Digital Data GPU Enabled AI based WAF

DATASHEET

Key Benefits

GPU Enabled

AI Driven Threat Protection

OWASP top 10 rule set

Adaptive deep ML learning

Flexible Deployment

Advance Features

Drill down actionable dashboard

GPU based Appliances

Managed cloud WAF Services

Virtual Edition

Artificial Intelligence (AI) Powered Application Protection

With the increasing number of applications developed and used today, mainly through cloud technologies, organizations face more complex cyber threats. Application security measures are integral for protecting assets and sensitive data and reducing the impact of application-related cyber-attacks.

Application security is constantly evolving, and many changes have been made to application development and deployment. The widespread adoption of cloud computing has ushered in a new era of software applications designed and built to leverage the capabilities, agility, and flexible benefits of cloud computing. As a result, modern cloud applications are developed and deployed using cloud technologies in either single-cloud stack or multi-cloud environments.

Artificial Intelligence (AI) is critical for protecting against cyberattacks because modern, increasingly sophisticated threats move too fast and are too complex for traditional, human-led security measures to manage. AI enables proactive, real-time defense by analyzing massive datasets, identifying subtle anomalies, and automating responses.

Digital Data AI powered advanced Web Application Firewall (WAF) enhances traditional rule-based security with intelligence, AI-driven threat detection to address modern attack techniques that bypass static controls. While rule engines effectively block known threats, today's attacks rely on obfuscation, automation, and novel patterns that require adaptive protection beyond signatures.

The platform analyzes incoming web traffic at multiple levels, examining request structure, behavior, and contextual signals to accurately distinguish malicious activity from legitimate users. Designed to learn, adapt, and scale, the system continuously evolves by learning from real-world traffic, enabling it to detect threats before they become incidents.

This adaptive approach delivers highly accurate threat detection while ensuring legitimate traffic flows uninterrupted, Built for enterprise environments, the solution supports seamless integration, consistent policy enforcement, and compliance-driven deployments-providing adaptive web security for modern applications and precision defense designed for trust and mitigate bots, client-side protection (CSP), API protections, Login protection and defend against application denial-of-service (DoS).

The solution is GPU enabled to get real time performance benefits of deep Machine Learning modules to analyses complex cyber-attack and protect with zero false positive.

The Digital Data AI powered advance WAF is offered as an GPU based appliance, virtual edition, and as a managed service—providing automated WAF services that meet complex deployment and management requirements while protecting your apps with great precision.

.

OWASP Top Ten Coverage

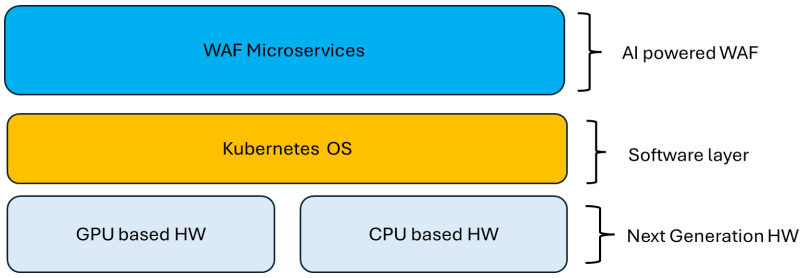
Key benefits

GPU enabled and Microservices Architecture

Digital Data WAF is designed on robust architecture to ensure the performance, scalability and availability for AI/ML based deep adaptive learning algorithms to protect against complex cyber-attacks. Microservices architecture offers significant advantages over traditional, monolithic software design, particularly for large, complex, and rapidly evolving applications. By breaking down software into small, independent, and loosely coupled services.

GPUs are the industry standard for training deep learning AI/ML models, enabling WAF to process massive datasets for proactive analysis, natural language processing, and neural networks to reduce false positive and provide better accuracy for zero-day protection.

The solution provides separate dedicated management plane for communicating between different micro services to ensure the isolation between user traffic and management traffic.



Comprehensive pre-defined Guard Rule Sets (GRS)

The Digital data WAF's Negative security mode used very comprehensive pre-defined Guard Rule Sets (GRS) block known malicious patterns and attack with great accuracy and minimum false positive and making it ideal for immediate protection for OWASP Top Ten and more. Negative Security models are well-suited for fast-moving environments or organizations that frequently update their applications.

