Penta SECURITY
Web and Data Security Platforms

MANAGING AND PROTECTING YOUR VALUABLE DATA

An Essential Security Guide for the New Age Enterprise

New age enterprises integrate information, processes, work and people by embracing the latest technology to gain competitive advantage, drive innovation and stay relevant to their customers.

Securing the New Age Enterprise

Security threats have gone beyond being mere annoyances to the realm of highly sophisticated attacks. It is now a **domain of highly motivated professional hackers** because of the **potentially lucrative financial benefits**.

Managing a Digital Enterprise

Today's businesses are more connected, context aware, digital, and data-driven than ever. Consumer and enterprise customer experiences are melding seamlessly into one.

Data Privacy Concerns

Data is the new currency in the digital economy. Protecting the digital business is more than protection from cyber-threats, it also includes the confidentiality, integrity, and availability of your digital assets.

Industry & Regulation Compliance

Stringent regulations and new compliance requirements govern how an organization approaches the detection and prevention of cyber threats.

Solutions for Cloud Security

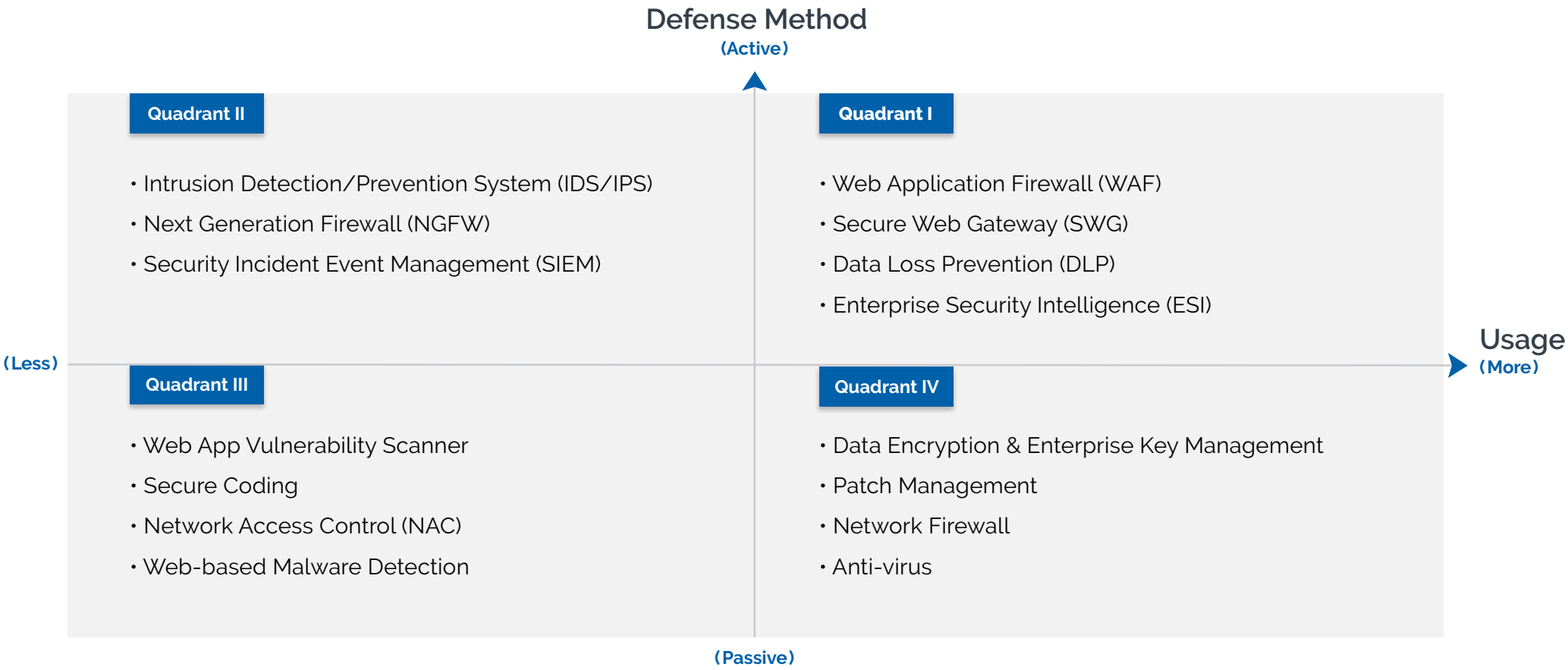
With the recent improvements in cost and efficiency, organizations are increasingly moving applications and data to the cloud. This introduces additional security concerns that need to be addressed.

