

Traditional Security Infrastructure is Failing

Peter Paszkiewicz

GASystems

QUESTNET JULY 13 2012 CAIRNS

www.gasystems.com.au

iTrust





The Web Presence Demand





INTERNET USERS

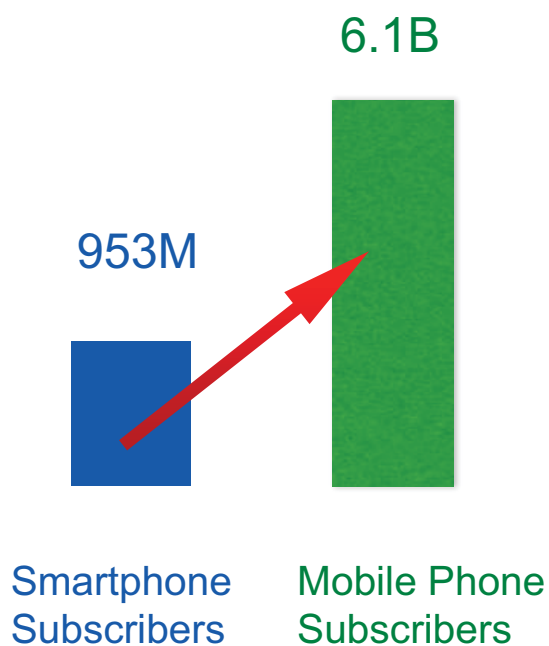
2006 1.2B Internet Users
18% of 6.5B people

2011 2.4B Internet Users
35% of 7B people

KPCB 2012



Huge potential for the mobile web

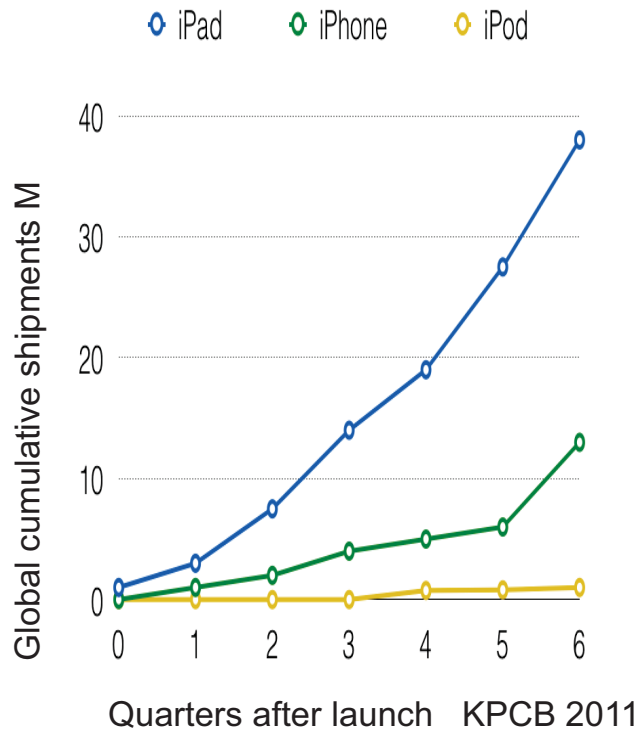


KPCB 2012



Tablets – are the chosen platform

iTrust



PentaSECURITY

The Need for Effective Web Application Security

PentaSECURITY



75% of ALL threats target
the Web Application layer

Gartner

93% of organizations
hacked in the past two years
were breached via insecure
web applications

Ponemon Institute

Ponemon Institute

- White House Cybersecurity Advisor, Richard Clarke

conjecture of relative breach impact is based on publicly disclosed information regarding leaked records and financial losses

Attack Type

- SQL Injection
- URL Tampering
- Spear Phishing
- 3rd Party Software
- DDoS
- SecureID
- Unknown

Size of circle estimates relative impact of breach in terms of cost to business

Feb 2011 Mar 2011 Apr 2011 May 2011 Jun 2011 Jul 2011 Aug 2011

Attackers/Targets shown in chart:

- Bethesda Software
- Italy PM Site
- IMF
- Northrop Grumman
- Fox News X-Factor
- Citigroup
- Spanish Nat Police
- Gmail Accounts
- PBS
- Booz Allen Hamilton
- Vanguard Defense
- Sega
- PBS
- SOCA
- Malaysian Gov Site
- Peru Special Police
- Monosanto
- SK Communications Korea
- AZ Police
- NATO
- US Senate
- Turkish Government
- Nintendo
- Lockheed Martin
- Sony BMG Greece
- L3 Communications
- RSA
- HB Gary
- Epsilon
- Sony

Are Your Credit Card Details Safe ?

iTrust



Subscription based provider of
geopolitical analysis

George Friedman CEO

*"our website had been hacked and our
customer credit card and other
information had been stolen"*

THE AUSTRALIAN

Dec 29 2011 ...

"credit card details of **MP Malcolm Turnbull,
and David Smorgon** have been published on the
internet"

... tens or hundreds of thousands of people whose
customer information was stolen... The big four
Australian banks, BHP Billiton and energy giant
Woodside Petroleum were also caught up in the
breach. Foreign casualties include the US Army, the
US Department of Homeland Security, Air New Zeala
nd, the NZ Department of Prime Minister and Cabin
et, Apple, Google, American Express, Microsoft,
Coca- Cola, Boeing and Sony."



Penta SECURITY

Is your Customer/User data safe ?

iTrust



GAMEARENA

Security Advisory

We have reset the passwords of GameArena and Games Shop customers, after the sites were victims of a hacking attack.

Information that might have been obtained was limited to BigPond Games usernames, the email address used to join the site and the encrypted GameArena and Games Shop passwords.

No financial or credit card details were kept on the sites.

While your password for access to the site has been changed, and the new password has been emailed to you, we encourage you to change it at any other site where you might have used the same password.

Telstra BigPond Broadband password details, used for games service access, have not been affected.

If you have not received an email with your new password, [please click here](#).

THE AGE Hackers hit Telstra site: 35,000 affected *May 24, 2012*

The Office of the Australian Information Privacy Commissioner, Timothy Pilgrim said in a statement

"These incidents highlight the importance of businesses ensuring that they maintain the most up to date security systems to ensure the protection of the personal information they hold about customers,"

"Having appropriate levels of security is a requirement of the Privacy Act."

Penta SECURITY



400,000 Yahoo accounts reportedly hacked,
published online

Jul 12, 2012



“...the breached appeared to be a SQL injection attack to extract the sensitive information from the database.”