It provides strong, pre-configured protection against common, well-known attacks, such as those listed in the OWASP Top 10 (e.g., specific SQLi or XSS signatures).

Digital data WAF provides a very flexible and AI enabled user-defined custom WAF rules set to detect and block specific, targeted attacks that are not covered by pre-defined WAF rule sets, such as proprietary application vulnerabilities, unique data leaks, or emerging threats. The core of the rule set, which can include simple strings or Regular Expressions to match against traffic.

While the negative model is excellent for stopping common threats, it is generally considered insufficient on its own for full protection against novel or zero-day attacks. Therefore, Digital Data WAF uses hybrid approach—using a negative security model for immediate, broad protection, paired with a positive security model with AI/ML capabilities to protect more sophisticated, unknown, or tailored attacks.

AI/ML based deep learning for Zero-day protection

Digital Data WAF's positive security and deep learning model provides effective zero-day protection by using a proactive, layered security approach that focuses on behavioral analysis rather than known signatures. AI/ML deep learning model establishes system behavior by analyzing traffic behavior and risk context in real time to stop sophisticated and previously unseen threats with precision.

A Character-level deep learning architecture used primarily in Natural Language Processing (NLP) that operates directly on characters rather than words or sub-words. It reads every tiny character, even symbols and hidden Unicode help to catch attacks even when attackers change spelling, break words, or hide code and detects suspicious substrings like wrong spelling, mixed case, broken tags and encoded characters.

Digital data WAF to have layered approach uses sequence-aware DL model. It is a type of Recurrent Neural Network (RNN) that doesn't just look at individual characters but remembers the order of inputs over time. It observes the sequence of characters or actions in a payload, even if an attacker splits their attack into multiple steps, can reconstruct the sequence and detect malicious intent.

Digital data WAF's AI/ML deep learning approach also uses in conjunction of the above deep learning models, which are a type of Deep Learning model designed to understand the context of input data, not just individual characters or sequences over time. It looks at all parts of the input at once and figures out which parts are important to capture long-range relationships and global context to detect and block semantic anomalies, structured payload attacks, and obfuscated payloads.

Digital data WAF does not rely on one model but uses all three models together. Each model gives its own risk/probability score (0 - 1) for a request or sequence then the combined score is calculated by merging their results, giving a more reliable and robust decision to achieve greater accuracy and zero false positive.

Application Programming Interface (API) protection

Application Programming Interfaces (APIs) are important because they enable seamless communication and data exchange between different software systems allowing businesses to drive innovation, improve efficiency, and expand their market reach.

Digital data WAF provide very comprehensive API protection against OWASP Top Ten Security vulnerabilities including GraphQL, REST/JSON, XML, and GWT APIs. It supports user authentication for enhanced validation and utilizes AI/ML based deep learning protection through rate limiting and behaviour analysis.

It provides the option for uploading manually Swagger latest version to avoid any false positive and configure policies using API-specific parameters. The Solution provides a predefined API security template that automatically applies WAF policies and automatically discover New API Paths, Shadow API Paths, Stale API Paths, Authenticated API Paths and unauthenticated API Path. API protection is improved through comprehensive authentication and token enforcement.

AI Powered Bot Guard.

Bot mitigation is the process of identifying, managing, and blocking malicious, automated traffic (bad bots) from accessing websites, applications, and APIs, while allowing legitimate traffic (good bots, such as search engine crawlers) to pass through. With over 50% of web traffic now driven by bots, effective mitigation is crucial to prevent resource overloading, data scraping, account takeovers, and fraudulent transactions.

Digital Data WAF rely on AI based deep learning Layered Security, a defense-in-depth approach, combining behavioural analysis, fingerprinting, and threat intelligence rather than relying on a single method like IP blocking. It Analyses user interaction in real-time—such as mouse movements, typing speed, and click patterns—to distinguish human

behaviour from automated, inhuman speed or precision. It also Identifies unique browser, device, and operating system attributes to create a signature for tracking, even if the bot

rotates IP addresses.

The solution challenges the client to execute JavaScript, which many simple bots cannot do, or uses CAPTCHA to verify human intent, though advanced bots can bypass these. It restricts the number of requests a single client can make within a specific time frame, slowing down or stopping scrapers and brute-force attacks and utilizes Threat intelligence databases of known malicious IP addresses and botnet signatures to pre-emptively block or flag suspicious traffic.