Managing a Mobile Workforce

With more organizations implementing flexible workspaces and Bring Your Own Device (BYOD) policies, it is now critical to secure mobile access and devices.

Defense Methods for Security

Technologies such as the cloud, the Internet of Things (IoT), mobility, and big data introduce unique threats and risks. **Adopting a widely used and active security system** will help enterprises prevent, detect, respond and recover from advanced threats.



Securing Your New Age Enterprise

Finding the Right Firewall

As new age enterprises continue adopting digital technologies, most attackers are using methods which are specifically aimed at **exploiting potential weak spots in the web application** software itself. As new mechanisms and attack vectors are constantly invented and old ones are upgraded, a **WAF is the best protection for the new age enterprise**.

OWASP Top 10 (2013)	Network Firewall	IDS/IPS	WAF
A1 Injection	✗	△	✓
A2 Broken Authentication and Session Management	✗	△	✓
A3 Cross-Site Scripting (XSS)	✗	△	✓
A4 Insecure Direct Object References	✗	✗	✓
A5 Security Misconfiguration	✗	✗	✓
A6 Sensitive Data Exposure	✗	✗	✓
A7 Missing Function Level Access Control	✗	✗	✓
A8 Cross-Site Request Forgery (CSRF)	✗	✗	✓
A9 Using Components with Known Vulnerabilities	✗	✓	✓
A10 Unvalidated Redirects and Forwards	✗	✗	✓

Securing Your New Age Enterprise

Top 6 Security Threats*

The enterprise threat landscape continues to evolve, and there is a constant battle between cyber criminals and security experts. **A combination of attacks listed below are used to cause more damage.**

Injection
(not limited to just SQL injection)

Cross Site Scripting
(XSS)

Cross Site Request Forgery
(CSRF)

Broken Authentication and Session Management

Security Misconfiguration

Sensitive Data Exposure

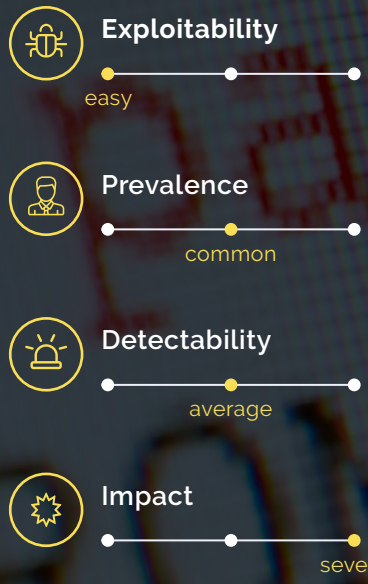
*Threat risk rating based on OWASP methodology

The Threat Risk Rating in the following pages are based on "OWASP Risk Rating Methodology." - OWASP. N.p., n.d. Web. 2016.

TOP 6 THREATS

Injection

(not limited to just SQL injection)



Injection attacks involve the insertion of malicious code into web applications. There are many types of injections: SQL, Hibernate Query Language (HQL), LDAP, XPath, XQuery, XSLT, XML, OS command injection to name a few.

How can it affect your enterprise?