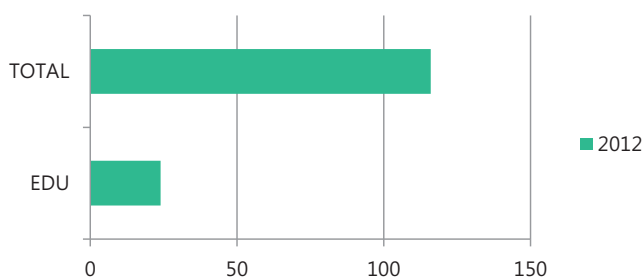


```
703:      !nemr.net:gcgo4
704:      e@yahoo.com:mercadona
705:      6@aol.com:Slayer26
706:      yahoo.com:softlink
707:      1@aol.com:nanul982
708:      @aol.com:yellow77
709:      umbc.edu:ndngpy27
710:      23@hotmail.com:tyler
711:      @cs.com:love
712:      @hotmail.com:indigo
```

```
#####
# [ - Owned and Exposed - ] #
# Brought to you by the D33Ds Company #
# Target: <censored>.yahoo.com #
# Method: Union-based SQL Injection #
#####
```

Reported Privacy Breaches in US via Hacking

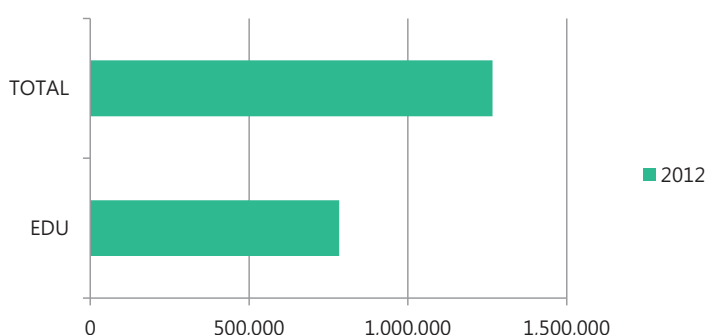
Reported Breaches 2012



Source: “www.privacyrights.org”

Privacy Breach recorded as data useful to identity thieves such as social security, account , credit card numbers

Records Taken 2012



EDUCATION SECTOR :

**20% total reported
60% total records**



BUSINESS

The Criminal Cloud

Criminals are using cloud computing to share information and to superpower their hacking techniques.

MONDAY, OCTOBER 17, 2011 BY SIDSON L. GARFINKEL

Audio

Technology Review

The cloud opens a world of possibilities for criminal computing. Unlike the zombie computers and malware that have been the mainstay of computer crime for the past decade, cloud computing makes available a well-managed, reliable, scalable global infrastructure that is, unfortunately, almost as well suited to illicit computing needs as it is to legitimate business.

The mass of information stored in the cloud—including, most likely, your credit card and Social Security numbers—makes it an attractive target for data thieves. Not only is more data centralized, but for the security experts and law enforcement agencies trying to make the cloud safe, the very nature of the cloud makes it difficult to catch wrongdoers. Imagine a virtual Grand Central Station, where it's easy to mix in with the crowd or catch a ride to a far-away jurisdiction beyond the law's reach.

Most of all, the cloud puts immense computing power at the disposal of nearly anyone, criminals included. Cloud criminals have access to easy-to-use encryption technology and anonymous communication channels that make it less likely their activities will be intelligible to or intercepted by authorities. On those occasions that criminals are pursued, the ability to rapidly order up and shut down computing resources in the cloud greatly decreases the chances that there will be any clues left for forensic analysis.

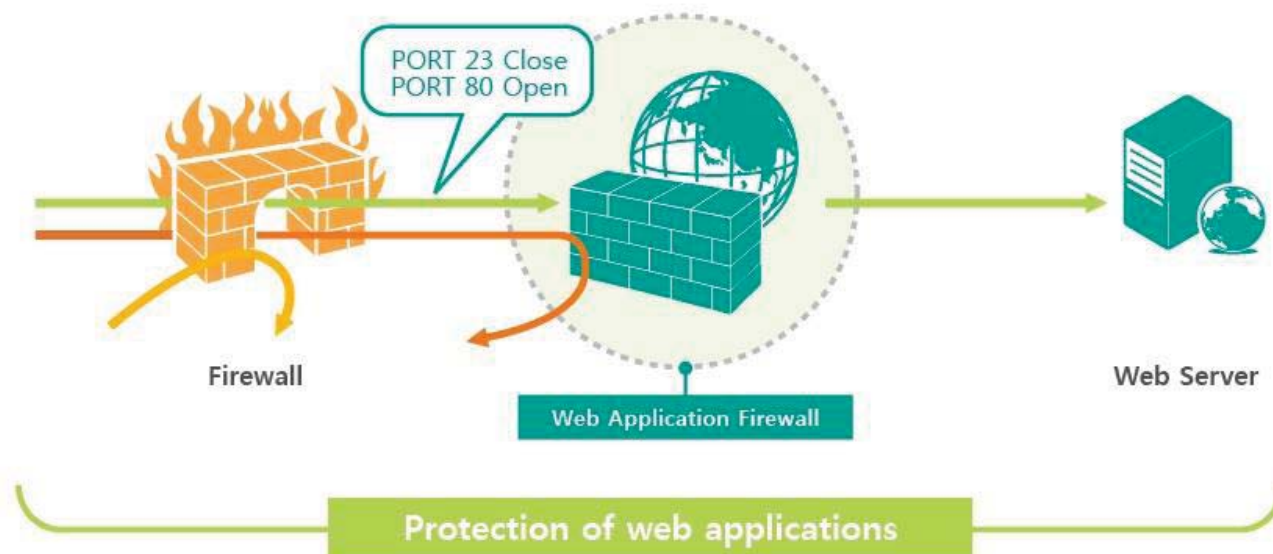
Widely Available to Criminals

Source: 17 October 2011
Technology Review

“..... cloud computing makes available a well-managed, reliable, scalable global infrastructure that is, unfortunately, almost as well suited to illicit computing needs as it is to legitimate business.”

