Protecting Against Online Fraud

Citrix ADC, Citrix Web App Firewall, and Cleafy

Ready

Online services are under constant attack by fraudsters using increasingly sophisticated tools.

Expanding attack surfaces in the form of mobile platforms, open banking APIs, and online transactions present a vast opportunity for criminality. Compromised umnanaged user devices (endpoints) represent the weakest link, presenting a vulnerability to malware infection that can be used to attack online services. With a focus on early detection and rapid response, Citrix and Cleafy combine to provide an innovative and effective threat detection solution.

Full protection for online services

Online fraud is at an all-time high, with identity hacking, transaction tampering, account takeovers, and payment frauds all increasingly common. Sophisticated and constantly-adapting malware can steal credentials, generate client-side injection attacks, and launch trojans to compromise services. Complementing Citrix Web App Firewall and integrating closely with Citrix Application Delivery Controller (ADC), Cleafy's client-less and application-independent threat detection approach helps detect attacks in real time, while offering advanced protection against them.

Compromised user endpoint devices have emerged as a significant source of attacks against online services. Due to their unmanaged nature, these endpoint devices represent a common point of entry for malware bent on attacking on-line services. Unfortunately, the costs of successful breaches can be dire, including:

- Financial losses due to fraud
- Operational disruption
- Brand and reputational damage
- Customer dissatisfaction
- Regulatory fines
- Loss of proprietary information, sensitive data, or other strategic assets

Malware on endpoint devices can be particularly insidious and difficult to repel, since actions like stealing credentials or exfiltrating data are often not apparent to the organizations under attack until the damage is done. Attack techniques can include malicious BOTs, Man-in-the-Middle (MITM) attacks, Man-in-the-Browser (MITB) attacks, RAT-in-the-Browser attacks, web injects, mobile overlays, repackaged apps, Simple Messae Service (SMS) grabbing, and jail-broken devices.

The Citrix Ready Program

The Citrix Ready technology partner program offers robust testing, verification, and joint marketing for Digital Workspace, Networking, and Analytics solutions—with over 30,000 partner verifications listed in the Citrix Ready Marketplace.

Modern attacks are particularly impervious to traditional approaches.

- Malware detection is often ineffective since zero-day malware variants have no known signature.
- Application firewalls can miss these attacks since there is no server-side injection.
- Transaction monitoring is often ineffective since apps exhibit normal user behavior to achieve abnormal transactions.

In the face of these rapidly-evolving attacks, traditional solutions often don't work, as they often fail to identify new frauds before the fraud has been replicated. Attack campaigns are often in full operation before malware is identified and characterized (if ever) and well before signatures and matching rules are implemented. Malware often changes over time, escaping detection. Multiple networks of compromised endpoints (BOTnets) are often employed before they have been blacklisted.

Citrix and Cleafy provide all of the capabilities required to defend against cyberthreats and attacks from compromised endpoints. Cleafy complements Citrix Web Application Firewall capabilities and is smoothly integrated into architecture powered by Citrix ADC. With Citrix and Cleafy, attack campaigns are identified and characterized in the early stages, and followed if malware changes over time in an attempt to escape detection. Compromised endpoints are immediately blacklisted, thus minimizing the operational effort for anti-fraud teams. Potential customer impact is also greatly reduced.

Citrix Web App Firewall

Citrix Web App Firewall protects web applications and sites from both known and unknown attacks, including all application-layer and zero-day threats. Organizations can protect their web infrastructure against DDoS, SQL injection, XSS, and SSL attacks. Available as a standalone appliance, or integrated with the Citrix ADC platform Citrix Web App Firewall delivers comprehensive protection without degrading throughput or application response times.

Citrix ADC

Citrix ADC is a world-class application delivery controller with the proven ability to load balance, accelerate, optimize, and secure applications. The award-winning product is built with a software-first approach to delivering applications across hybrid and multi-cloud architectures. Citrix ADC provides proven L4-7 load balancing and global server load balancing (GSLB) to ensure the best application performance and reliability. The platform supports integration from other Citrix products as well as Citrix Ready partner solutions such as those provided by Cleafy.