- The hacker can delete, modify, or steal your data
- He or she can compromise the safety and trust of user data
- A company's competitiveness and reputation can be at stake

Protecting against Injection Attacks

- Do not store sensitive data in clear-text in a database
- Do not use dynamic query interfaces
- Review your web applications' code before going live

IN THE NEWS

SQL injection attacks at Qatar National Bank expose one million credit cards to the dark web

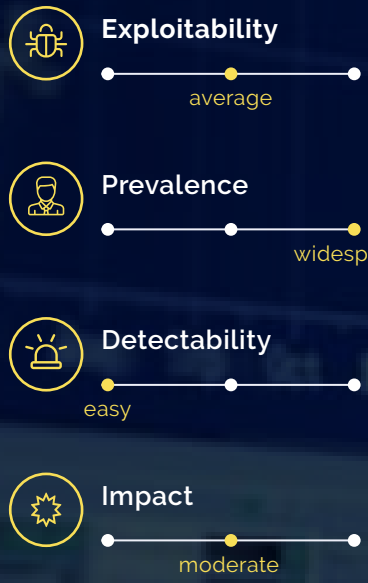
Find Out More

134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems

Find Out More

TOP 6 THREATS

Cross-Site Scripting (XSS)



XSS vulnerabilities permit attackers to include malicious code in the content a website sends to a victim's browser. The malicious code is typically written in JavaScript or any other type of code that will be interpreted by the browser.

How can it affect your enterprise?

- These attacks can scan and exploit internet applications
- Attacks can result in key logging as well as identity and cookie theft
- The attacker can impersonate the user to carry out unauthorized transactions

Protecting against Cross-Site Scripting

- Ensure your website is accessible only via SSL connections
- Only place secure cookies on the user's browser
- Use an automated WAF to check for XSS vulnerabilities

