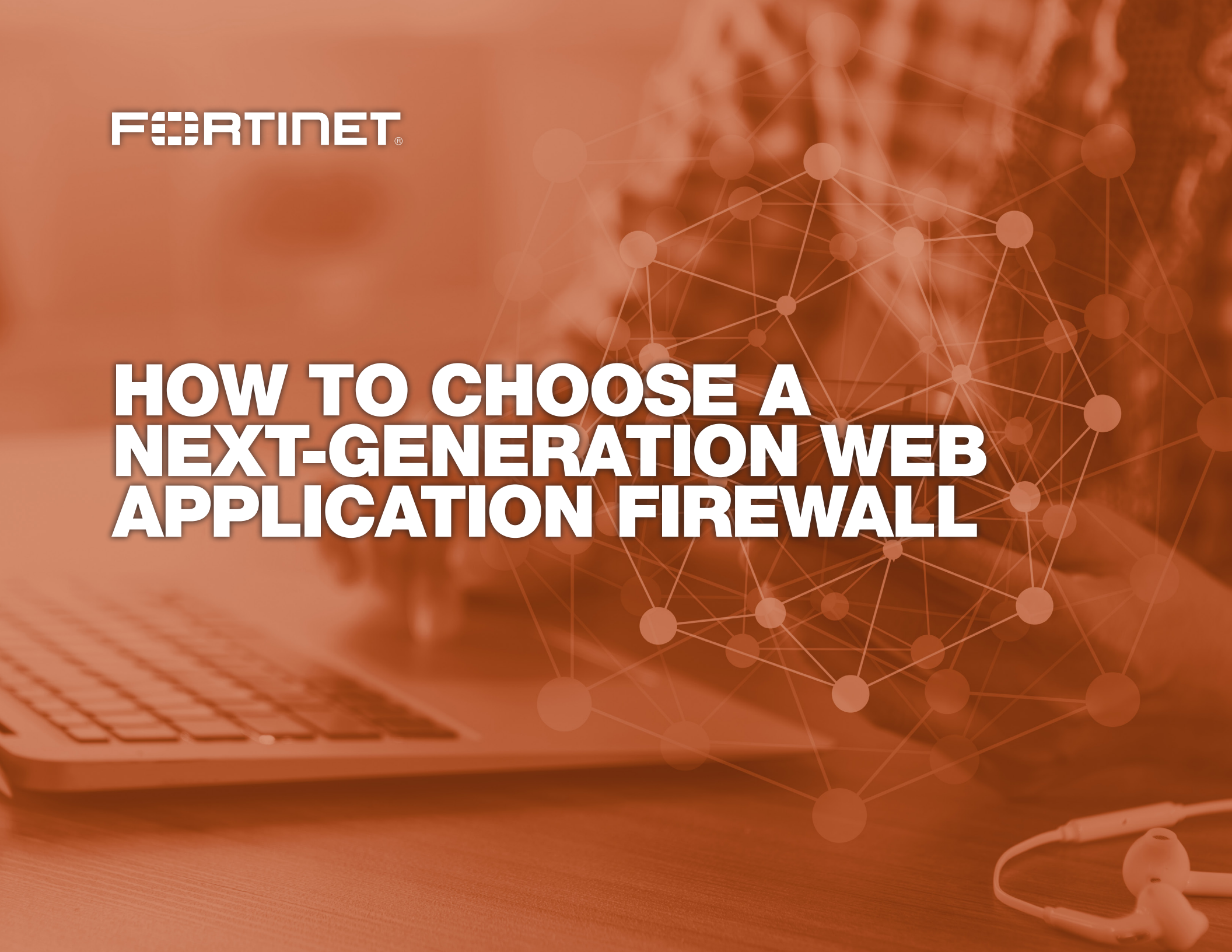


HOW TO CHOOSE A NEXT-GENERATION WEB APPLICATION FIREWALL

CONTENTS

EXECUTIVE SUMMARY

The more companies rely on web applications to support basic business processes, the more crucial web application firewalls (WAFs) become for protecting corporate data and preventing operational disruptions. Organizations shopping for a WAF need to evaluate several different types of functionality.