Citrix and Cleafy integration

As shown in Figure 1, Cleafy seamlessly integrates with Citrix ADC, without touching any other server-side component. Cleafy does not require any application change, is completely transparent to the end-user, and does not

impact user the experience. Cleafy smoothly integrates in any Citrix ADC architecture by utilizing Citrix ADC's unique traffic switching and transformation mechanisms, such as Rewrite Policies and HTTP Callouts.

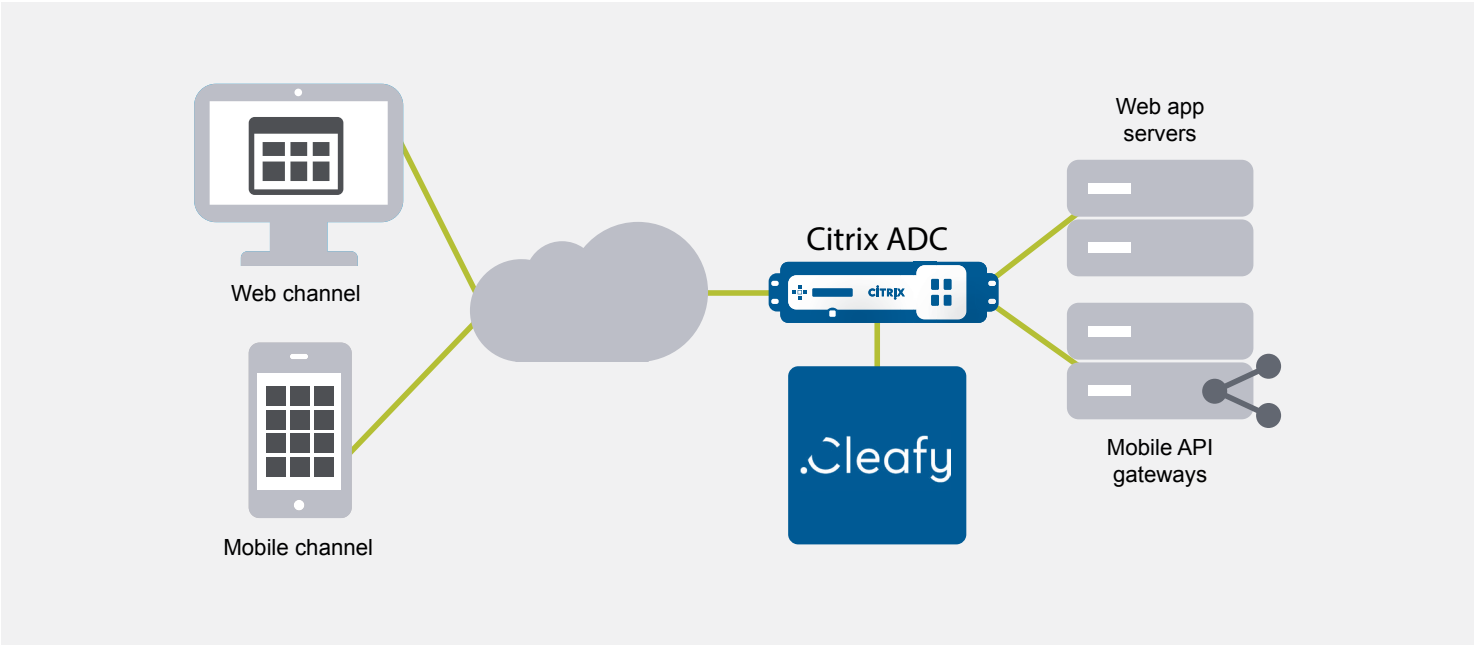

Figure 1. Cleafy high-level architecture and integration with Citrix ADC.

Cleafy

Cleafy is an innovative solution based on patented technology that has been specifically designed to protect online services from attacks from unmanaged endpoints. Cleafy detects advanced, targeted attacks based on Man-in-the-Browser (MITB), Man-in-the-Middle (MITM), RAT-in-the-Browser, App Repackaging, SMS Grabbing, Mobile Overlay and other vectors used by modern fraudsters. Cleafy's key capabilities include:

- **Endpoint transparency**. Cleafy is an agent-less solution, and imposes zero impact on either user experience or endpoint performance. No computing is done on endpoints and all communications back to the Cleafy engine are asynchronous.
- **Application transparency**. Cleafy requires no application changes and zero touch on the application back-end. Cleafy controls are delivered automatically through integrations with the application delivery infrastructure for web applications and via a passive Mobile SDK for mobile applications.
- **Real-time threat detection**. Cleafy performs continuous monitoring and real-time risk scoring of user sessions—even before the authentication phase—applying deterministic malware detection, behavioral and transactional analysis, and cross-session correlation.