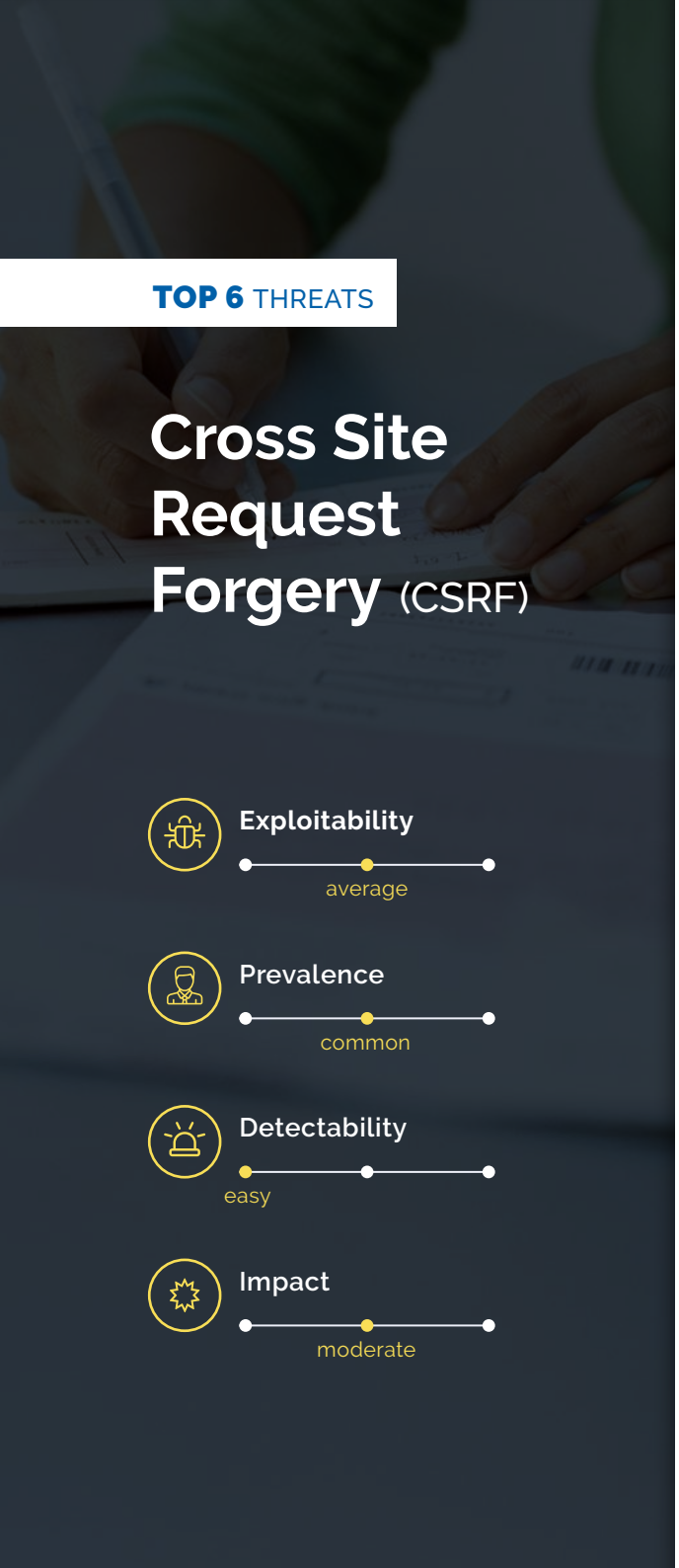
IN THE NEWS

320 million Apple iMessage users and 3,593 websites using Zen Cart affected by XSS attacks

Find Out More

400 million Yahoo Mail users vulnerable to XSS attack

Find Out More



TOP 6 THREATS

Cross Site Request Forgery (CSRF)

Exploitability
average

Prevalence
common

Detectability
easy

Impact
moderate

Hackers use Cross Site Request Forgery (CSRF) to exploit the user's browser into performing an action on a website like transferring funds or changing the email address.

How can it affect your enterprise?

- The attacker can make arbitrary HTTP requests on behalf of a victim
- Users can be redirected to a phishing page that gathers sensitive information
- It can harm your reputation and cause financial loss by compromising your users' information

Protecting against CSRF Attacks

- Generate random tokens in addition to secure cookies to authenticate users
- Use CAPTCHAs to re-authenticate users
- Use penetration testing and code analysis to detect CSRF attacks