One is the set of core WAF capabilities that include antivirus and malware protection, signature engine, IT-reputation checks, and protocol validation. But the explosion in known and unknown threats creates security gaps, with application learning used for behavioral threat detection. The binary nature of application learning results in high false-positive rates that stretch already overburdened staff resources. Many are looking to artificial intelligence (AI) and machine learning as tools to address false positives while improving the accuracy of threat detection.

The WAF must also integrate into an organization's broader security architecture. And it must incorporate the same concerns that are front and center in most security solution decisions: scalability, impact on throughput, and ease of use.

WEB APPLICATION SECURITY CHALLENGES

Companies rely on web applications—on-premises, in the cloud, or both—for all sorts of functions. When these applications fail, the disruption not only affects corporate operations but also ripples up and down the supply chain. Web applications also access and process critical data such as customer and financial data. Without vigilant protection, that data may be compromised.

The more a business relies on web applications, the more it needs a WAF to protect those applications against external and internal threats. That's because at the same time the corporate attack surface is ballooning, the volume and variety of cyberattacks is expanding as well. Nearly half (48%) of all data breaches now result from the hacking of a web-based application.[1] An organization that depends only on a firewall and intrusion prevention system (IPS) is inadequately prepared to thwart attacks that are increasingly polymorphic, employing multiple attack vectors simultaneously.

Companies need a WAF that effectively identifies and protects against both known and unknown exploits while minimizing false positives, which may dilute the resources available for threat response. Some WAF technologies struggle to meet this objective. Chief information security officers (CISOs) looking to improve security of their organization's web applications need to find a WAF that offers:

- Excellence in core WAF capabilities
- Sophisticated behavioral threat detection that doesn't require a lot of resources to manage
- Scalability that does not reduce throughput

[1] "2018 Data Breach Investigations Report," Verizon, March 2018.

INSIST ON BEST-IN-CLASS CORE CAPABILITIES

Because attacks on web applications are so varied, security for those applications needs to employ a combination of protection approaches. These approaches not only must be varied to combat the diverse attack vectors but they also need to be correlated. And the WAF should take appropriate action to protect web applications whenever it detects threats.

1. Antivirus and Malware Protection

The most fundamental of security products, an antivirus and malware-detection engine is a crucial building block for any successful WAF. The engine needs to scan all web application traffic for threats that could potentially infect servers and other devices on the corporate network.

2. Frequent Signature Updates

Another capability included in every WAF is signature detection, which compares the contents of incoming packets against the signatures of known web attacks. These can include botnets, advanced threats, and distributed denial-of-service (DDoS) attacks.

To provide effective signature detection, a WAF requires:

1. Resources of a large and reputable threat research organization.
2. The ability to incorporate threat research insights into its signature-detection database. Ideally, these updates will flow into the WAF in real time.
3. The faculty to either redirect potentially malicious packets to a sandboxing tool or else block them from the corporate network.

3. IP-Reputation Verification

Like signature detection, IP-reputation checks compare incoming traffic against known threats. The difference is that they look not at the content of the incoming packets but at their source. The WAF maintains a blacklist of IP addresses known to be associated with delivery of botnets and other types of attack. The WAF compares traffic hitting protected web applications against its malicious-source blacklist, and when it detects a match, it prevents the associated traffic from entering the network.

As with signature detection, excellence in IP-reputation checks requires a WAF to tie into a threat intelligence service that provides frequent updates to the blacklist. The more sophisticated WAFs are also able to identify and blacklist the sources of malicious packets tagged by their signature-detection engine.

