The Future of Web Security

10 Things Every Web Application Firewall Should Provide

IMPERVA®

Share this eBook

Contents

The Future of Web Security

OVER 50%

of organizations experienced a Web application breach in the past year. Many of these incidents led to **severe financial losses.**

- Infosecurity Magazine, citing Forrester Consulting

The Future of Web Security

Securing Web applications against cybercriminals, hacktivists, and state-sponsored attackers is a never-ending effort. Why?

HACKERS

EVADE TRADITIONAL NETWORK SECURITY DEFENSES TO TAKE DOWN WEBSITES AND TO STEAL DATA

MALICIOUS USERS

PROBE WEBSITES AROUND-THE-CLOCK LOOKING FOR VULNERABILITIES

AUTOMATION TOOLS

SUCH AS OFF-THE-SHELF ATTACK TOOLKITS AND BOTNETS MAKE IT EASY TO EXECUTE LARGE-SCALE ATTACKS

Time and again, organizations that rely solely on network security solutions to protect their applications have seen their Websites breached.

The Future of Web Security

Web application firewalls have become the central platform for protecting applications against all online threats.

TECHNICAL WEB ATTACKS

- SQL INJECTION
- CROSS-SITE SCRIPTING
- REMOTE FILE INCLUSION

BUSINESS LOGIC ATTACKS

- DISTRIBUTED DENIAL-OF-SERVICE
- SITE SCRAPING
- BRUTE-FORCE ATTACKS
- COMMENT SPAMMING

ONLINE FRAUD ATTACKS

- MALWARE
- IDENTITY THEFT
- ACCOUNT TAKEOVER

Why Traditional Network Security Fails

TRADITIONAL NETWORK SECURITY SOLUTIONS

CANNOT
block attacks that exploit custom Web application vulnerabilities

CANNOT
detect cookie, session, or parameter tampering attacks

CANNOT
stop fraudulent devices or business logic attacks

IMPERVA®

Share this eBook

WEB APPLICATION FIREWALLS

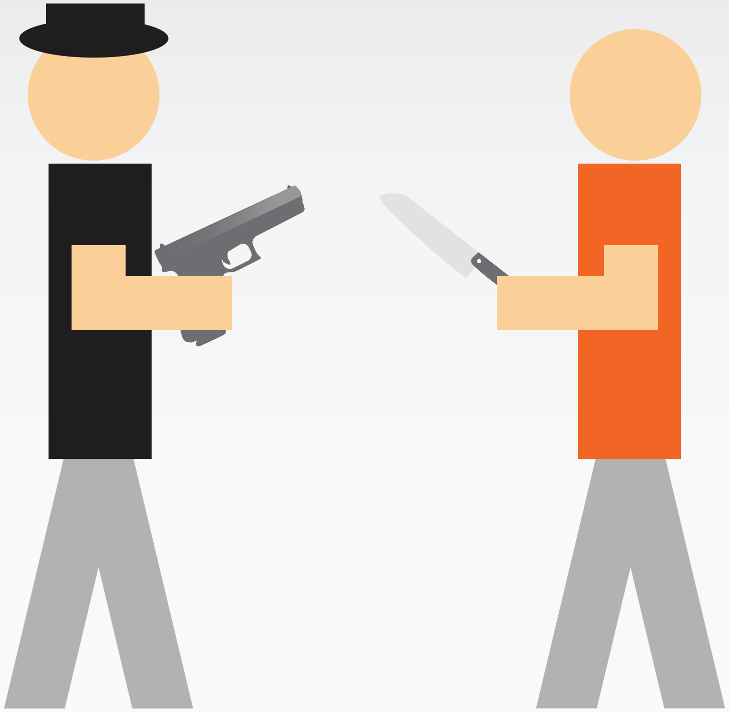
CAN
block attacks that exploit custom Web application vulnerabilities

CAN
detect cookie, session, or parameter tampering attacks

CAN
stop fraudulent devices or business logic attacks

10 Things Every Web Application Firewall Should Do

Advanced, custom Web attacks outpace signatures.