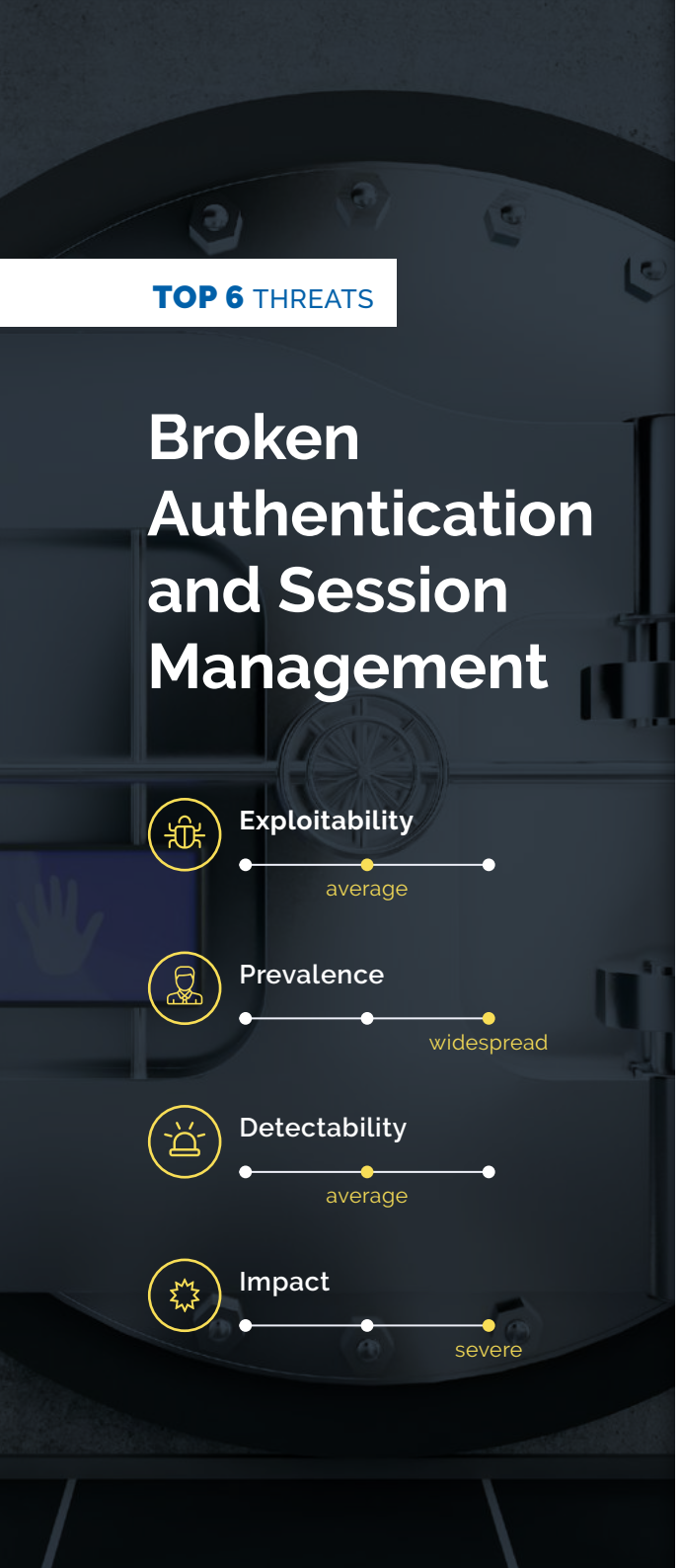
IN THE NEWS

CSRF attack alters DNS settings and compromises 300,000 home routers

Find Out More

CSRF bug exposes EVERY PayPal account to hijacking

Find Out More



TOP 6 THREATS

Broken Authentication and Session Management

Exploitability
average

Prevalence
widespread

Detectability
average

Impact
severe

These attacks are caused when hackers attempt to steal accounts from others or to disguise their actions using flaws in the authentication or session management functions (like passwords, exposed accounts, session IDs) to impersonate users.

How can it affect your enterprise?

- It can make your organization vulnerable to brute force attacks
- The trust that your users have in your web services is lost
- The attacks can cause financial loss due to data privacy violations

Protecting against Broken Authentication and Session Management

- Use SSL, two factor authentication and enforce strong passwords
- Rotate session IDs after successful logins
- Use authentication tokens to identify and manage users until they logout