The Protection: Web Application Firewall

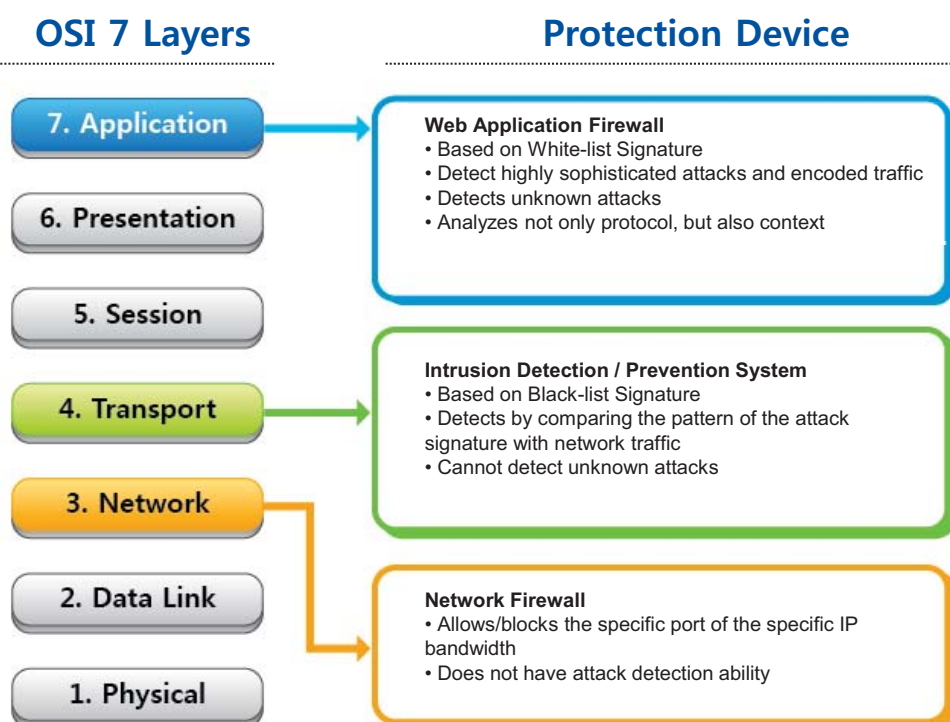




- Protects against web attacks
- Prevents leakage of personal, confidential, and/or proprietary information
- Enables regulatory compliance

Network Firewall, IDS/IPS, or WAF

WAFs protect the OSI 7 (Application) Layer





OWASP Top 10 (2010)	Network Firewall	IDS / IPS	WAF
A1: SQL Injection	X	△	√
A2: Cross Site Scripting (XSS)	X	△	√
A3: Broken Authentication and Session Management	X	△	√
A4: Insecure Direct Object References	X	X	√
A5: Cross Site Request Forgery (CSRF)	X	X	√
A6: Security Misconfiguration	X	X	√
A7: Failure to Restrict URL Access	X	X	√
A8: Insecure Cryptographic Storage	X	X	√
A9: Insufficient Transport Layer Protection	X	√	√
A10: Unvalidated Redirects and Forwards	X	X	√

WAF is only solution to protect against OWASP Top 10 Threats

WAF delivers compliance

iTrust

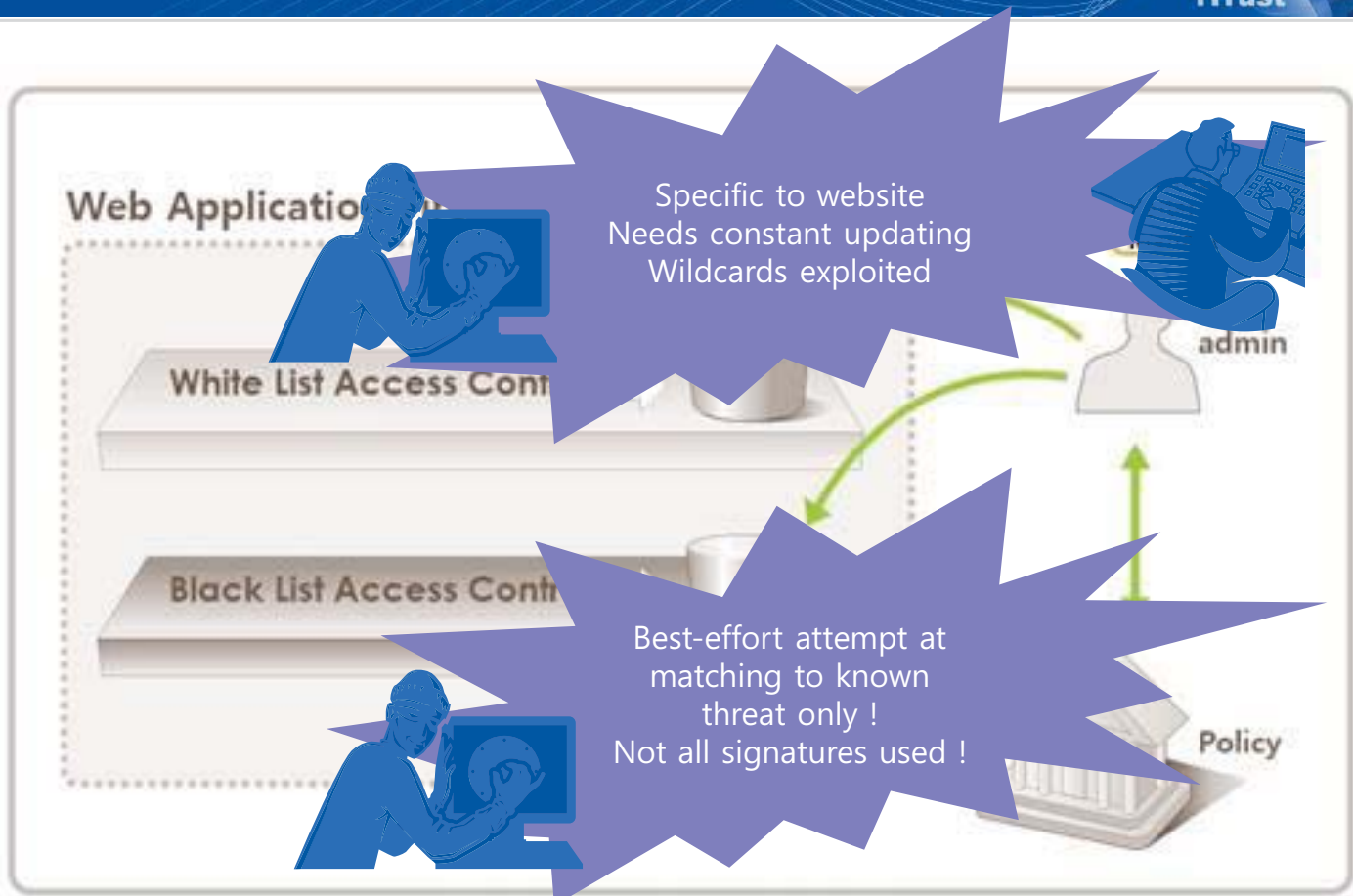
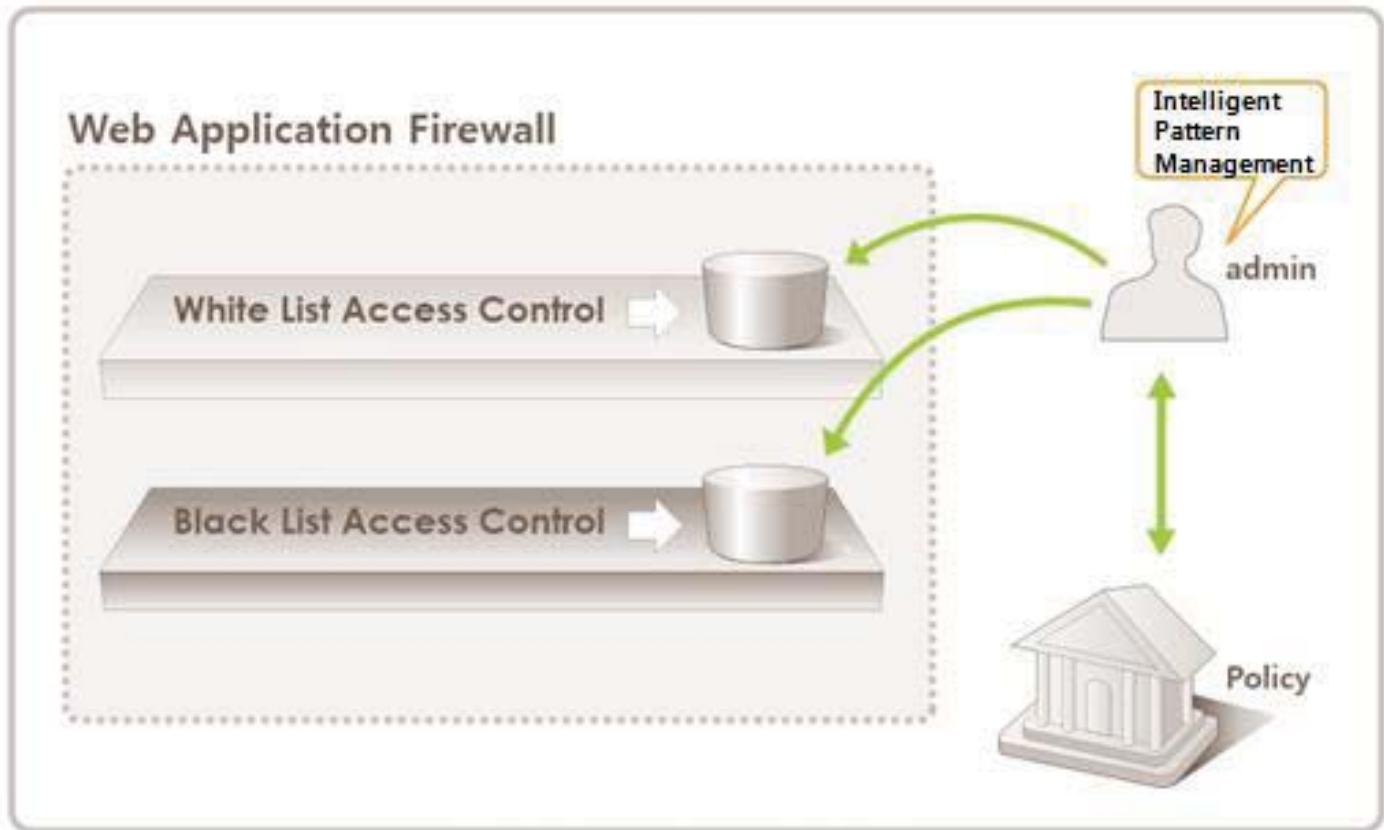