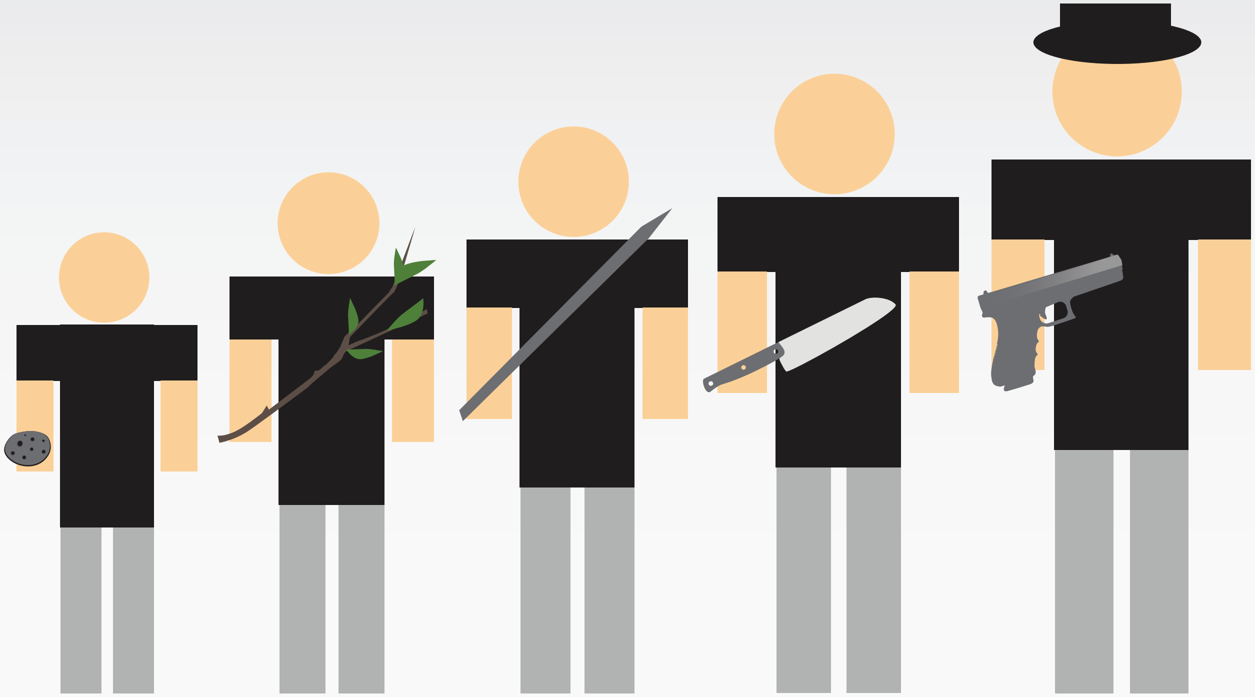


YOUR WAF MUST Detect Unusual Requests

- Understand the protected application including URLs, parameters, and cookies
- Inspect parameter values for special characters and recognize when these characters are expected or indicative of an attack
- Learn application changes without manual intervention

> “Input validation is the single best defense against injection and XSS vulnerabilities.”
>
> – BRENT HUSTON, State of Security

Threats to online applications continue to evolve.



