1.4 mCloud WAF

Micron21 - 2025-03-18 - Section 1: Networks & Security

mCloud WAF

Experience unparalleled security and flexibility with our mCloud WAF service, powered by the advanced capabilities of NSFOCUS technology.

In today's digital landscape, web applications are the lifeblood of businesses, enabling critical functions such as customer engagement, transactions, and data exchange. As these applications become more sophisticated, they also become prime targets for cyber threats. Organisations that require absolute control and security over their web applications need a robust, dedicated solution that goes beyond standard protections. The mCloud Web Application Firewall (WAF) emerges as the premier choice for such organisations, offering unparalleled security features, comprehensive control, and the benefits of a dedicated appliance.

Provided as a dedicated Web Application Firewall appliance, mCloud WAF is designed to protect any Micron21 service—including mCloud Virtual Machine Instances, Colocation services, Dedicated Servers, and even externally hosted services. By deploying this dedicated appliance, you gain absolute control over your web application security infrastructure, ensuring robust protection against a wide range of cyber threats.

Our mCloud WAF integrates seamlessly with global threat intelligence feeds to automatically block known malicious traffic, keeping your services safeguarded against the latest threats. It offers comprehensive API protection, defending your APIs from a multitude of attacks by validating requests and enforcing strict adherence to protocols. The WAF's advanced behavioural analysis monitors user interactions in real-time, identifying and blocking malicious activities by analysing patterns and anomalies in user behaviour.

Enhancing your security further, mCloud WAF provides website defacement protection through page prefetch management. This feature ensures that even if your web server is compromised, the WAF can serve the correct, untampered content to your users by prefetching and caching clean pages. Our sophisticated bot protection employs patented technology and human-machine recognition mechanisms to effectively neutralise malicious bots. With dynamic encapsulation and dynamic obfuscation, the WAF prevents unauthorised crawling and submission of business data, protecting your information from being tampered with or harvested.

This licensed subscription product is tailored to your specific needs, with licensing based on the device's throughput capacity and the features you require. By choosing mCloud WAF you invest in a solution that not only addresses current security challenges but is also equipped to evolve with emerging threats.

The Imperative for Absolute Control and Security

While cloud-based WAF services like AWS WAF and Cloudflare WAF offer convenience and ease of deployment, they may not meet the stringent security and compliance requirements of organisations that handle sensitive data or operate in regulated industries. These services often involve shared infrastructure and limited customization, which can be a concern for businesses needing full control over their security environment. In contrast, deploying a dedicated WAF appliance like mCloud WAF ensures that all security measures are under the organisation's direct management, providing the highest level of protection and compliance.

mCloud WAF: The Ultimate Dedicated Security Solution

mCloud WAF is a comprehensive security solution designed to protect web applications from a wide array of cyber threats, including the most sophisticated attacks. By deploying mCloud WAF as a dedicated appliance, organisations gain complete control over their web application security infrastructure, ensuring that all policies, configurations, and data remain within their secure environment.

Key Features and Benefits

Comprehensive Threat Protection

mCloud WAF offers robust protection against known and emerging threats, including SQL injection, cross-site scripting (XSS), and other vulnerabilities listed in the OWASP Top 10. Utilising a combination of signature-based detection, behavioural analysis, and advanced security technologies such as machine learning and artificial intelligence, it identifies and blocks malicious activities in real-time. This multi-layered approach ensures that both known threats and zero-day exploits are effectively mitigated. Additionally, mCloud WAF leverages global threat intelligence feeds to automatically block known malicious traffic. By continuously updating its database with the latest threat information, it preemptively identifies and neutralises threats originating from blacklisted IP addresses, malicious domains, and other sources, significantly reducing the risk of successful attacks by stopping them at the perimeter.

Advanced Security Features

The WAF incorporates cutting-edge security technologies to enhance detection accuracy and reduce false positives. Its virtual patching capability provides immediate protection against known vulnerabilities, allowing organisations to secure applications before official patches are applied. mCloud WAF offers comprehensive API protection, safeguarding against a wide range of attacks targeting APIs, such as SQL injection, XSS, and unauthorised access. It validates API requests, enforces strict schema adherence, and monitors for abnormal patterns, ensuring that only legitimate traffic reaches your backend services.

Furthermore, the WAF delivers advanced bot protection mechanisms based on patented technology and human-machine recognition systems. By utilising dynamic encapsulation and dynamic obfuscation, it effectively neutralises malicious bots, preventing automated attacks like credential stuffing, web scraping, and denial-of-service attacks. It obfuscates business data, preventing unauthorised crawling and submission, and protects against tampering.

Behavioural Analysis

Understanding user behaviour is essential for detecting sophisticated threats that bypass traditional signature-based detection. mCloud WAF employs advanced behavioural analysis to monitor and analyse user interactions in real-time. By establishing a baseline of normal behaviour, it can identify anomalies indicative of malicious activity—such as credential

stuffing, session hijacking, or data exfiltration attempts—and block them effectively. This proactive defence mechanism enhances security by detecting and mitigating threats that might otherwise go unnoticed.

Website Defacement Protection and Page Prefetch Management

Website defacement can severely damage an organisation's reputation and erode customer trust. mCloud WAF offers robust website defacement protection through its page prefetch management feature. The WAF maintains a cache of clean, original web pages and can serve these to users even if the underlying web server has been tampered with. This ensures continuous delivery of authentic content while the compromised server is being addressed, minimising disruption and preventing the spread of malicious content.