- **Adaptive threat response.** Cleafy enables automatic execution of response actions in case of high-risk sessions or specific threats, including the activation of Cleafy threat protection mechanisms.
- **Open and scalable.** Cleafy smoothly integrates into any ecosystem thanks to extensive APIs and push/pull mechanisms, including the ability to feed higher-level risk engines such as Citrix Analytics.

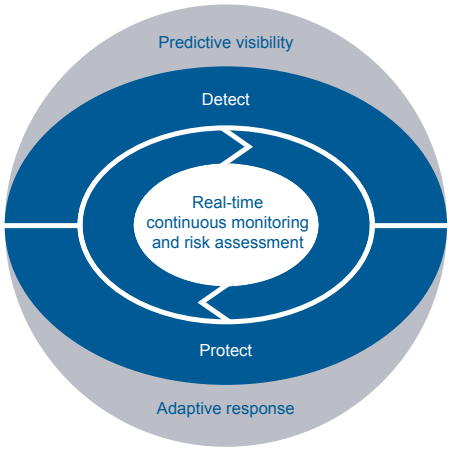

Figure 2. Cleafy provides real-time continuous monitoring and threat classification.

In almost all modern attacks, malicious code is injected into the content delivered by the application. This code might be used to hijack user credentials as in the case of Account Take-Over (ATO) attacks, or tamper with transactional data as in the case of Automatic Transfer System (ATS) attacks. Cleafy's malware detection technology is based on patented technology that verifies in real-time the integrity of the application as delivered to endpoints. For example, Cleafy analyzes the entire Document Object Model (DOM) as well as on XHR and API calls executed by web applications to detect any malicious code which is compromising the integrity of the application on the endpoint—all in real-time.

Since Cleafy does not rely on signatures and pattern matching, it can deterministically detect both known and unknown malwares (i.e. zero-day attacks), without generating false positives. Cleafy integrity detection capabilities provides unparalleled threat visibility at the level of malicious web-injects (the snippets of code that are injected by malware) and malicious mobile apps. This ability makes it possible to get unique insights on attack techniques, understand the attacker's tactics, techniques, and procedures (TTPs), and get predictive visibility. As a consequence, online frauds are dramatically reduced, and the security team efficiency greatly improved.

Cleafy's real-time risk scoring and threat classification can trigger threat response rules implementing the desired security posture with respect to the specific level of risk or threat (Figure 2). Responses might include dropping the session, deflecting the attack, raising an adaptive authentication, or activating Cleafy protection capabilities. By protecting delivered content against MITB and MITM attacks, Cleafy allows end-users to perform transactions safely—even if their endpoints or network is compromised. Cleafy threat protection does not require any application change and can be activated dynamically when a specific threat is detected or when the level of risk is too high.

In order to transparently inspect the application traffic and deliver its dynamic controls, Cleafy integrates with the application delivery infrastructure. The integration with Citrix ADC supports the ability to inject a Cleafy script when a resource is requested by the endpoint. The script can log requests and responses to compare in real-time the executed and rendered content on the browser with the generated content on the server. Moreover, thanks to Citrix ADC's unique traffic switching and transformation mechanisms (e.g. rewrite policies and HTTP callouts), Cleafy can dynamically deploy its threat protection capabilities without any change to the application-delivery infrastructure (such as adding a reverse proxy). Cleafy can also use Citrix ADC authentication mechanisms.

Cleafy can manage multiple applications within a single implementation by setting application-specific threat detection and protection policies. Cleafy also allows granular roles and privileges for each application to be assigned to each user, thus also supporting multi-tenant environments.

The Cleafy Console provides detailed visibility on sessions, events and threats, down to the level of malicious web injects and apps (Figure 3). Cleafy query language allows users to quickly discover new attack patterns, create custom dashboards, generate both on-demand and scheduled reports, and also define correlation rules and automatic response actions.