4. Protocol Validation

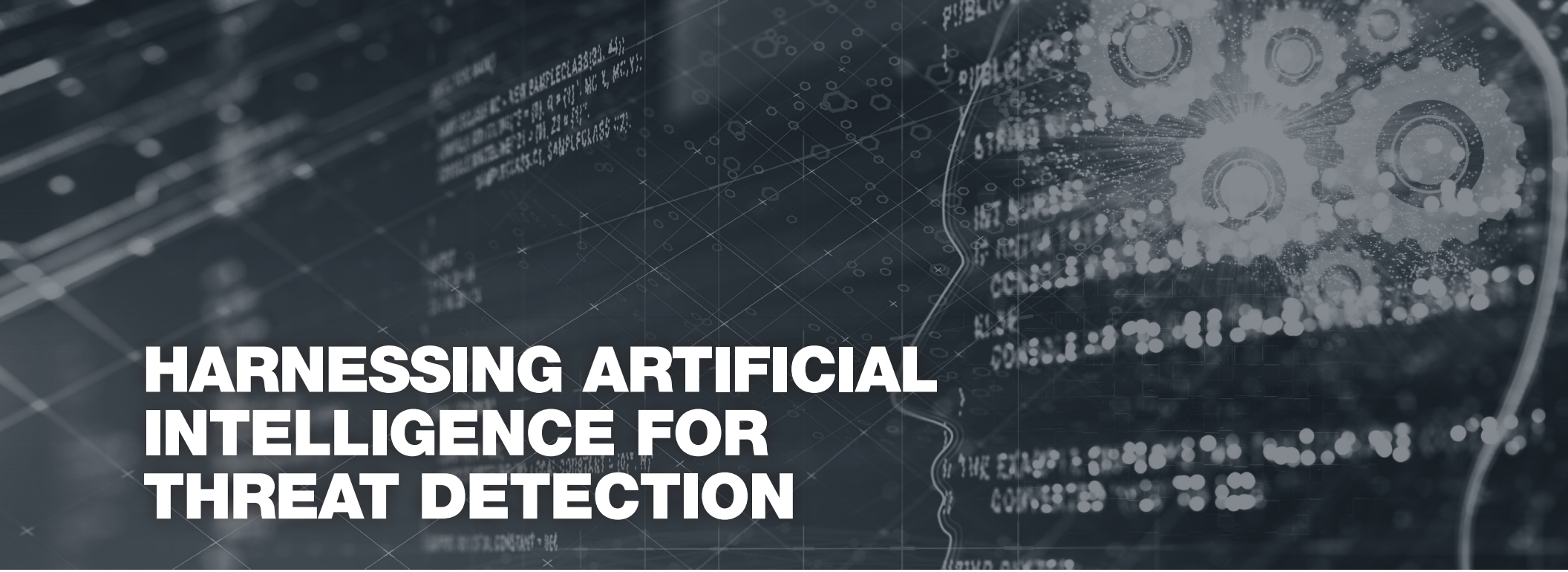
A WAF must also be able to root out improper HTTP code. When applications that use different communications protocols interact, they create a vulnerability. An attack might be able to bypass strong security measures in each application by mimicking the other application's protocol. Such an exploit could bypass even strong security measures by feigning translation errors. All web-based applications should comply with HTTP RFC specifications. To nip prospective protocol exploits in the bud, a WAF needs to validate the protocol of any code that protected web applications try to execute.

5. Integration of Capabilities

Each of these WAF capabilities alone is key to protecting web applications from one or more common types of exploits. To optimize protection, the WAF should integrate these functions in two ways:

Data correlation. Data on application-layer signatures, malicious bots, suspicious IP addresses, and emerging viruses should be correlated so that threat intelligence is shared across capabilities. For example, when the WAF identifies a botnet, it can add the botnet's originating IP address to its IP-reputation blacklist, automatically flagging any future traffic coming from that address.

Intelligence sharing. The WAF should also fit seamlessly into the organization's broader security architecture. Many cyberattackers employ polymorphic malware and simultaneously take multi-vector attack approaches. Combating such threats requires real-time intelligence sharing across all network components. For example, an attack might probe vulnerabilities across multiple vectors—endpoints, email, and cloud services, among others—and employ machine learning to hone the exploits based on information learned. In these instances, the WAF needs to share threat intelligence in real time with each of these security elements—and vice versa—to successfully thwart these advanced threats.



HARNESSING ARTIFICIAL INTELLIGENCE FOR THREAT DETECTION

Blacklisting and whitelisting security technologies may catch a significant proportion of threats, but they are only as good as the lists they rely upon—namely, they can identify only previously recognized exploits. With security providers unable to create signatures for unknown threats, traditional security approaches are unable to prevent and detect emerging and zero-day attacks.

