Citrix Application and API Security

Citrix Application and API security solution is a comprehensive, FIPS-certified solution that offers protection against a broad range of security threats from network to web application layer.

Citrix Web App Firewall threat protection includes, but is not limited to:

- SQL injection
- Cross-site scripting
- Cookie tampering/stealing
- Form validation and protection
- Signature and behavior-based protections
- Virtual Patching
- HTTP and XML reply and request format validation
- JSON payload inspection
- AI/ML Based zero-day attack protection
- Bot Management
- API Security: Rate Limit, Auth, Threat Protection
- Data loss prevention (DLP) support, including the monitoring of traffic for intended and unintended data exposure
- DoS protection: Authentication, authorization, and auditing support and reporting
- Policy tools that provide for easier PCI-DSS compliance verification
- Centralized controller
- Detailed Analytics
- SIEM Integrations

The Citrix application and API security solution is a layered security solution that comprises of a full-featured Web Application Firewall (WAF), bot management, API gateway and SSL termination to protect web applications & APIs across multi-cloud deployments. It is available across all form factors (including virtual, hardware, public cloud IaaS and containerized) and can be easily consumed as a cloud WAF through Citrix Application Deliver Management (ADM) service. These various deployment form factors and modes ensure a consistent security posture across clouds, private DCs, and application architectures including 3-tier and Kubernetes based microservices.

Addressing Application Security Challenges

Applications and APIs are valuable business assets. It is reported that the overwhelming majority of security vulnerabilities are in the application, which means they are also the most vulnerable asset. Applications are attractive targets for cyber criminals because they have direct connectivity to databases of sensitive data. A comprehensive solution that combines WAF, bot management and API gateway functionality is required to mitigate the combination of threats prevalent today.

Holistic, Integrated, and Layered Solution

The Citrix application and API security solution provides holistic, proven and layered protection for all your applications. The integrated solution layers WAF, bot management and API protection and gateway as well as comprehensive analytics and cloud-based control to offer comprehensive protection against modern cyber threats.

Simplicity of a Single License

The Citrix application and API security solution offers a single license approach, that includes all security features (WAF, bot mitigation, API protection, SSL/TLS) which brings simplicity and reduces TCO.

Operational Consistency Across Clouds

The Citrix Application and API security solution is available in a variety of form factors with the same code base and controlled, centrally by Citrix ADM Service. This enables you to ensure operational and security consistency across your

WAF, bot management, API gateway, and SSL/TLS capabilities are included in a single Premium license and available across all form factors.

applications wherever you deploy them - on premises, public cloud or a cloud-based WAF - helping you overcome security barriers and maintain a consistent security posture on the journey to multi cloud.

Centralised, Cloud-Based Controller to Manage Your Security Posture Across Your Multi Cloud

With Citrix ADM Service as the control plane you can control your Web application security from the cloud and get real-time insight into the security of all your applications holistically and ensure compliance with you corporate and regulatory standards (e.g. PCI-DSS; HIPPA).

Citrix Web Application Firewall: Proven Robust Security

Citrix WAF provides proven, robust security to all your applications types wherever you choose to deploy them. Citrix WAF is a mature product deployed in thousands of customer environments, constantly evolving to enhance protection and security performance.

Hybrid Security Model to Protect Against Known and Unknown Attacks

The Citrix WAF employs a hybrid security model with thousands of signatures to filter out known attacks quickly and a learning mode that mitigates unknown attacks by monitoring user interactions and learning your application behavior. This positive security model is the only proven approach to deliver zero-day protection against unpublished exploits. Citrix WAF also uses machine learning techniques to detect behavior-based attacks including business logic abuse and Layer 7 DDoS.

Easier Deployment and Simple to Keep up to Date

Citrix WAF is easy to purchase and deploy, which helps you secure your applications quickly. The single license gives you all the protections you need for your apps with no other devices required.

The simple stepwise deployment means that you can enable the default protections to defend against the most common threats and add more advanced protections as you need them.

Session aware: Citrix WAF is session aware and secures dynamic elements like cookies, form fields and session-specific URLs. It also defends against attacks that target the trust between the client and server, including request forgery by checking for a unique ID inserted by Citrix. Such protection is imperative for any application that processes user-specific content, such as an e-commerce site.

Application learning: To ensure security measures are compatible with any application, Citrix Web App Firewall learning capabilities help the administrator create managed exceptions and relaxations when the application's intended—and legal—behavior might otherwise cause a violation of the default security policy. This helps reduce the number of false positive dramatically.

Scanning tool integration: Citrix WAF integrates with the leading vulnerability scanning tools - Rapid 7, IBM, Qualys, White Hat - so you can convert scan results into WAF configurations to set up protections quickly and easily.