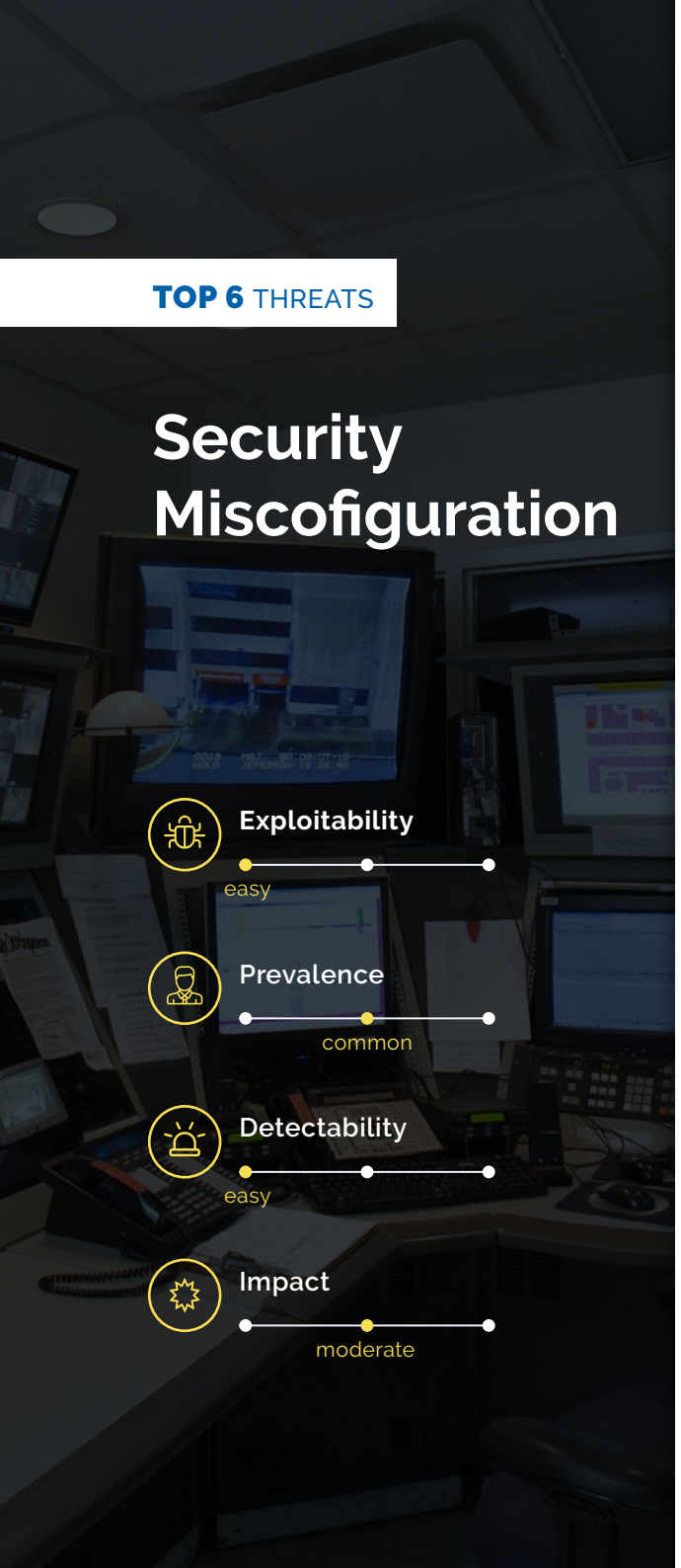
IN THE NEWS

LinkedIn beefs up security to add session management after data breach exposes nearly 6.5 million user accounts

Find Out More

Forced browsing, account harvesting, and broken authentication compromise Hilton's loyalty club members' accounts

Find Out More



TOP 6 THREATS

Security Miscofiguration

Exploitability
easy

Prevalence
common

Detectability
easy

Impact
moderate

Security Misconfiguration attacks happen when security settings are re-defined and the system is compromised, giving hackers access to private data.

How can it affect your enterprise?

- Your reputation is at stake when sensitive data is stolen and modified
- The attacks can cause unplanned downtime due to an IT lockdown
- It may result in severe financial loss as recovering data is expensive

Protecting against Security Misconfiguration

- Prevent human error by ensuring IT security managers are aware of security trends
- Update software and disable unnecessary ports, accounts and services
- Remove sensitive information from log reports

IN THE NEWS

Security misconfiguration exposes thousands of health records in Californian hospitals

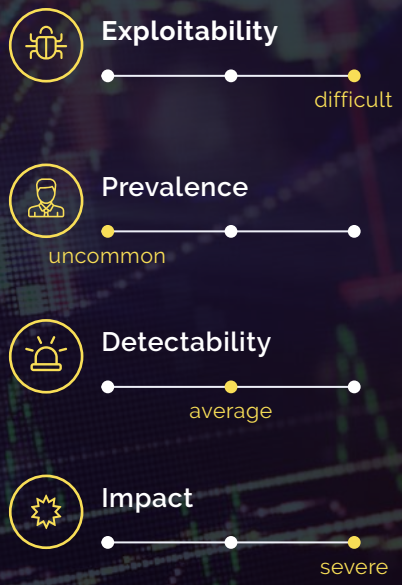
Find Out More

Misconfigured server exposes personal information of 146,000 students at Indiana University

Find Out More

TOP 6 THREATS

Sensitive Data Exposure



Companies have access to their customers' passwords, credit card numbers, health records, and other personal information. Data can be stolen when it is at rest in the system, in transit or in a backup store.

How can it affect your enterprise?