SSL/TLS Traffic Inspection

mCloud WAF can decrypt and inspect SSL/TLS traffic, detecting threats concealed within encrypted connections. By offloading encryption and decryption tasks from web servers, it enhances overall system performance while maintaining secure communication channels. This capability ensures that encrypted traffic does not become a blind spot in your security posture.

Intrusion Prevention System (IPS) Integration

The WAF includes IPS features that detect and prevent vulnerability exploits by monitoring network traffic for malicious activities. This integration provides an additional layer of defence, safeguarding applications against a broader spectrum of threats. By combining WAF and IPS functionalities, mCloud WAF offers comprehensive protection that addresses both application-layer and network-layer attacks.

Granular Customization and Policy Management

mCloud WAF allows for detailed customization of security policies to meet specific organisational needs. Administrators can tailor rules based on application requirements, user behaviours, and threat landscapes. With advanced customization at a granular level, organisations have absolute control over their security policies, configurations, and data. This level of control ensures that security measures do not interfere with legitimate traffic, maintaining optimal application performance and user experience.

In contrast, cloud-based WAFs often offer limited customization, relying on predefined rulesets that may not cover all unique requirements.

Deployment Flexibility

Available as a hardware appliance, mCloud WAF can be deployed on-premises, providing complete control over the security environment. This is particularly advantageous for organisations with strict compliance requirements or those that prefer to keep their security infrastructure separate from cloud environments. The dedicated appliance ensures absolute control, essential for businesses that cannot compromise on security due to regulatory requirements or the sensitive nature of their data.

mCloud WAF supports various deployment modes, including reverse proxy, transparent bridge, and out-of-path (OOP), allowing seamless integration into existing network architectures. Additionally, for organisations subject to strict data protection laws, mCloud WAF enables compliance with data sovereignty regulations by ensuring that all data processing and storage occur within their controlled environment.

High Performance and Scalability

Designed for high throughput with minimal latency, mCloud WAF ensures that robust security does not come at the expense of performance. By residing within the organisation’s network, it reduces latency associated with cloud-based solutions. mCloud WAF ensures consistent performance and does not rely on external networks, which is critical for applications requiring high availability and responsiveness. Its scalable architecture can handle increasing traffic demands, making it suitable for businesses of all sizes. Load balancing capabilities further optimise performance, ensuring consistent protection even during peak traffic periods.

Comprehensive Reporting and Analytics

Detailed logs and reports provide insights into security events, trends, and compliance status. This information is crucial for auditing purposes and helps organisations meet regulatory requirements such as PCI DSS, HIPAA, and GDPR. The comprehensive reporting facilitates transparency and supports informed decision-making regarding security policies and incident responses.

Integration Capabilities

mCloud WAF can integrate seamlessly with existing security infrastructure, including Security Information and Event Management (SIEM) systems, intrusion detection systems, and other network security tools. This interoperability enhances the overall security posture and simplifies management by providing a unified view of security across the organisation. By integrating with other systems, mCloud WAF contributes to a cohesive and efficient security ecosystem.

mCloud WAF: A Comprehensive Security Powerhouse

NSFOCUS WAF is designed to protect web applications from a vast array of cyber threats by integrating advanced security technologies and offering extensive customization. Here are the key features and benefits that make NSFOCUS WAF the optimal choice for organisations requiring the highest level of security.

Real-World Applications

Organisations across various sectors can significantly benefit from NSFOCUS WAF's advanced features:

Financial Institutions: Protect online banking platforms and financial services from sophisticated attacks targeting APIs and user accounts, ensuring compliance with stringent regulatory standards.

Healthcare Providers: Safeguard patient data and healthcare applications against breaches, while complying with regulations like HIPAA through robust data protection and audit capabilities.

Government Agencies: Secure critical infrastructure and sensitive information with a dedicated WAF that meets high-security standards and provides defense against nation-state-level threats.

E-Commerce Platforms: Defend against bot-driven attacks, prevent website defacement, and ensure a secure shopping experience for customers, thereby maintaining brand reputation and customer trust.

Conclusion: mCloud WAF—The Ultimate Choice for Uncompromised Security

When absolute control and security are non-negotiable, mCloud WAF

stands as the superior choice. Its dedicated appliance model ensures that organisations have full ownership of their security environment, enabling them to implement tailored policies, respond swiftly to emerging threats, and comply with regulatory mandates.

By choosing mCloud WAF, businesses invest in a solution that not only protects against current cyber threats but is also adaptable to future challenges. Its advanced features, combined with high performance and scalability, make it the ideal choice for organisations that cannot afford to compromise on security.

In a world where cyber threats are constantly evolving, and the cost of a data breach can be catastrophic, having the right defences in place is crucial. mCloud WAF provides the comprehensive protection, control, and peace of mind that organisations need to operate securely in the digital age.

The Imperative for Complete Control and Security

While cloud-based WAF services provide convenience, they often lack the depth of control and customization that organisations with stringent security requirements demand. Industries such as finance, healthcare, and government agencies cannot afford to compromise on security or rely on shared infrastructures. A dedicated WAF appliance like mCloud WAF ensures that all security measures are under direct organisational control, providing robust defence mechanisms tailored to specific needs.