Advance Client-Side Protection

Digital Data WAF provides advance Client-side protection against attacks that execute in the user's browser. The client-side protection specifically targets supply chain attacks that exploit third-party JavaScript code, unauthorized scripts, and browser vulnerabilities.

The solution analyzes the behavior of scripts in real-time within the end-user's browser to identify suspicious activities, such as attempts to access sensitive data. It uses CSP headers to control which resources can load onto a page, reducing the risk of Cross-Site Scripting (XSS) and other code injection attacks.

It provides real-time protection of sensitive data such as credentials, credit card numbers, and personal information entered in web forms. The solution supports HTML field-level encryption and obfuscation to prevent data theft via malware, keyloggers, or man-in-the-browser attacks.

The WAF ensures secure transmission of sensitive fields even before HTTPS encryption is applied. Uses JavaScript injection to protect form fields dynamically without requiring application code changes. detect and block malicious scripts or unauthorized client-side code attempting to read or exfiltrate sensitive data. It prevents credential harvesting, form scraping, and overlay attacks by securing input fields at the browser level.

Advance Login Security

Digital Data WAF secures login pages by filtering, monitoring, and blocking malicious HTTP/S traffic, preventing unauthorized access, brute force attacks, and credential stuffing. It protects against OWASP Top 10 threats, including SQL injection and XSS, by analyzing requests in real-time and enforcing rules, such as IP whitelisting, rate limiting, and geo-blocking.

The Solution detects and blocks automated bot traffic trying to guess passwords and use JavaScript challenges, CAPTCHA, and human interaction algorithms to distinguish users from malicious bots. Brute-force attack prevention through rate limiting, login thresholds, progressive delays, and account lockout policies.

Credential stuffing detection and mitigation, using behavioral analysis, IP reputation, and integration with known leaked credential databases. It does suspicious login identification based on browser fingerprinting, OS type, user-agent behavior, and geolocation anomalies. It also provides Real-time alerting and logging for credential misuse patterns (e.g., password spraying, rapid login failures).

Intelligent HTTP Protocol Protection

Digital data WAF's HTTP protocol protection is used to protect data as it is transferred between a web browser (client) and a web server with layered approach. The primary security measure for data transmitted over HTTP is the use of HTTPS (HTTP Secure) and

HTTP to HTTPS redirection which uses Transport Layer Security (TLS) to encrypt communication between the client and server. This prevents eavesdropping and man-in-the-middle attacks. HTTP to HTTPS redirection for all unencrypted traffic, Adds/enforces secure headers

Other general HTTP security protection sanitizes and validates all data received in HTTP requests (headers, URL parameters, and body) to prevent common vulnerabilities as enforces HTTP protocol RFC compliance, Allows/blocklists HTTP methods (e.g., allow GET/POST, block TRACE/CONNECT/PUT), HTTP/2 and HTTP/3 inspection and enforcement, Traffic Normalization and Inspection, URL normalization and decoding to catch obfuscated/masked payloads. Restricts header names, length, count, and detects unusual headers, Limits request URI, query string, and parameter lengths, Enforces max request/response sizes (headers + bodies).

The solution Inspects and validates cookie names, patterns, and usage. optionally masks or encrypt session cookies to prevent theft. The Anomaly and Evasion Detection engine detects malformed or out-of-spec HTTP requests (e.g., null bytes, illegal chars). Flags header injection, smuggling, and splitting attempts. Recognizes suspicious behavior as unusual header ordering, excessive headers, or line folding and WebSocket Inspection.

Advance JSON protection

JSON (JavaScript Object Notation) is a widely used, lightweight data interchange format that is generally secure on its own, but it becomes vulnerable depending on how it is parsed, transmitted, and handled in applications.

Digital Data WAF provides JSON protection through dedicated JSON parser to inspect complete payloads, including nested objects and binary data. The solution does the schema validation to enforce expected keys, value types, and data structures. Detection of malformed JSON and evasion techniques (e.g., invalid syntax, oversized payloads).

The solution provides granular policy enforcement on allowed URLs, parameters, methods, and JSON object fields, Control over wildcards and HTTP methods to prevent abuse of REST APIs. Inspection of embedded or binary-encoded data within JSON (e.g., Base64), Rate limiting and anomaly detection to mitigate automated JSON abuse

Advance XML protection

Digital Data WAF provide advance XML Security as a comprehensive set of standards, protocols, and best practices designed to protect XML (extensible Markup Language) documents and data from unauthorized access, modification, and exploitation. It is critical because XML is widely used not just for data interchange, but for configuration files, build manifests (like Maven pom.xml), and API payloads (SOAP).