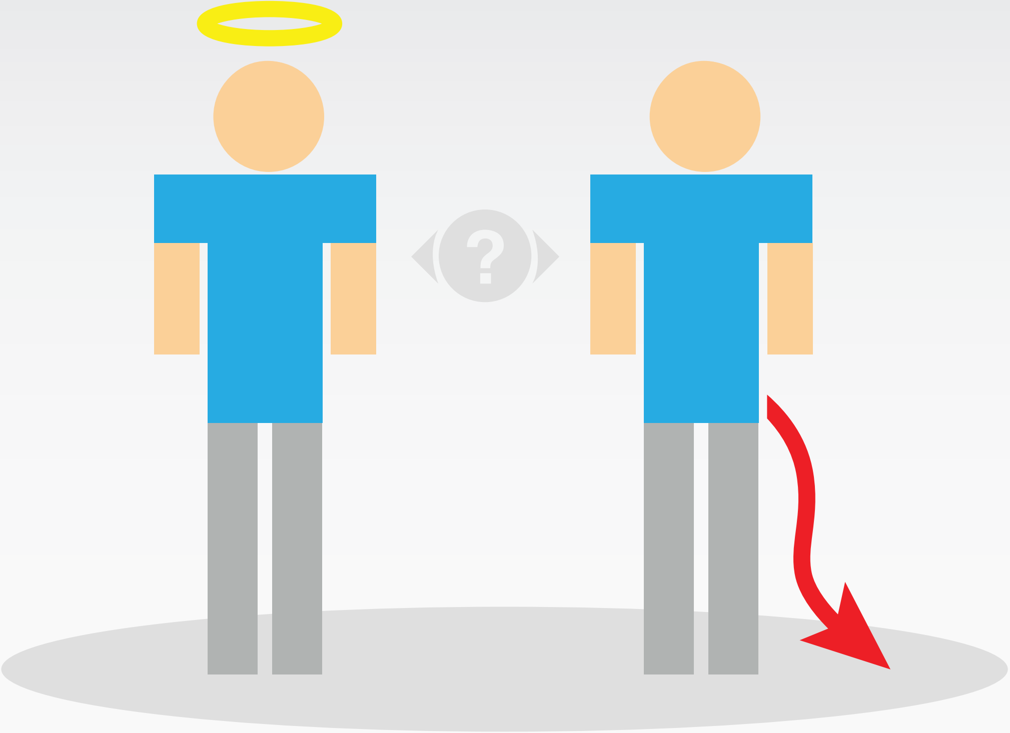
YOUR WAF MUST Stay in Front of Hackers

- Leverage live attack, reputation, and fraud data to identify active attacks and the attackers
- Provide automatic updates to security signatures, policies, reputation data, and fraud intelligence

A WAF should "automatically receive and apply dynamic signature updates from a vendor or other source."

– Recommended WAF capability in the PCI DSS Information Supplement: Application Reviews and Web Application Firewalls Clarified

Stop Web attacks without blocking legitimate traffic.