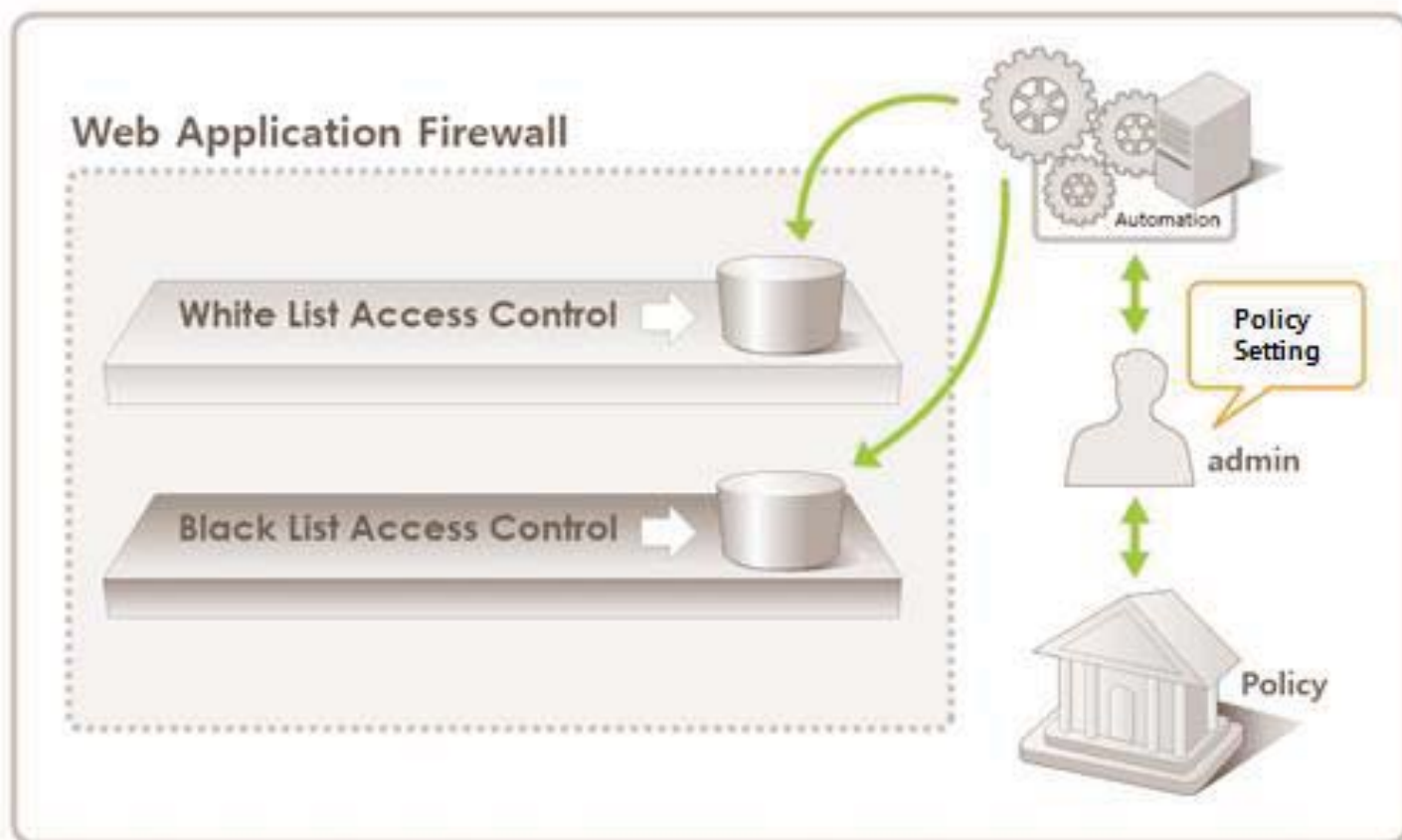
Payment Card Industry Data Security Standard



Attorney General for Australia May 2 2012

“Australia’s privacy laws will be reformed to better protect people’s personal information, simplify credit reporting arrangements and give new enforcement powers ... The changes will be introduced into the Parliament in the winter sitting period.”







