Safenames

CLOUDFLARE
PARTNER NETWORK

What can we learn from past vulnerability exploits?

The onset of 2020 was marked by the disclosure of a 'serious' cyber attack against the United Nations, which took place in September 2019 and compromised 42 core servers. In the case of the United Nations, the attackers exploited a known vulnerability in an Internet-facing Microsoft SharePoint server, a web-based collaborative platform integrated with Microsoft Office. Even though Microsoft had issued fixes for this vulnerability in March 2019, the U.N. had not patched its infrastructure, resulting in the successful attack.

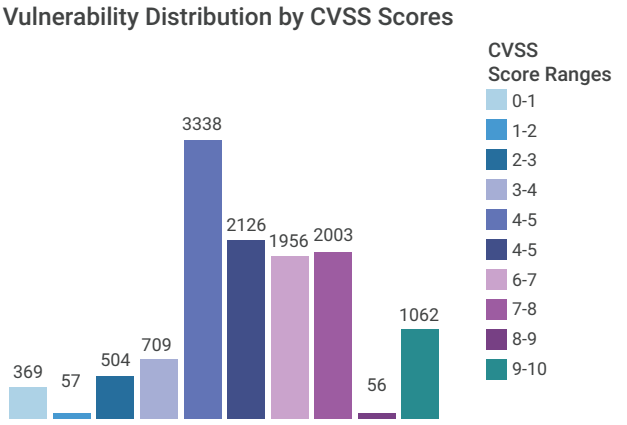
Targeting infrastructure with known vulnerabilities is a common tactic adopted by numerous cyber criminals. The U.N. is not the only victim of this attack tactic. There are numerous examples, including Equifax's 2017 breach that exploited an Apache Struts vulnerability and vBulletin's remote code execution vulnerability that affected numerous enterprises. These organizations have their best efforts and intent to safeguard their infrastructure and data. However, it is extremely difficult to operationally implement security efforts in a world where every gap could be a potential for an attack.

To thwart these types of attacks, it's important to focus on the fundamental issues and solutions that help solve them.

Patching infrastructure is fundamental, but not trivial

An increasing number of security leaders are investing the majority of their resources to ensure a good level of cyber hygiene for their infrastructure. Up-to-date infrastructure patching is a key component of developing good cyber hygiene.

However, it's not a trivial task. Even the largest security teams are usually not able to patch their entire infrastructure owing to the sheer number of patch fixes and the significant velocity of patch releases by numerous vendors. In 2019, there were a total of 12,174 common vulnerabilities and exposures (CVE) announced, out of which 1,062 (8.7%) were considered critical with a CVSS score of between 9 and 10.



*Courtesy: 2019 Vulnerability distribution by **CVSS Scores***

The conventional way of dealing with this problem is to prioritize vulnerabilities per certain organizational risk metrics and patch them by categorizing vulnerabilities as P0, P1, P2 and so on, with SLAs attached to each category. It's a constant balancing act between 'fixes to be deployed' and 'resources available,' and attackers take advantage of this balancing act.

In the case of the U.N. attack, the attackers exploited the fact that the U.N. had not yet patched their infrastructure against the known vulnerability.

Secure the fundamentals with a layered defense approach

A layered defense approach empowers security leaders to build a strong security posture against this attack tactic. A vital component of today's layered defense strategy is a cloud-based web application firewall (WAF). Appliance-based hardware WAFs are an extremely outdated solution considering the current threat landscape. Applications and data today mostly reside both within on-premises infrastructure and in the cloud.

In contrast to hardware WAF appliances, a cloud-based WAF provides protection against vulnerability-based attacks, no matter whether the application and infrastructure are on-premises, in the cloud, or part of a hybrid deployment.