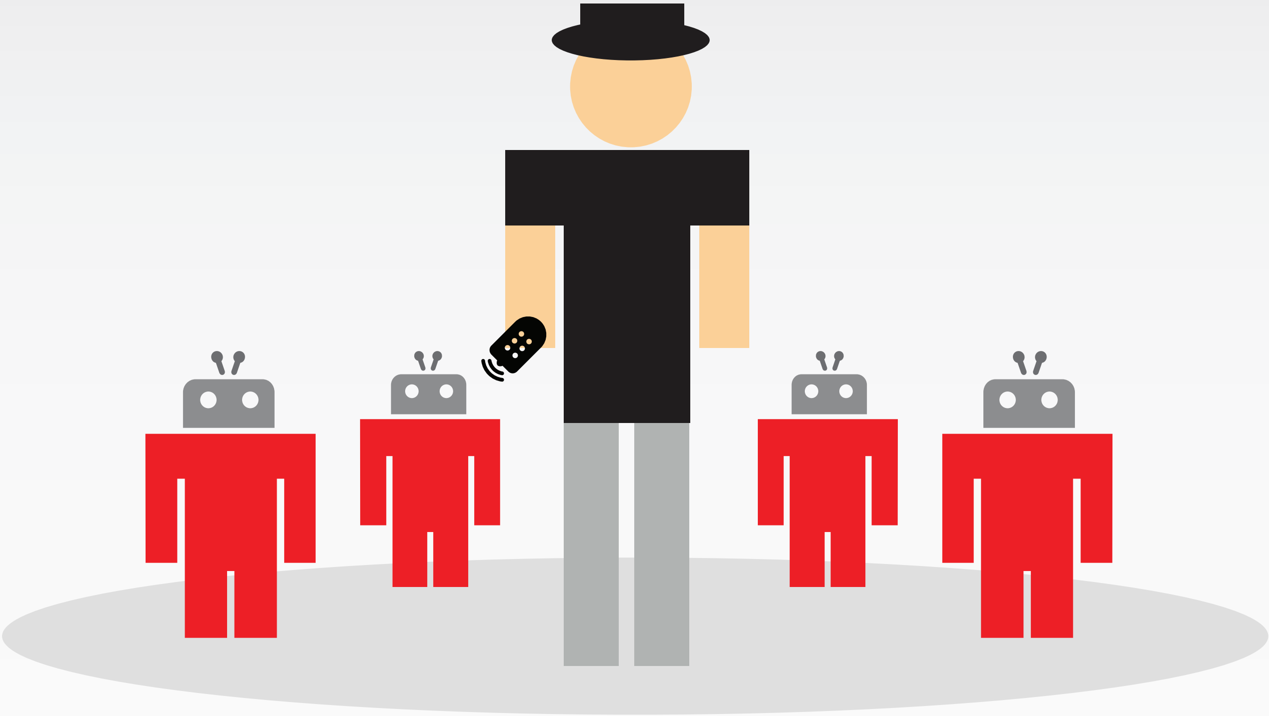


YOUR WAF MUST thwart Evasion Techniques

- Examine multiple attack indicators with an analytics engine and block attacks without false positives
- Compare requests over time to detect repetitive attacks, such as brute-force login or DDoS attacks

> "Web application firewalls must deliver more sophisticated control at the application layer through a variety of contextual rule sets and behavioral analysis."
>
> – SANDRA KAY MILLER, Core of the Matter,
> Information Security Magazine

Protect applications from automated attacks.



YOUR WAF MUST Prevent Automated Attacks and Shut Down Bots

- Analyze browser capabilities to distinguish bots from legitimate Web browsers
- Detect an excessive number of Web requests in a short period of time

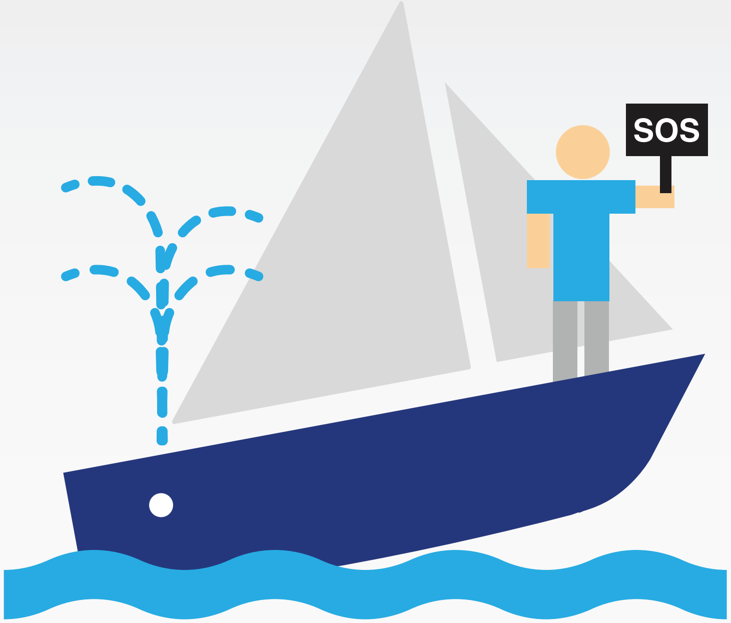
CHALLENGE #5

Identify malicious users or illicit sites before the damage is done.

YOUR WAF MUST Recognize Known Malicious Sources

- Detect access from anonymous proxies and Tor networks
- Restrict access by location to eliminate unwanted traffic and to thwart DDoS attacks originating from a specific country
- Recognize users referred from a phishing site
- Link to a cloud-based community defense that shares accurate, live information about hackers, bots, and fraudsters

Patch vulnerabilities that could leave applications exposed for days or months.