The solution validates incoming XML requests against defined XML schemas (XSD) to detect malformed or unauthorized XML structures. It prevents XML External Entity (XXE) attacks and supports XPath detection, ensuring malicious queries embedded within XML payloads are blocked. Identifies and blocks schema-less or unexpected XML traffic using behavioral learning and rule set. It inspects embedded XML within SO AP envelopes for SOAP-based web services and APIs,

Large Language Model (LLM) Applications Protection

Digital Data WAF extends protection to AI-powered applications, chatbots, and LLM-driven APIs by detecting prompt injection attempts, indirect prompt manipulation, data exfiltration patterns, and token abuse attacks. The platform analyzes inbound prompts and outbound model responses to identify semantic anomalies, hidden instruction overrides, and

malicious payload injection. Advanced rate controls and behavioral scoring protect LLM APIs from automated abuse, scraping, and cost-exhaustion attacks. This ensures secure deployment of Generative AI applications while maintaining application integrity and data confidentiality."

Comprehensive Access Control list.

Digital data waf provides a very comprehensive Access Control List (ACL) which is a foundational security component that defines a set of rules used to monitor, filter, and control incoming HTTP/HTTPS traffic for web applications. It acts as a security filter, determining which requests are allowed to reach your application and which should be blocked based on specific conditions.

The solution defines conditions such as IP addresses, HTTP headers, URI strings, Geo locations that identify malicious or unwanted traffic. When a request matches a rule, the WAF takes an action, such as Allow, Block, or Count (monitors without acting). The default Action is that requests do not match any of the specifically configured rules (usually set to Allow or Block) that is black or white access list.

Advance Application (L7) DDoS Protection.

Digital data WAF provides a very comprehensive Layer 7 (Application layer) Distributed Denial-of-Service attacks for user-facing applications, websites, and APIs operate. These attacks aim to crash servers by overwhelming them with seemingly legitimate requests, such as HTTP GET or POST, which consume significant CPU and memory resources.

Key Characteristics of L7 Attacks, Low and Slow, unlike volumetric attacks (Layer 3/4) that flood network bandwidth, L7 attacks often use fewer resources to create a large impact, often flying under the radar of traditional network security. They specifically target the application stack, such as web servers (Apache, Nginx) or database connections. Common L7 Attack Methods HTTP/HTTPS Floods,

SlowLoris that opening multiple connections to a target web server and holding them open as long as possible, eventually exhausting the server's maximum concurrent connection pool. API Abuse: Repeatedly calling specific API endpoints to cause service crashes.

Enhanced SSL offloading

SSL offloading is used for security devices primarily to inspect encrypted traffic for threats that would otherwise be hidden from deep packet inspection. Because over 90% of web traffic is encrypted, attackers often use SSL/TLS tunnels to hide malicious code. Once the SSL traffic is decrypted, it is passed through a Web Application Firewall (WAF) blocking malicious code that is disguised in HTTPS.

Digital data WAF used the dedicated SSL hardware acceleration for cryptographic operations for better performance because encrypting and decrypting data is CPU-intensive. The solution provides simplified Certificate Management for managing SSL certificates on dozens or hundreds of individual web servers, certificates are managed in one central location and reduce the risk of misconfiguration or neglected renewals.

Centralizing SSL allows security administrators to enforce uniform, up-to-date TLS versions 1.2 and 1.3 and cipher suites across the entire organization.

In cloud deployments, sometimes it is not possible to deploy private key to decrypt the traffic, Digital data WAF utilizes the Automatic Certificate Management Environment (ACME) protocol, used by Let's Encrypt, relies on "challenges" to validate that a request for

certificate is authorized by the domain owner. The DNS-01 challenge is a popular method, especially for wildcard certificates or when a server is not publicly accessible over HTTP.

Flexible Deployment

The Digital data WAF provides a very flexible deployment for complex environments

A SaaS-based solution, often integrated with a Content Delivery Network (CDN) or through DNS changes, allowing for rapid deployment and automatic, 24/7 updates and with complete managed services by Digital Data security experts including emergency response team to manage the complex attack situation.

