Our Web Application Firewall

Powered by Imperva Cloud WAF

Traditional network security solutions are incapable of detecting, preventing, or alerting on attacks against the application layer. Xerox partners with Imperva to protect our web-based applications against known and emerging threats. This includes common web 2.0 threats, such as spammers, scrapers, SQL injection, cross site scripting, and other application-level attacks.

CLOUD WEB APPLICATION FIREWALL FAQS

What is changing when Xerox Internet web applications onboard to WAF?

Our strategic direction is to leverage Imperva as the front line of defense for Xerox internet-facing applications, thereby retiring any legacy WAF solutions. As such, the public record (DNS) will be updated to reflect the association.

Why do we recommend the fully qualified domain?

Using an application URL is the recommended method to access web resources.

Keeping pace with an ever-changing threat landscape requires cyber security solutions to deliver seamless, secure access, with little if any change in the user experience. The detail behind each URL is updated when the application onboards to Imperva. This is, by design, invisible to the consumer.

Authentication can be accomplished through interactive and non-interactive methods.

- People access internet resources through a URL, an interactive method.
- Device-to-device communications can be interactive or non-interactive.

When should an IP address be used?

If a customer does not choose the recommended method, explicit IP address management can be leveraged for device-to-device communications.

Explicit IP address management allows organizations to have better control over what devices are authorized to communicate with each other. This is typically handled through traditional corporate firewall management. By design, a cloud web application firewall sits BEFORE a traditional corporate firewall; therefore, this method must be translated for cloud consumption.

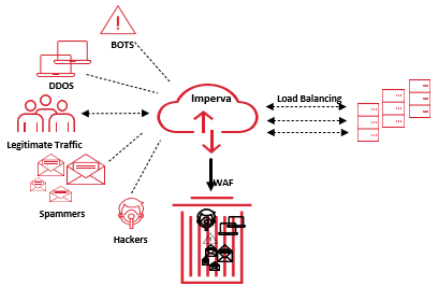
When IP address is mandatory, associating the dedicated Imperva IP assigned to each Xerox application allows for hard coding into customers' traditional firewall solutions.

RISK

If/when the Imperva IP addresses change, an update to firewall rules will be required to ensure connectivity continues uninhibited.

How does WAF inspect traffic?

Every request is inspected at three levels: the connection level, the request format and structure level, and the content level. The WAF matches the HTTP/S requests against a set of security engines, known attack patterns, heuristic rules, anomaly detection and known "good" patterns.



Conclusion

These are not new practices, only new technology. These practices align with the current control structure outlined in the National Institute of Standards and Technology which will never dictate the technology used but will identify the controls that must be enforced to maintain compliance.

xerox™