“There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time.

The threat is real.

You are compromised; you just don't know it ! ”

Gartner Inc 2012

PentaSECURITY

PentaSECURITY

Introducing WAPPLES

The Intelligent Web Application Firewall
The only 3rd Generation WAF



The only solution that delivers

iTrust



Agility To Your
Web presence

Change website anytime
when you need to



Penta SECURITY

28

The only solution that delivers

iTrust



Agility To Your
Web presence

Change website anytime
when you need to

Protects your
business

No brand damage or legal liability



Penta SECURITY

29

The only solution that delivers

iTrust



**Agility To Your
Web presence**

Change website anytime
when you need to

**Protects your
business**

No brand damage or legal liability

**Protects your
customers**

Prevents private and
credit card data leakage



Penta SECURITY

30

The only solution that delivers

iTrust



**Agility To Your
Web presence**

Change website anytime
when you need to

**Protects your
business**

No brand damage or legal liability

**Protects your
customers**

Prevents private and
credit card data leakage

**Secured Web
presence**

Protects against all threats
known and unknown



Penta SECURITY

31

The only solution that delivers

iTrust



Agility To Your Web presence

Change website anytime when you need to

Protects your business

No brand damage or legal liability

Protects your customers

Prevents private and credit card data leakage

Secured Web presence

Protects against all threats known and unknown

Frees Resources

No administration or 3rd party testers



Penta SECURITY

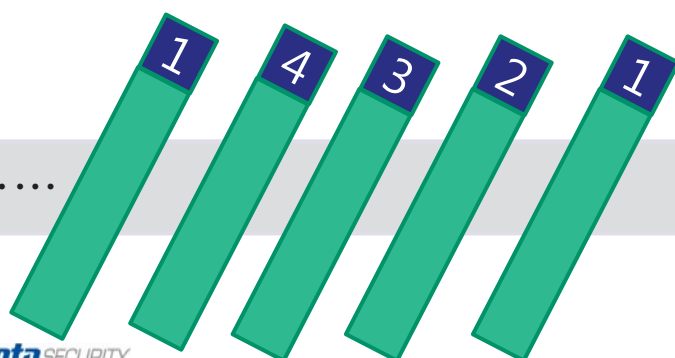
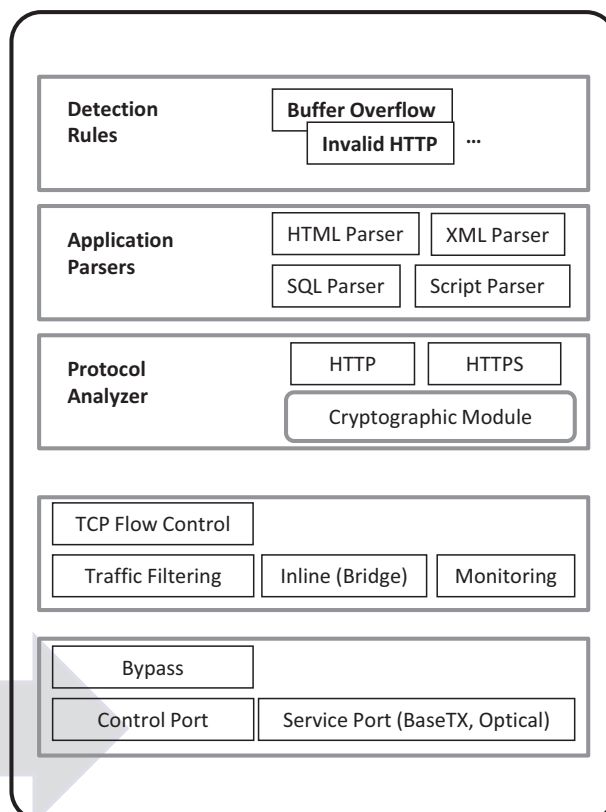
32

WAPPLES: The Intelligent WAF

iTrust



WAPPLES reassembles the payload Of packets and applies rules to the HTML user context