IP reputation service: IP reputation provides a continuously updated list of malicious IP addresses in near real-time, providing an additional layer of protection and helping to reduce the burden on security teams. Rather than relying on static, rapidly out-of-date public black lists, IP reputation automatically analyzes and correlates feeds from millions of global sensors in real-time. The IP reputation feature is built into the platform and is available at no extra cost with the Citrix WAF solution. No service contract, no yearly renewals necessary.

Industry-Leading Performance

The rise of encrypted traffic on the internet means that cyber threats are increasingly hidden in encrypted traffic.

SSL performance: Citrix WAF has industry-leading SSL decryption performance built in, which enables you to intercept and inspect all application traffic.

Scale security inspection: The Citrix Application and API security solution will decrypt traffic prior to inspection by other security devices (e.g. NGFW, IDP/IPS). This dramatically scales traffic inspection by removing the burden of decryption from security devices which are not designed to handle the process effectively. This results in smaller/fewer, and hence lower cost, firewalls, IDS and AV/DLP inspection devices but it also enables you to mirror traffic to recording systems for compliance and auditing purposes.

Other accelerations techniques are also used (TCP connection management, compression and integrated caching), all of which improve the performance of the application while still applying full WAF functionality.

Meeting PCI Compliance and Auditing Requirements

PCI-DSS Compliance: Citrix WAF is used by many customers to ensure they meet their compliance requirements for their payment card transactions.

Citrix WAF can be used to meet the Payment Card Industry Data Security Standard (PCI-DSS) requirements that stipulate that the deployment of a WAF in front of public-facing applications is a suitable method of maintaining a proper security posture.

To support this further Citrix WAF generates dedicated reports that detail all the security protections defined in the WAF policy that pertain to PCI-DSS. Additionally, Citrix WAF can prevent the inadvertent leakage of sensitive data, like credit card numbers, by removing them or masking them, prior to sending a response.

Defeating XML-Based Threats

Citrix Web App Firewall includes a rich set of XML-specific security protections. These include schema validation to thoroughly verify SOAP messages and XML payloads, and a powerful XML attachment check to block attachments containing malicious executables or viruses. It also thwarts a variety of DoS attacks, including external entity references, recursive expansion, excessive nesting, and malicious messages containing either long or a large number of attributes and elements.

Protect Your Applications against Bot Attacks

A large portion of internet traffic is generated by bots. This additional interaction can put a strain on your resources and drive up your costs when using cloud infrastructure. More than this, bots are used to abuse your applications and carry

out malicious activity against your websites. Bot management is a component of the Citrix application security solution and helps mitigate the effect of bad bots. You can defend your site against many different types of bot attacks. For example:

- L7 DDoS attacks
- Account takeover attacks
- Screen scraping attacks

Bot Detection

Citrix bot management detects bots through a variety of techniques depending on the sophistication of the bot attack.

IP address detection methods: The simplest methods revolve around the IP address of clients.

- **Blacklist and whitelist:** blacklist of known bad bots ensure they are not allowed into your site. Whitelist good bots (e.g. comparison sites, search engine crawlers etc.) and allow access as they can be beneficial and promote your business.
- **IP reputation:** Citrix Application and API security solution has a built in IP reputation filter that updates dynamically as new bot threats are discovered.
- **Geolocation data:** determine the location of the client via the IP address.

Sophisticated bot detection techniques: Citrix Application and API security solution employs additional techniques to identify bot traffic.

- **Signatures:** Request header information (IP address, source domain, user agent) is used to create a signature database of 3,500+ known bots. Incoming requests are checked against this to identify bot traffic.
- **Fingerprinting:** 34 different parameters, such as browser plugins, fonts, user agents and screen resolution, are used to construct unique fingerprints for client devices. Humans and bots have different identifying criteria and the fingerprint will identify more sophisticated bots.
- **Behavior analysis:** Sophisticated bots emulate humans well. Citrix uses machine learning to establish your applications characteristics then spot behaviour anomalies to detect bots.

Bot Mitigation

Citrix provides a variety of mitigation mechanisms to prevent bots straining your infrastructure and protect your applications from abuse.

- **Block:** Drop incoming traffic requests from a bot
- **Redirect:** Divert requests to an alternate quarantined zone for further analysis - e.g. a honeypot server
- **Rate limit:** Limit the rate of requests from a client to prevent back end resources being overwhelmed
- **Challenge:** Issue a challenge CAPTCHA to clarify and avoid false positives

Bot Traffic Analytics

Determining whether traffic is human or a bot has other benefits. Citrix ADM's bot insight can examine the bot to human request ratio and normalize important business intelligence data skewed by bot traffic for clearer decision making.