YOUR WAF MUST Virtually Patch Vulnerabilities

- Prevent attempts to exploit application vulnerabilities
- Provide input validation, HTTP protocol validation, and attack signatures that can block most vulnerability exploits out-of-the-box
- Integrate with application scanners and build custom policies to ensure strict security measures are applied to known application vulnerabilities

> "Web Application Firewalls genuinely raise the bar on application security…they 'virtually' patch the application faster than code fixes can be implemented."
>
> – ADRIAN LANE, Securosis

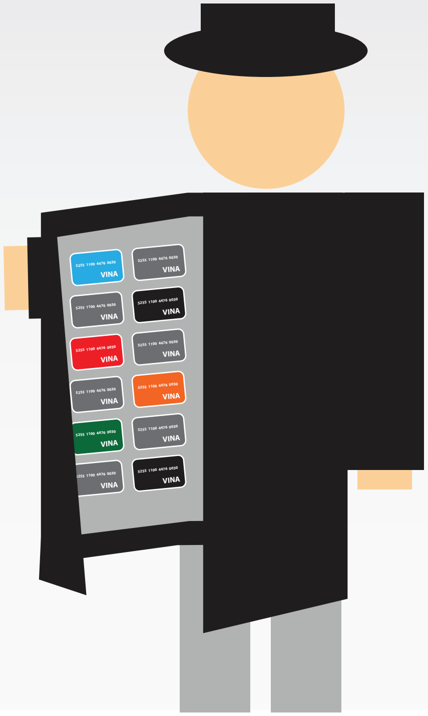
Detect users infected with malware.

YOUR WAF MUST Stop Fraud Malware

- Analyze end user attributes and Web traffic patterns for the tell-tale signs of malware infection and then block malware-infected devices
- Monitor a suspect user for a specified period of time, generate an alert, or integrate with a fraud management solution to open an investigation case

CHALLENGE #8

Fortify applications against fraudulent transactions.

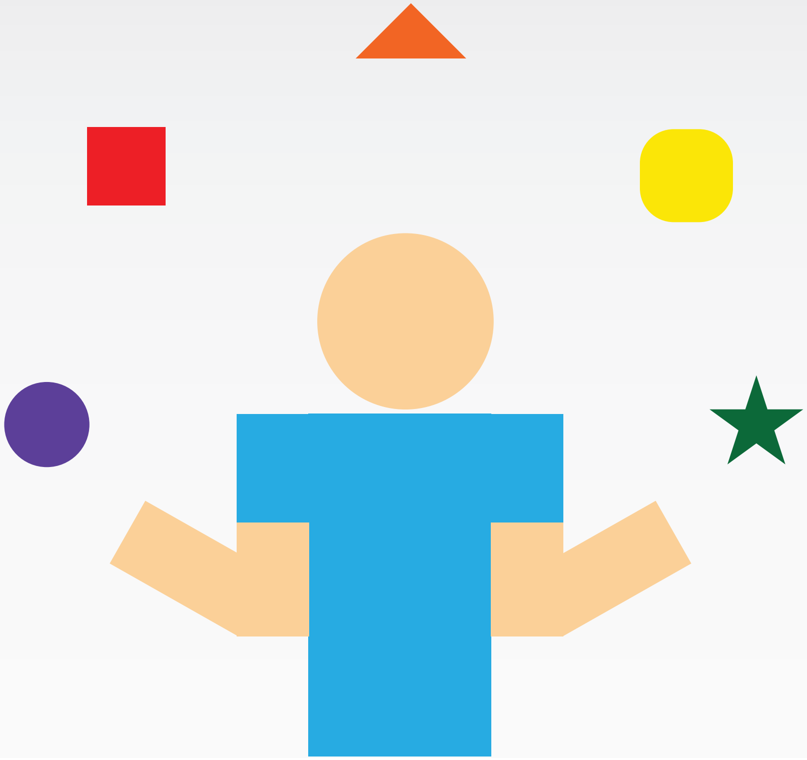


YOUR WAF MUST Stop Fraudulent Transactions

- Mitigate payment and new account fraud without requiring application changes
- Integrate with cloud-based fraud security solutions to extract and analyze a number of user and transaction attributes including browser irregularities, known fraudulent devices, and suspicious payment information
- Correlate fraud risk data with Web attack and user information to accurately identify and stop fraud

