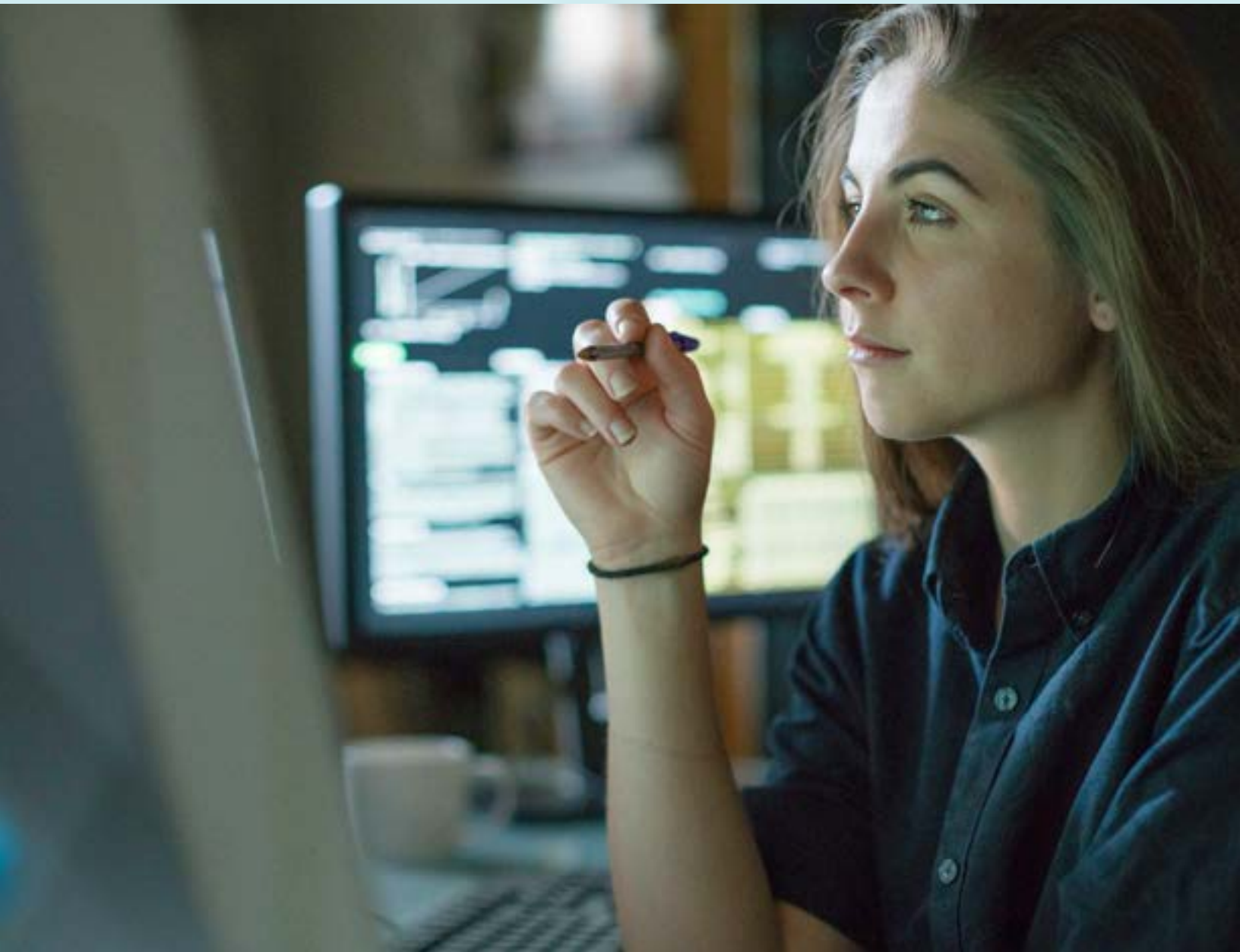
citrix

White Paper

Secure your applications with Citrix ADM service and Splunk

Exporting application-layer threats to Splunk dashboards for better visibility, rapid detection, and intervention



Citrix Application Delivery Management service **(Citrix ADM service) gives security operators new levels of visibility and intelligence into complex and evolving application-layer threats, with easy export of security violations to the Splunk dashboards they already use.**

Citrix ADM and Splunk Enterprise

Complex threats at the application layer

Most security operations are well versed in traditional security, protecting networks from internal and external threats and validating access from a host of remote devices. Unfortunately, threats leveled at the application layer have grown increasingly aggressive and sophisticated. Layer-7 distributed denial-of-service (DDoS) attacks, SQL injections, Slowloris attacks, and others target application services directly, leading to performance problems, data theft, instability, and unacceptable application downtime.

Worse, hackers exploit the large attack surface of the application layer to rapidly evolve their attack strategies. Bots and other automated mechanisms can efficiently attempt account takeovers from login pages or scrape website content. Traditional security approaches may miss these threats, especially if application-layer security solutions don't integrate well with dashboards commonly used by security professionals.

Citrix ADM closes this gap by providing advanced network, web application firewall (WAF), and bot security violation detection. Innovative machine learning (ML) algorithms let Citrix ADM proactively detect more sophisticated attacks and learn from evolving attack strategies. In addition to reporting violations to the Citrix console, Citrix ADM can now forward detected violations directly to Splunk Enterprise security dashboards. The result is greater application-level security awareness, better operational security, and safer and more reliable application infrastructure.

Citrix ADM: holistic visibility and actionable insights

Citrix ADM service provides an easy and scalable cloud-based solution to manage Citrix Application Delivery Controler (Citrix ADC) deployments.[1] Citrix ADM service can manage, monitor, and troubleshoot the entire global application delivery infrastructure from a single, unified, and centralized console. The service provides all the capabilities required to rapidly set up, deploy, and manage application delivery in Citrix ADC deployments, adding rich application health, performance, and security analytics.