Penta SECURITY

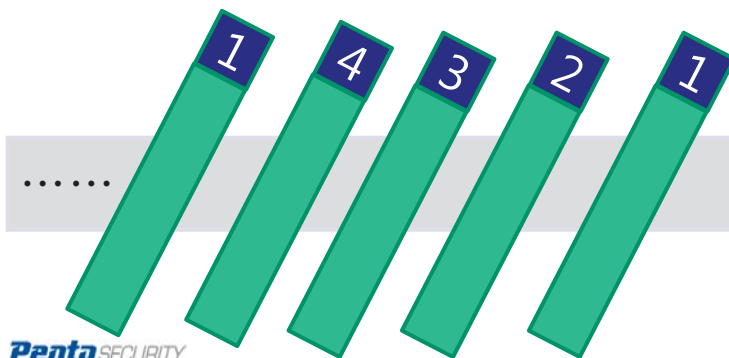
33

WAPPLES: The Intelligent WAF

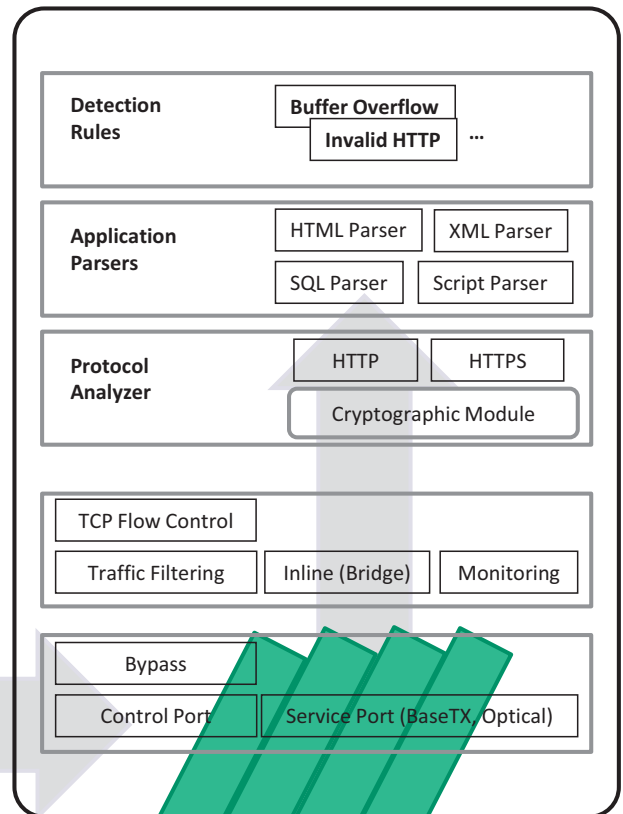
iTrust



WAPPLES reassembles the payload
Of packets and applies rules to the
HTML user context