> “A layered fraud prevention approach provides defense in depth, and it is the best policy for preventing and containing losses that result from today’s and tomorrow’s threats.”
>
> – AVIVAH LITAN, Gartner

Support diverse application architectures.

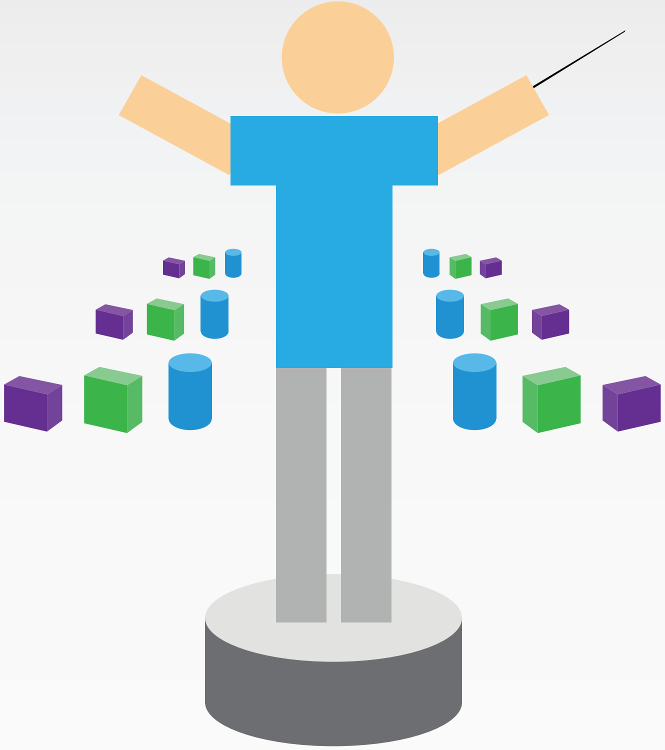


YOUR WAF MUST Support On Premise and Cloud Deployments

- Maintain flexible, inline and non-inline configuration options that support unique on premise requirements
- Support virtual appliance solutions for private clouds and cloud-based security services

> "Cloud-based security services offer an easy and effective way to make websites faster and protect websites against hackers and bots."
>
> – LAWRENCE PINGREE, Gartner

Manage multiple Web application firewalls.



YOUR WAF MUST Streamline and Scale Operations

- Incorporate point-and-click security policies
- Provide centralized management for synchronized policies and application profiles across all Web application firewalls, even those in separate locations
- Deliver detailed, actionable security event information

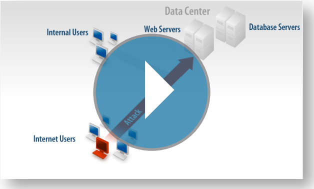
Additional Resources

The Future of Web Security:

10 Things Every Web Application Firewall Should Provide

IMPERVA

DOWNLOAD THE FUTURE OF WEB SECURITY WHITE PAPER



VIEW WEB APPLICATION SECURITY DEMO

Share this eBook

About Imperva

Imperva is a pioneer and leader of a new category of business security solutions for critical applications and high-value data in the data center. Imperva's award-winning solutions protect against data theft, insider abuse, and fraud while streamlining regulatory compliance by monitoring and controlling data usage and business transactions across the data center, from storage in a database or on a file server to consumption through applications.

LEARN MORE

Find Us on the Web | Contact Us Direct | Read our Blog

Imperva Headquarters
3400 Bridge Parkway, Suite 200
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

Toll Free (U.S. only): +1-866-926-4678
www.imperva.com

IMPERVA®

Share this eBook