Citrix ADM service is available on the Citrix Cloud. Agents enable communication between Citrix ADM service and the managed instances in your data center. The agents collect data from the managed instances in your network, sending it to Citrix ADM service and providing the following benefits:

- **Agility**. Since Citrix ADM service is cloud-based, it is easy to operate, update, and use. Frequent updates coupled with an automated update feature enhance your Citrix ADC deployments.
- **Faster time to value**. Unlike traditional on-premises deployments, administrators can configure Citrix ADM service with a few clicks. Adopters save installation and configuration time and avoid wasting time and resources on potential errors.
- **Multisite management**. With Citrix ADM service, you can manage and monitor Citrix ADCs across various types of deployments. The service offers one-stop management for Citrix ADCs deployed both on-premises and in the cloud.
- **Operational efficiency**. Citrix ADM service provides an optimized and automated way to achieve higher operational productivity. Organizations save time, money, and resources over maintaining and upgrading traditional hardware deployments.

1 Citrix ADC deployments include Citrix ADC MPX, Citrix ADC VPX, Citrix Gateway, Citrix Secure Web Gateway, Citrix ADC SDX, Citrix ADC CPX, and Citrix SD-WAN appliances that are deployed on-premises or in the cloud.

Powerful analytics with Citrix ADM service

Modern application infrastructure generates massive amounts of data. Effectively harnessing that data can help teams create better and more personalized user experiences by ensuring that applications perform properly, routine tasks are automated, and future trends are forecasted accurately. With Citrix ADM service, powerful machine learning algorithms continuously learn what normal usage looks like and identify malicious behavior rapidly. Machine learning is essential for transforming massive amounts of data into valuable, actionable insights.

Using various algorithms and statistical techniques, Citrix ADM service creates live models that are unique to each application environment. Citrix ADM service relieves administrators from labor-intensive modeling tasks. It is also highly effective at separating actual performance or security concerns from miscellaneous noise. Citrix ADM service can play an essential role in:

- Server response time baselining
- Predictive analytics for resource utilization
- Application security and anomaly detection, including extensive network, WAF, and security violations
- Application usage anomaly detection

Security violation categories reported by Citrix ADM

Network				
HTTP slow loris	DNS slow loris	HTTP slow post	NXDomain flood attack	HTTP desync attack
Bleichenbacher attack	Segment smack attack	SYN flood attack	Small window attack	
WAF				
Unusually high upload transactions	Unusually high download transactions	Excessive unique IPs	Excessive unique IPs per Geo	Cookie hijack
Infer content type XML	Buffer overflow	Content type	Cookie consistency	CSRF form tagging
Deny URL	Form field consistency	Field formats	Maximum uploads	Referrer header
Safe commerce	Safe object	HTML SQL inject	Start URL	Cross-site scripting
XML DoS	XML format	XML WSI	XML SSL	XML attachment
XML SOAP fault	XML validation	Others	IP reputation	HTTP DoS
TCP small window	Signature violation	File upload type	JSON cross-site scripting	JSON SQL
JSON DoS	Command injection			
Bot				
Excessive client connections	Account takeover	Unusually high upload volume	Unusually high request rate	Unusually high download volume
Website scanners	Account takeover for Citrix Gateway	API abuse	Content scrapers	Keystroke and mouse dynamics based bot detection
Scraper	Screenshot creator	Search engine	Service agent	Site monitor
Speed tester	Tool	Uncategorized	Virus scanner	Vulnerability scanner
DeviceFP wait exceeded	Invalid DeviceFP	Invalid Captcha response	Captcha attempts exceeded	Valid Captcha response
Captcha client muted	Captcha wait time exceeded	Requuest size limit exceeded	Rate limit exceeded	Block list (IP, subnet, policy expression)
Allow list (IP, subnet, policy expression)	Zero pixel request	Crawler	Feed fetcher	Link checker
Marketing				

Application security and anomaly detection

Newer and more sophisticated attacks often look like legitimate human requests, which can often pass through unchallenged. With Citrix ADM service, machine learning capabilities keep applications performing at their best while ensuring that they are secure and protected against increasingly complex attacks and malicious actors. The service can help provide a consistent security profile across the organization, aggregating data from all Citrix ADC, Web Application Firewall (WAF), and bot management instances to continually train Citrix ADM machine learning models.

With its machine learning capabilities, Citrix ADM service is ideal for detecting a wide range of otherwise undetectable security issues and anomalies, including:

- **Account takeover attempts**. When a bad actor attempts an account takeover attack, they may use stolen or otherwise compromised credentials to gain account access with credential stuffing or automatic password spraying attacks. Because Citrix ADM service creates a model of the typical ratio of login successes and failures, it can notify security administrators of subtle deviations that might otherwise go unnoticed.
- **Excessive client connections**. Similar to its abilities to predict resource utilization, Citrix ADM service builds an expected threshold for typical client connections, factoring in considerations like seasonality, trends, and noise. If excess client connections are detected, security administrators are alerted so that they can take timely action.
- **Other suspicious anomalies**. Citrix ADM service can detect other abnormal deviations across multiple categories, including excessively high upload or download numbers, large data transactions, high request rates, and unique IP addresses from any location.

Conclusion

Citrix ADM service provides application-level security event reporting, aggregates data from all Citrix ADC WAF and bot management instances, and exports violations directly to Splunk Enterprise security dashboards. Advanced machine learning algorithms help organizations stay abreast of sophisticated and rapidly evolving attacks, delivering application-level security insights that were not available before.

Read more about Splunks' Citrix-compatible solution or visit the Citrix.com for detailed instructions for configuring Citrix ADM service and Splunk Enterprise.

citrix

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