning technology that continuously monitors websites for malicious code, ensuring immediate detection and removal of threats.
3. **Security Information and Event Management (SIEM):** cWatch provides real-time monitoring and analysis of security events, helping organizations to quickly identify and respond to potential threats.
4. **Content Delivery Network (CDN):** The integrated CDN accelerates website performance by caching content and delivering it from the nearest server, reducing latency and improving user experience.
5. **24/7 Security Monitoring:** cWatch offers continuous surveillance and incident handling by a dedicated team of certified security analysts, ensuring prompt response to any security incidents.
6. **User-Friendly Dashboard:** The platform features an intuitive dashboard that allows users to monitor their website's security status and performance metrics easily.

cWatch integrate a Web Application Firewall (WAF) with a Secure Content Delivery Network (CDN)

cWatch integrates its Web Application Firewall (WAF) with a Secure Content Delivery Network (CDN) to provide comprehensive website security and performance optimization.

Web Application Firewall (WAF)

The cWatch WAF acts as a real-time intrusion prevention system that analyzes, blocks, or filters malicious HTTP/HTTPS traffic before it reaches the origin server. It provides protection against various threats, including:

- SQL injection
- Cross-site scripting (XSS)
- DDoS attacks
- Brute-force attacks
- Malware and bots

The WAF is fully managed by Comodo's security experts, ensuring that it is continuously updated to defend against the latest vulnerabilities.

Secure Content Delivery Network (CDN)

cWatch's CDN accelerates website performance by caching and delivering content from the closest data center to the user. This reduces latency and improves the user experience. The CDN also provides additional security benefits:

- Layer 3-7 DDoS protection
- SSL/TLS encryption
- Geo-blocking and IP filtering
- Bot mitigation

By leveraging the CDN's global network of servers, cWatch can scale to handle sudden traffic spikes and protect against volumetric DDoS attacks.
Integrated Security

Key Features

1. By combining the WAF and CDN, cWatch creates a multi-layered defense system for websites.
2. The WAF filters out malicious traffic at the application layer, while the CDN provides protection at the network and transport layers.
3. This integrated approach ensures that websites are safeguarded against a wide range of threats, from SQL injection to DDoS attacks.
4. Additionally, cWatch's Security Information and Event Management (SIEM) system collects and analyzes logs from both the WAF and CDN to provide real-time threat detection and prioritization.
5. This allows the Comodo Cyber Security Operations Center (CSOC) to quickly identify and respond to potential security incidents.

cWatch's integration of a WAF and CDN, combined with its SIEM and CSOC, offers a comprehensive and effective solution for protecting websites from cyber threats while optimizing performance and user experience.

Sources:
https://enterprise.comodo.com/cwatch-network/
https://enterprise.comodo.com/cwatch-network/