- Sensitive Information is protected by laws, regulations, and policies
- Severe legal and financial implications caused by data theft
- Intruders can gain access to confidential insider information

Protecting against Sensitive Data Exposure

- Change default usernames and passwords
- Minimize exposure by restricting access and using encryption
- Do not store unnecessary logs and other information

IN THE NEWS

Hollywood hospital pays hackers to regain control of its IT systems

Find Out More

Personal and medical information for nearly 5 million patients compromised by UCLA Health System

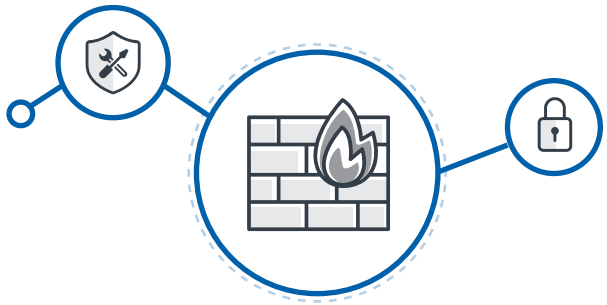
Find Out More

Securing Your New Age Enterprise

Finding the Right WAF

Enterprises are tasked with providing secure access to their web services. A Web Application Firewall (WAF) is one of the most effective defenses against common and unknown attacks, while providing easy security settings and operational convenience. **Here are the key considerations while selecting a WAF**.

1 High-end Security



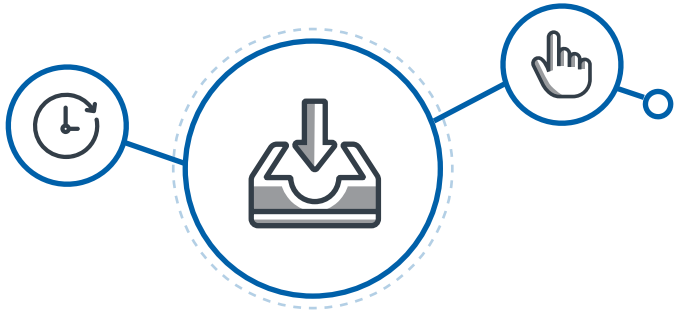
- Protection from unknown attacks using advanced technology, such as the **Contents Classification and Evaluation Processing (COCEP™) technology.**
- Extremely **low false positive rates**
- Validity testing to **prevent personal information leakage**

2 Stable, High Performance

- Engine optimization to **provide enhanced performance**
- **High processing power** with in-memory computing capability
- **Stable performance** even with strict security policy settings enabled

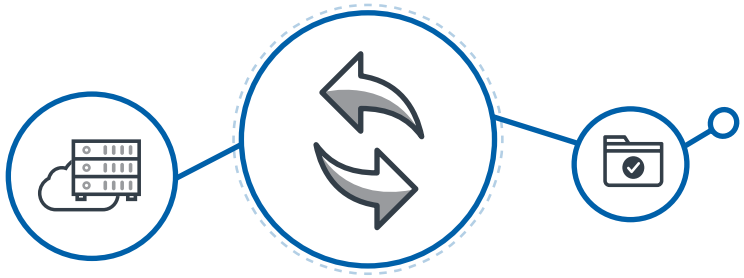
Finding the Right WAF

3 Easy to Install & Configure



- **Minimal changes** to existing systems
- **Intuitive and easy-to-use** GUI management console
- **Reduce time spent** on web security management

4 Works in Various Environments



- On-premise, virtualized environments, or cloud deployment
- When on-premise, **can be deployed in Reverse Proxy, Inline, or High Availability configuration modes**
- When virtualized or cloud deployment, **supports various hypervisors**

WAPPLES

Intelligent Web Application Security

As the virtual environment evolves and expands, the threats against web applications continue to proliferate and grow ever stronger. While it is vital that organizations **secure their web applications**, it is also imperative that they do so in an **efficient, accurate, and cost-effective manner**.

WAPPLES decreases administrative costs and increases efficiency and security using:

1

Intelligent Threat Engine

A logic analysis based engine that intelligently detects and blocks both known and unknown attacks.

2

Proven Solution

A tested and proven solution to web application security with over 3000 satisfied customers.

3

User-Intuitive GUI

A user-intuitive GUI that enables web application management to be performed by a small team.

The Best Solution for Web Security

Frost & Sullivan has named WAPPLES as the No. 1 WAF in APAC


Penta SECURITY
Web and Data Security Platforms
WAPPLES is an award-winning WAF that accurately detects and prevents web attacks.
Find out how WAPPLES can secure your enterprise.
Visit the site