

## Visibility and Analytics for Application and API Security

Citrix Application Delivery Management: Holistic and intuitive security insight from a single pane of glass across multi cloud.

Visibility of your security posture is just as important as the posture itself. It is easy to define what you should be doing, but if you can't track it then you can't tell if you are compliant or not. To protect applications from attack, you need visibility into the nature and extent of past, present, and impending threats, real-time actionable data on attacks, and recommendations on countermeasures.

### Citrix Application Delivery Controller and Application Delivery Management: A Unified Approach to Actionable Security Insights

Citrix Application Delivery Controller (ADC) takes a holistic approach to security and provides comprehensive protection from Layer 3-7 to all your applications (both traditional monolithic and microservices-based) across multi cloud. A rich set of applications and security capabilities like web application firewall (WAF), bot management, API protection and SSL termination are integrated into the Citrix ADC and available as part of the Premium license.

Citrix Application Delivery Management (ADM) works with Citrix Application Delivery Controller (ADC) to bring deep, comprehensive visibility of your security posture across all your multi clouds and all your applications from a single pane of glass. Citrix ADM collates telemetry from all your Citrix ADCs and uses artificial Intelligence and machine learning techniques to provide detailed insights for all of the security functionalities - WAF, bot management, APIs and SSL. This makes it easier to understand the threat your applications face and enables you to react more quickly to remediate security issues.

You can provide security operations teams with dashboards that are dedicated to security issues. These role-based dashboards can be customised with insights that fit with the roles in your organisation. This level of focus allows you to clear irrelevant information from their path and focus on the parameters they understand and are authorised to fix. Getting the right people involved at the right time with the right information helps fix issues faster.

### Visualise Attacks Against your Applications Without Cognitive Load

The Security Insight dashboard, shows you at a glance what attacks you are facing both on aggregate and against any particular application. You can easily and immediately see the number and type of violations faced by your applications. It also provides details on the origin of the attacks - both by IP address and the GeoLocation on a map. By understanding the types and severity of the attacks and the security posture of your apps, Citrix ADM tells you straight away which apps are most at risk so you can prioritise your remediations. For example, Citrix ADM may detect attacks that target different particular applications but your

---

security configuration is protecting only one of them. Citrix ADM will also alert you to missing security configurations for a particular application. For example, it will show how many applications firewall signatures and security entities are not configured for a particular application. Similarly, Citrix ADM will assess the configuration of the system security settings on individual Citrix ADCs and alerts you if anything is not set correctly.

### **Gain Bot Insights**

Citrix ADM has a bot insight dashboard that alerts you to the types of bot attacks you are experiencing, where they come from, their severity and how your systems reacted to them.

You can see which detection mechanism was triggered to determine bot activity - IP address, Signature, device fingerprinting etc. You can also see what action was taken on the incoming request - drop, redirect, rate limit, challenge - so you know your systems are protected.

Importantly, the dashboard calculates the proportion of bot traffic to human traffic which is crucial when you want to correct and normalise the business intelligence data about your site.

### **Define, Monitor and Enforce SSL policies**

The SSL dashboard in Citrix ADM brings all of the statistics about your SSL policy and usage into a single place. You can define the SSL policy - protocol, cipher, key strengths, certificate issuers - that is acceptable to your organisation, quickly within Citrix ADM in just a few clicks. You can set specific SSL profiles for specific entities to ensure different levels of SSL security - perhaps a stronger profile is required for external site to achieve an A+ security rating and perhaps self-signed certificates are acceptable for internal sites.

Citrix ADM will track and monitor all the SSL transactions on your site and alert if any deviate from your policy. Citrix ADM will also track all the SSL certificates deployed across your Citrix ADCs, their expiry and even enables you to update them easily and quickly. This ensures that you are always compliant and administrators don't inadvertently weaken the encryption posture with low strength certificates for example.

The SSL insight enables you to explore the impact of configuration changes on customer usage. For example, Citrix ADM will analyse historical SSL transaction data to see how many clients would be affected by switching off TLS 1.1 or removing a cipher like RC4-MD5. This helps you balance security with site usability. Similarly, you can examine the application response time based on the ciphers and protocols and understand if you have the capacity to handle higher security.

### **Gain API Insight**

API Insight brings together all the data and analytics about your applications' API usage both on aggregate or by drilling into for individual APIs. You can view data about API requests, responses, the data transmission as well as the origin of each API call (IP address and Geolocation). You can also view the performance data including API latency, the authentication successes and failures for each API as well which rate limiting actions have been taken. Similarly, you can monitor the TLS protocols, ciphers and key-strengths used.

---

Citrix ADM understand the status of your applications and the delivery infrastructure and offers valuable real-time and historical insight into the security of your systems, across your entire multi cloud deployment, in a single place. This holistic visibility makes it the obvious place for your administrators to start with monitoring and troubleshooting security issues. Further, it provides a central point to ensure governance and compliance with your corporate security standards and enforce consistent policies across all your environments. After all, best practice is only any good if you actually practice it.

### **Holistic Visibility Across Multi Cloud with Simplicity of Single Pane of Glass**

Citrix ADM collates telemetry from all your Citrix ADCs deployed on premises or in cloud environments in a single place. It provides a holistic approach to visibility for all your applications wherever they are deployed.

Citrix ADM is available as a virtual machine for installation on premises or as a Citrix Cloud Service. It is licensed per vServer under analysis. Citrix ADM includes all the security dashboards and insights in a single license.



#### **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

©2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).