Protect Your APIs with Citrix

Applications are becoming API-driven, which leads to greater efficiency of communications and innovation but creates exposure for cyber-attacks. The Citrix Application and API security solution provides comprehensive protection for your APIs so that you can secure your valuable application and data assets.

Comprehensive Protection for your APIs

As a gateway and proxy, the Citrix application security solution sees all requests and responses between applications and is able to intercept, check and monitor API communications. Several run-time features are available to protect an application's APIs.

- **Whitelisting and blacklisting:** Create lists of IP addresses that are specifically allowed or blocked from making an API call to an application.
- **Authentication:** Authenticating API calls ensures only permitted devices to communicate, which protects against the abuse and misuse of APIs.
- **Authorization:** Enforce which applications can communicate and which API calls they can make.
- **Rate limiting:** Throttle the rate at which API calls are received to prevent overwhelming back end resources.
- **Encryption:** Uses TLS to encrypt the APIs to protect the data in transit between the client and the API server.
- **Content routing:** A rich stack of content routing capabilities is available for APIs, like load balancing, GSLB and content switching to ensures each API call reaches the best destination for processing.

With these protections, and the integrated Web Application Firewall (WAF) and bot mitigation modules, Citrix Application and API security solution is able to provide comprehensive API protection for all your application types including against the OWASP top 10 for APIs–e.g. SQL injection, buffer overflow protection, JSON threat protection.

Secure your Microservices-Based Applications

Modern, cloud native applications have functionality distributed among independent microservices, which allows faster innovation, quicker time to market, easier scalability and better portability. It is a complex architecture and requires specific security measures.

Citrix web application security solution provides a rich set of integrated security features - WAF, bot management, SSL termination and API Gateway functionality to protect your microservices-based applications from attack.

Protect N-S traffic: The Citrix Application and API security solution can act as an ingress proxy and intercept and inspect traffic as it enters your Kubernetes cluster. Encrypted traffic can be decrypted and inspected with the various security modules (WAF, bot management etc.) to protect your applications against the OWASP top 10 security threats.

Protect E-W traffic: Because of the multiple form factors, a containerised version of the Citrix solution can be deployed inside your Kubernetes cluster. You can use the runtime protections e.g. mutual TLS, rate limiting etc. to protect your E-W traffic.

Integration with Istio: The Citrix solution integrates with the Istio control plane in service mesh environments either as a gateway or sidecar proxy. Define your policies with Istio and have them enforced by Citrix.

Offload security functions to sidecars: Handling security functionality on the Citrix sidecar proxies - like mutual TLS, circuit breaking - alleviates the load on the microservices themselves. This creates a simpler, more consistent codebase that is easier to manage and update and reduces security errors.

Centralised, Cloud-Based Control and Management Plane

Citrix Application Delivery Management (ADM) service enables you to deploy, manage, monitor, and troubleshoot your entire global application and API security infrastructure from a single, unified, and centralized cloud-based console. With Citrix ADM service, there is nothing to install or maintain, it's always securely patched and the latest features are always available. Further, as a cloud services Citrix ADM is always reachable and you can make changes even when you cannot visit your own data centers.

Deploy and Configure your Application and API Security Devices Centrally

Citrix ADM service talks directly to all your Citrix Application and API security devices wherever they are deployed—on prem; public cloud—and enables you to configure them all centrally.

Config jobs: Create and reuse configuration jobs to push security policies across all your devices as required.

Stylebooks: Automate configuration with stylebooks to ensure consistent security posture across your multi cloud and simplify and secure application migration.

Config audit/Config diff: Check configs against corporate definition for compliance.

Config alerts: Alert on missing security configurations for a particular application (e.g. missing WAF rules). Similarly, Citrix ADM will assess the configuration of the system security settings on individual devices and alert you if anything is not set correctly.

Autoscale: Automatically scale your application and API security devices to meet demand.

SSL Dashboard: Enables you to define, monitor and enforce SSL Policies across all your Citrix application and API security devices from a central point.

- Set acceptable SSL protocols, cipher suites and key strength
- Track all SSL transactions across your applications
- Track expired and install new SSL certificates centrally from Citrix ADM
- Analyse historical SSL transactions to explore the impact of SSL configuration changes

Holistic Visibility Across Multi Cloud with Simplicity of a Single Pane of Glass

Citrix ADM service collates security telemetry data from every Citrix Application and API security device and uses data analytics engines and the latest AI/ML techniques to provide actionable security insight about your applications, infrastructure and networks across your entire multi cloud. With Intuitive dashboards you can visualise your security posture at a glance.