Network-based WAF (Hardware/Virtual Appliance) to position on-premises within the local network infrastructure. This model offers high-performance throughput, low latency, and full control over configuration including GPU for faster AI/ML deep learning algorithms in near real time.

The solution also provides reverse proxy mode, Bridge mode and TAP (SPAN) mode i.e. out of path mode.

Hybrid WAF: Combines on-premises appliances for sensitive, high-speed, local traffic with cloud-based services for edge protection against DDoS and bot threats.

Actions

The Digital data WAF provides a different action as ability to log or block requests and responses, Block the application user, or IP address. The solution generates unique identifier transaction to track attack event and mask the sensitive data for regulatory compliances.

AI Powered drill down dashboard

Digital Data WAF uses AI powered dashboard as a centralized monitoring interface that provides real-time visibility into the security posture of your web applications. It summarizes traffic data, identifies ongoing attacks, and tracks the effectiveness of your security rules

The solution provides real time and historical data for OWASP TOP ten Compliance, PCI compliance. The dashboard provides holistic and interactive interface that clearly measures the security posture with high level of visibility with drill down capabilities.

The solution provides historical attack log display, access logs, Filtering and searching on key fields, Co-relation for complex attack patterns, Geo location-based display, Top source, Top destination, Option to exclude the signature. The solution captures complete attack details – request, response and payload for deep investigation and analysis the attack.

AI driven centralized Policy Management

Digital data WAF provides a AI based powerful centralized policy management involves configuring, deploying, and maintaining security rules to protect web applications from threats including defining rules, setting modes (Detection vs. Prevention), and managing rule sets.

The WAF policy acts as a container for all security settings to build a base policy and inherit child policies from the same. Inheritance to support restricting modifications to the base policy settings. The Security Policy applied per application, rather than one single policy for an entire system.

The Policy narrows down to each URI for same URL if required and provides different WAF policy and WAF rules set based on URI, URL based real service, detailed parameters control for each feature. The solution provides AI based suggestions for enhancing the security aspect of the policies.

Comprehensive Threat Intelligence

The Digital data WAF provides very comprehensive Threat intelligence to provide evidence-based information regarding existing or emerging cybersecurity threats targeting an organization. It provides the context, such as who is attacking, their motivations, their capabilities, and the specific indicators of compromise (IoCs) to look for. By understanding these factors, organizations can shift from a reactive security posture to a proactive and predictive one, enabling them to anticipate and block attacks before they occur.

AI used to automate threat data collection and analysis, reducing the burden on human analysts. Reputation Threat Intelligence provides a continuously updated, real-time stream of indicators—such as IP addresses, URLs, domains, and file hashes—that are assessed for trustworthiness to enable proactive blocking of cyber threats.

Role based Administration

The Digital data WAF provides a very comprehensive Role-Based Access Control (RBAC), that restricts system access to authorized users based on their defined role within an organization. Instead of assigning permissions to individual users, administrators assign permissions to roles and then assign users to those roles.

This approach streamlines access management, enhances security, and aids in regulatory compliance. The solution provides two factor authentication for layered security and enforces the principle of least privilege, ensuring users only have access to the resources necessary for their job.

Scheduled predefined security reports

The Digital data WAF provides scheduled reporting including automated generation and distribution of reports at predefined times or intervals, allowing for consistent performance monitoring without manual intervention. These reports are typically delivered to stakeholders via email or saved to a shared folder in formats such as PDF, CSV, Excel, or HTML.

Digital Data Basic and Advanced WAF Features and Specifications

Features	Basic WAF	Advance WAF
WAF rule set	Yes	Yes
Dashboard	Yes	Yes
Access control List (ACL)	Yes	Yes
Role Based Administration	Yes	Yes
L 7 DDoS Protection	Yes	Yes
Logging and reporting	Yes	Yes
Policy Management	Yes	Yes
SSL Offloading	Yes	Yes
Actions	Yes	Yes
Threat Intelligence	Yes	Yes
SaaS deployment	Yes	Yes
On Premises Deployment	No	Yes
GPU Enabled	No	Yes
AI/ML Deep Algorithm	No	Yes
API Protection	No	Yes
XML Protection	No	Yes
JSON Protection	No	Yes
Client-Side Protection	No	Yes
HTTP Protection	No	Yes
Emergency response team	No	Yes

Digital Data Enterprises ,15th Floor,
Oberoi Exquisite, Ciba Road,
Goregaon East, Mumbai,
Maharashtra 400063