In addition to list-based monitoring capabilities, most WAFs incorporate behavior-based threat detection, an approach to web application security that compares the actions of users or applications against expected behaviors to recognize and flag anomalies. Solutions that incorporate application-learning technologies monitor responses to certain inputs over time and extrapolate, or "learn," what responses they should expect to receive in the future.

These WAFs automatically build a profile of the structure of a protected application, as well as how the application is used in the organization. Then, they associate rules for threat response to characteristics of these profiles. Behaviors that trigger an alert might cause incoming web application traffic to be blocked entirely or to be routed to a corporate sandboxing tool.

1. Challenges of Application Learning

WAFs with these capabilities incorporate application "learning," but that doesn't mean they are very intelligent. They develop the profile for a protected application by observing data entries and other facets of user behavior as it relates to each parameter of the application, including value ranges for form fields, HTTP methods, cookies, etc. And they do continue to update these profiles over time, as they gather more and more data on user behavior.

The problem is that any behavior which doesn't fit into a WAF's specified profile—in other words, any behavior that the WAF hasn't previously observed—triggers an alert. This creates an exorbitantly high rate of false positives in the WAF's threat detection. Anytime a new data trend in user behavior emerges, application traffic may be blocked until a human can review and decide that it is not actually a threat. Over time, the new behavior will become expected, but many actions that present no threat to the organization get flagged and require manual follow-up processes.

2. Benefits of AI-Based Machine Learning in a WAF

Companies with limited security staff should look for ways to reduce the often-high resource requirements entailed in managing a WAF's application-learning capabilities. One area where WAF providers can turn is true AI-based machine learning.

Machine learning enables a WAF to view deviations from normal user or application behavior, not as an immediate cause for alarm but as a context for considering security concerns. Potential alerts aren't evaluated from the perspective of a simple "yes" or "no" rule violation; they inform the WAF's automated calculation of the probability that a user or application behavior represents a threat requiring a security response.

Few WAFs have incorporated this type of machine learning. Those that have done so are able to respond to behavioral anomalies according to predefined rules depending on the threat likelihood determined across multiple parameters. This can virtually eliminate the false-positive problem created by application learning. Thus, unlike organizations that rely on WAF application learning, those that use machine learning can avoid allocating valuable staff resources to resolve false positives.

Moreover, machine learning enables the WAF to classify files and data sources much more accurately. Combined with core WAF capabilities, machine learning can detect almost all legitimate threats. This helps protect the network against scanners, crawlers, scrapers, credential stuffing, and a host of unknown attacks.

PERFORMANCE AND OPERATIONAL CONSIDERATIONS

Clearly, a WAF's ability to protect the network's web applications is a key consideration in the CISO's solution research. But it's not the only one.

1. **Throughput.** As business-critical as security may be, few organizations can afford to have traffic slowed down when their WAF conducts comparisons against blacklists, whitelists, and behavioral profiles. Further, security leaders evaluating WAFs need to understand not only typical throughput for their different options but also the characteristics of their network and security architecture that might reduce each device's throughput in their unique environment.
2. **Scalability.** Related to throughput concerns are the struggles some WAFs have in supporting a large volume of web application traffic. Most companies will continue to see their data volumes grow rapidly for the foreseeable future. Thus, their WAF needs to be scalable enough to support not only the organization's current traffic volume at its desired level of throughput but also its anticipated future web application traffic.
3. **Administrative resources.** In addition to the massive amount of staff time that false positives in application learning can consume, WAF buyers should consider each solution's ease of use, as well as how much effort the security team must dedicate to configuring and fine-tuning threat-response rules.
4. **Reporting and compliance.** The reporting provided by a WAF needs to comply with all the appropriate regulatory requirements, such as National Institute of Standards and Technology (NIST) 800 security controls, the Payment Card Industry Data Security Standard (PCI DSS), etc.

Evaluating WAF alternatives against all these criteria takes time, but the huge potential to protect web applications and data both effectively and efficiently makes the process well worth the effort.

www.fortinet.com