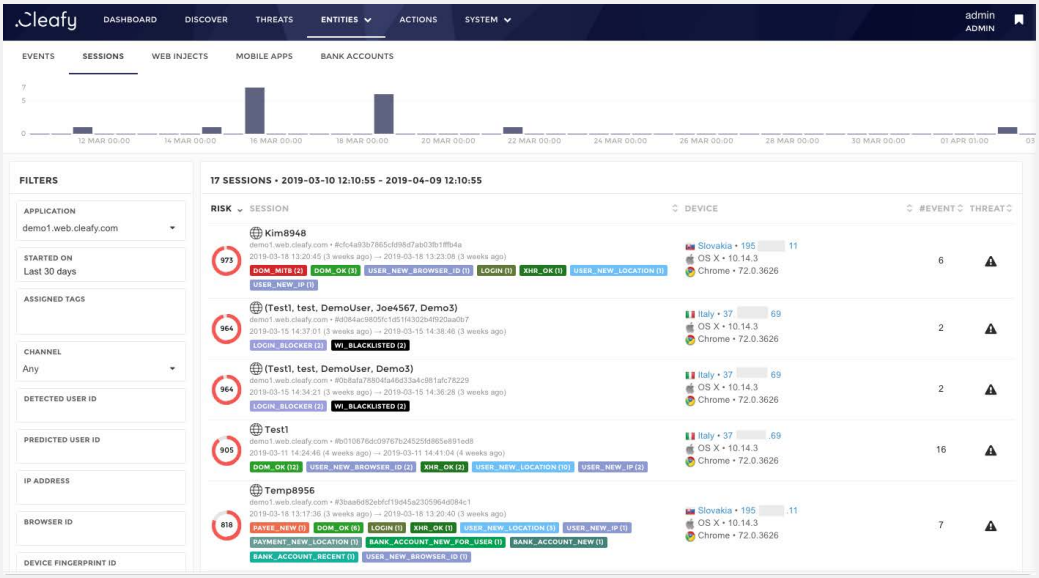

Figure 3. Cleafy Console showing monitored sessions

Cleafy and Citrix Analytics

Citrix Analytics collects data across Citrix offerings and generates actionable insights, enabling administrators to handle user and application security threats, improve app performance, and support continuous operations. By using security policies, machine learning and artificial intelligence, Citrix Analytics helps you take a proactive approach by integrating with the entire Citrix portfolio to uniquely protect each user, the workspace, and the network.

Citrix Analytics is designed to allow integration from partners. Cleafy can be used to feed information into Citrix Analytics, providing the opportunity to promote Cleafy information to the Citrix Analytics dashboard. Everything that Cleafy collects is available through APIs, including real-time scoring. As an example, the Citrix Analytics dashboard could access Cleafy and display a risk score for a particular user session.

Conclusion

Together with Citrix, Cleafy's adaptive approach to application security lets organizations proactively respond to threats in real-time. Cleafy's innovative threat detection and protection approach has been proven to be effective against MITB, MITM, RAT-in-the-Browser, SMS grabbing, mobile overlay, and other techniques often used from infected endpoints. As a Citrix Ready solution, Cleafy complements Citrix Web App Firewall and integrates with Citrix ADC to access it's load balancing and context switching capabilities. Cleafy can be added easily into any Citrix ADC infrastructure, providing a robust application protection strategy without user or application disruption.

For more information, view Cleafy's profile on the Citrix Ready Marketplace at citrixready.citrix.com/cleafy.html.

Cleafy

About Cleafy

Cleafy is a leading provider of fraud management solutions against today's most advanced attacks to online services. Cleafy enables customers to continuously monitor and assess the risks of users sessions in real-time and to implement adaptive responses without impacting delivered service and users. Cleafy is used by major financial services, on-line lending and providers of critical on-line services to avoid online frauds, reduce operational efforts, and achieve compliance. Cleafy has been a Citrix Ready partners since 2017. Read more about Cleafy at cleafy.com

CITRIX Ready

About Citrix Ready

The Citrix Ready technology partner program offers testing and verification for joint Digital Workspace, Networking, and Analytics solutions. After a robust testing process, validated partner solutions are listed in the Citrix Ready Marketplace, giving customers and channel partners a simple and effective way to explore and select Citrix Ready verified solutions—increasing confidence while reducing risk. Learn more at citrixready.citrix.com

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