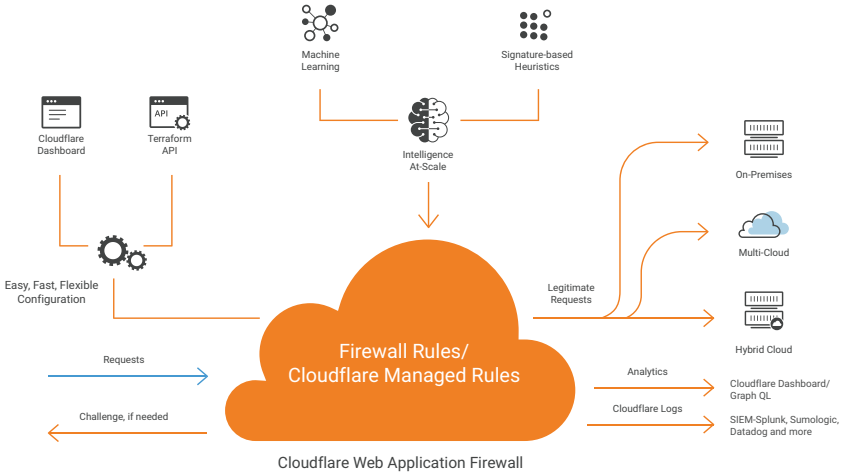
There are several key aspects of the cloud-based WAF that security leaders need to take into consideration.

The WAF market is growing, driven by the adoption of cloud WAF services. Enterprise security teams should use this research as part of their evaluations of how WAFs can provide improved security that's easy to consume and manage, while respecting data privacy requirements.

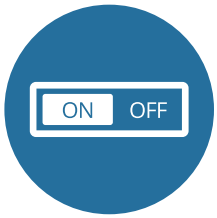
-Gartner Magic Quadrant for WAF report

A WAF solution for today and the future

In its latest 2019 report 'The Future of Network Security Is in the Cloud,' Gartner states, "The enterprise perimeter is no longer a location; it is a set of dynamic edge capabilities delivered when needed as a service from the cloud." Cloud-based WAF is a key aspect of the security posture of today and the future.

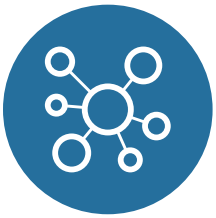


The following aspects are of paramount importance when selecting a cloud-based WAF to protect your applications, data, and infrastructure.



EASE OF USE

Usability from a perspective of onboarding and managing is an extremely important factor when selecting a WAF. Onboarding a WAF should not take weeks or months, and managing it should not require an army of professionals. Enterprises commend Cloudflare WAF's ease of use. With just a few clicks through an intuitive dashboard, businesses can quickly strengthen their security posture. Terraform API integrations allow convenient ways to build and manage WAF rules.



REAL-TIME THREAT INTELLIGENCE

One of the key shortcomings of a hardware-based WAF is that it lacks real-time context on threats and attacks. Even integrating threat intelligence feeds with a hardware-based WAF only makes for a reactive solution. In today's world, where the threat landscape is evolving rapidly, real-time threat intelligence context is critical for a WAF solution. The Cloudflare WAF is built on an always-learning network connected to Cloudflare data centers in 200 cities globally and protecting over 20M Internet properties worldwide. The collective intelligence derived from analyzing diverse global traffic enriches the WAF with real-time context to thwart the latest attacks.

COMPREHENSIVE COVERAGE

Protection against common vulnerabilities, including the OWASP Top 10, is fundamental to every WAF. But while attackers do attempt to exploit them, they are especially interested in critical and 0-day vulnerabilities. Cloudflare's Managed Rulesets are regularly updated to ensure that attacks attempting to exploit 0-days and other critical vulnerabilities are thwarted at the Cloudflare edge and never reach your infrastructure. Cloudflare's Managed Rulesets can be toggled on with a click within its WAF. Firewall Rules allow businesses to build, test, and deploy their own customized rules with a few clicks.

AGILITY

When any vulnerability, especially a 0-day vulnerability, is announced, it kicks off a race between malicious actors and enterprise security teams. An outside perimeter at the edge allows for instant protection against attacks while security teams patch their infrastructure. Cloudlfare's WAF Rulesets propagate globally within an unprecedented speed of less than 30 seconds through our Anycast network.

ACTIONABLE ANALYTICS

While control and protection is important, visibility into attack events and relevant data is equally important. Cloudflare Analytics provides a dashboard view to security leaders and teams to quickly and comprehensively analyze data. GraphQL API enables integration with existing enterprise dashboards. In addition, enterprises can integrate comprehensive Cloudflare Logs with popular SIEMs, including Splunk, Sumologic, Datadog, and more.