PentaSECURITY



34

WAPPLES: The Intelligent WAF

iTrust

INTELLIGENT ENGINE AND RULE SET

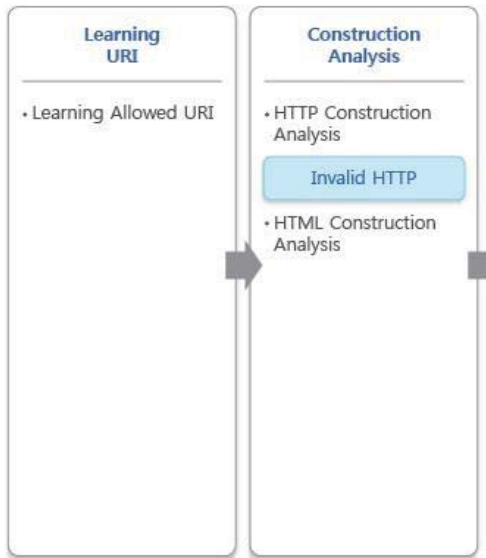


PentaSECURITY

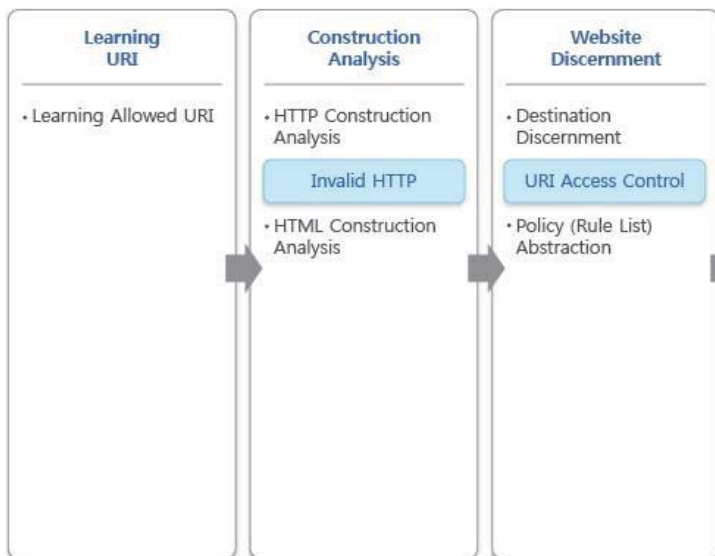
35



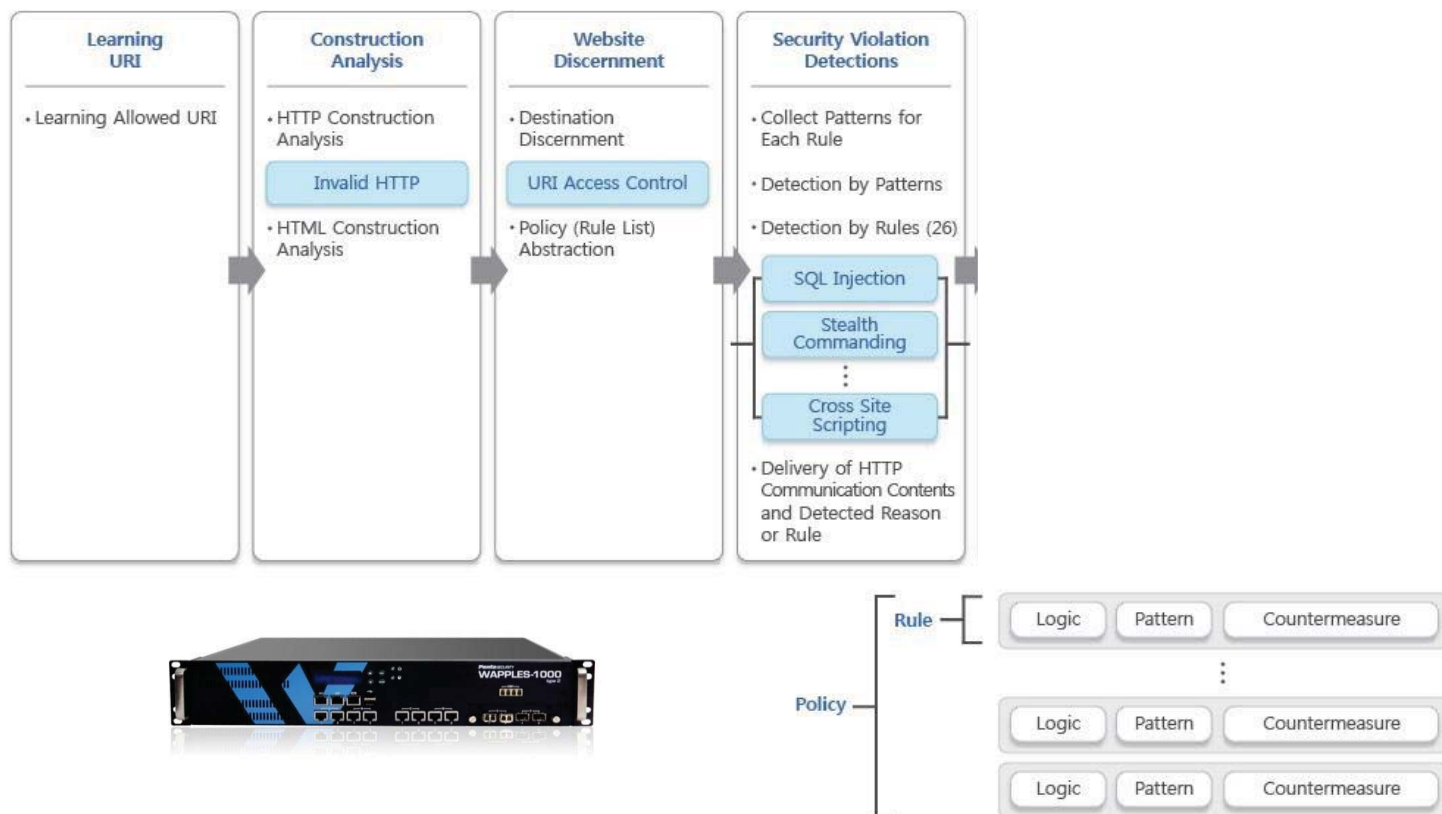
INTELLIGENT ENGINE AND RULE SET



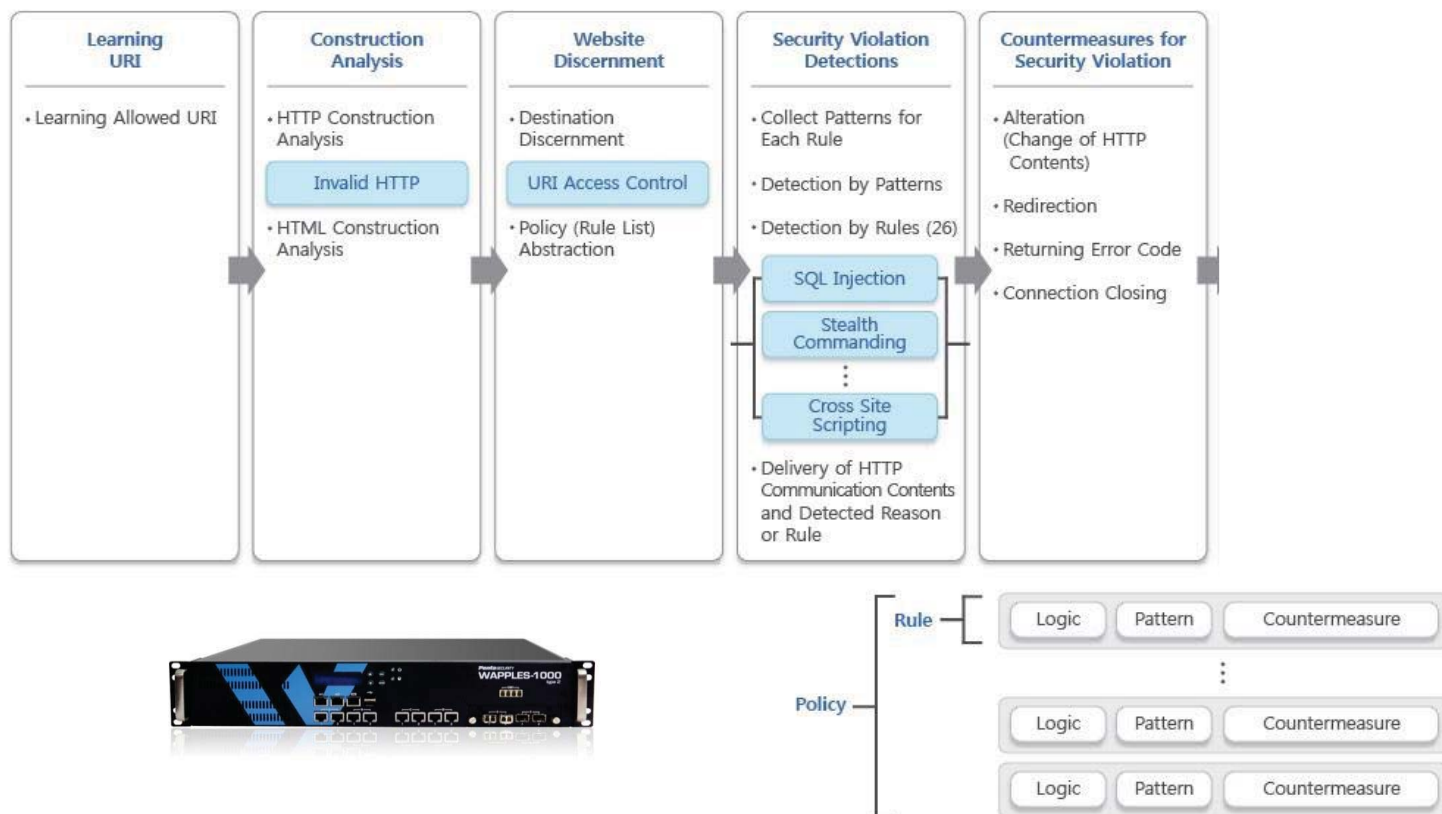
INTELLIGENT ENGINE AND RULE SET



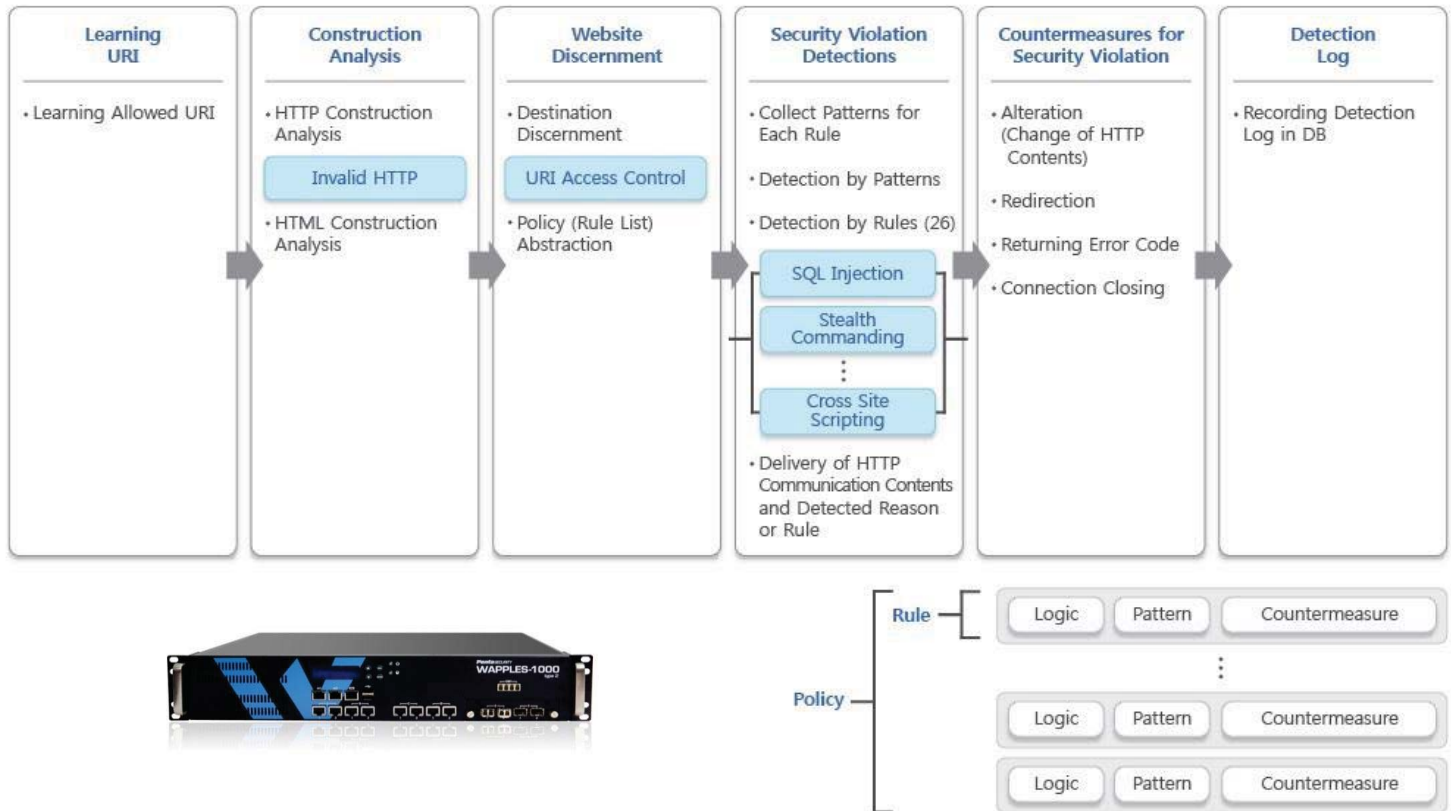
INTELLIGENT ENGINE AND RULE SET



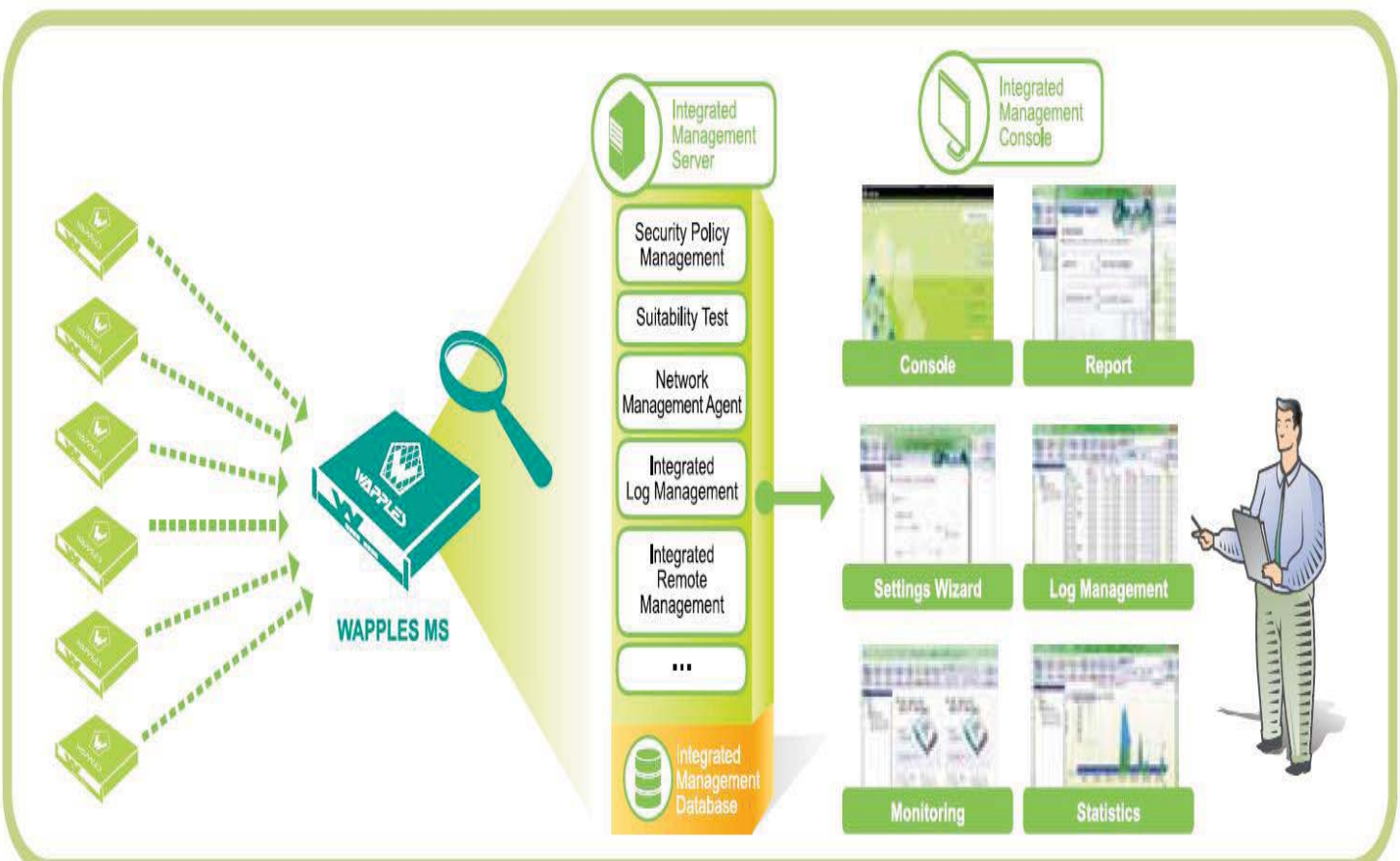
INTELLIGENT ENGINE AND RULE SET



INTELLIGENT ENGINE AND RULE SET



Comprehensive Management



Secure your Internet Presence with Wapples

iTrust



SECURE YOUR WEB SITES

AUTOMATE THE PROCESS
NO SIGNATURES, UPDATES OR TESTING

SET AND FORGET

PROTECT AGAINST KNOWN AND UNKNOWN
THREATS

TRUSTED AND PROVEN IMPLEMENTATION
OVER 1,600 CUSTOMERS



Penta SECURITY

42

QUESTIONS ?

iTrust



SECURE YOUR WEB SITES

AUTOMATE THE PROCESS
NO SIGNATURES, UPDATES OR TESTING

SET AND FORGET

PROTECT AGAINST KNOWN AND UNKNOWN
THREATS

TRUSTED AND PROVEN IMPLEMENTATION
OVER 1,600 CUSTOMERS



Penta SECURITY

43