Security insight: Shows at a glance what attacks your applications face both on aggregate and for each individual application. From a single dashboard you can easily see:

- Number and type of violations
- Details on the origins of the attacks (by IP address and geolocation)
- Which applications are most at risk so you can prioritise your remediation

Bot insight: Alerts you to the types of bot attacks your applications face, where they originate, their severity and how your systems reacted to them.

- See which bot detection mechanism was triggered
- See the actions taken (Drop, rate limit, redirect, challenge)
- Calculate the proportion of bot to human traffic to normalise business intelligence data

API Analytics: Citrix ADM brings presents insight into you applications API usage on aggregate or into individual APIs. View API requests, responses, data transmitted, origin of each API call (by IP address and Geolocation) and more. Also analyse additional security data at a glace:

- Authentication success and failures for each API
- Rate limiting actions taken
- Monitor the TLS protocols, ciphers and key-strengths used

AI/ML-driven Analytics for Faster Troubleshooting

The interactive nature of Citrix ADM enables you to drill into security issues for individual applications aggregated across your multi cloud environment to discover root causes and explore remediation.

Role based dashboards: Provide security ops teams with data based on their role in your organisation. This may be per security feature (e.g. SSL management; WAF policy management) or per application etc. Read-only roles can also be created.

AI/ML driven analysis: Automatically generate application baseline behaviour and identify anomalies that are note visible through manual analysis

- Detect account takeover attacks by ratio of successful to failed login attempts
- Detect anomalous download activity
- Detect lookup requests for non-existent domains
- Detect layer7 DDoS attacks based on clients, sessions and Geos

Citrix ADM service provides you with the centralised control and management plane to secure, monitor and troubleshoot your application and API security quickly and effectively and helps you maintain a consistent security posture for all your applications across your entire multi cloud environment.

Citrix Web Application Firewall Technical Aspects

Protects Online Revenue Sources

- Buffer overflow
- CGI-BIN parameter manipulation
- Form/hidden field manipulation
- Forceful browsing protection
- Cookie or session poisoning
- Cross-site scripting (XSS)
- Cross-site request forgery
- Command injection
- SQLinjection
- Error triggering sensitive information leak
- Insecure use of cryptography
- Server misconfiguration
- Back doors and debug options
- Rate-based policy enforcement
- Well-known platform vulnerabilities
- SOAP array attack protection
- Content rewrite and response control
- Content Filtering
- Authentication, authorizating and auditing
- L4-7 DoS protection

Simplified Management and Deployment User Interface

- Secure web-based GUI
- SSH-based CLI access network management
- SNMP
- Syslog-based logging
- PCI-DSS compliance reporting tool
- AppExpert Templates for Web Interface and Microsoft SharePoint
- Import/export Application Firewall profiles
- Convert third party application vulnerability tool output to Citrix rules
- Quick deployment of new rules from Common Event Format (CEF) logs

Comprehensive Web Server and Web Services Security

- Deep stream inspection; bi-directional analysis
- HTTP & HTML header and payload inspection

- Full HTML parsing; semantic extraction
- Session-aware and stateful
- HTTP Signature scanning
- Scan thousands of signatures
- Response side checks
- Protocol neutrality
- HTML form field protection:
  - Required fields returned; no added fields allowed; read-only and hidden field enforcement
  - Drop-down list & radio button field conformance
  - Form-field max-length enforcement
  - Cookie protection – Signatures to prevent tampering; cookie encryption and proxying
  - Legal URL enforcement – Web application content integrity
  - Full SSL offload:
    - Decrypts traffic prior to inspection; encrypts traffic prior to forwarding
    - Configurable back-end encryption
    - Support for client-side certificates
  - XML data protection:
    - XML security: protects against XML denial of service (xDoS), XML SQL and Xpath injection and cross site scripting
    - XML message and schema validation, format checks, WS-I basic profile compliance, XML attachments check
  - URL transformation
  - WSDL scan prevention to protect unpublished APIs
  - Support for Chunked POST requests

Bot Detection Techniques

- IP address blacklisting/whiltelisting
- IP reputation filtering
- Geolocation
- Bot signatures
- Device fingerprinting
- AI/ML Based Bot detection

Bot Mitigation Actions

- Drop client requests
- Redirect client to alternate (honeypot) destination for further analysis
- Rate limit connections
- Challenge with CAPTCHA

Comprehensive API Protection

- Whitelisting and black listing
- Authentication
- Authorization
- API rate limiting
- API session Encryption
- API Content routing
- API Threat Protection with WAF & Bot

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States