SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Web Applications Security

Radovan Gibala

F5 Networks

How does the current situation look like ?

Application Trends and Drivers

- “Webification” of applications
- Intelligent browsers and applications
- Increasing regulatory requirements (PCI)
- Untargeted attacks – BOTs
- Targeted attacks – (D)DoS
- Public awareness of breach attempts and data security
- Tough economy = constrained resources and budgets cuts increasing security risks; reducing compliance

Almost every web application is vulnerable!

- "97% of websites at immediate risk of being hacked due to vulnerabilities! 69% of vulnerabilities are client side-attacks"

  - Web Application Security Consortium http://www.webappsec.org/projects/statistics/

- "8 out of 10 websites vulnerable to attack"

  - WhiteHat "security report " http://www.whitehatsec.com/home/assets/WPstats0808.pdf

- "75 percent of hacks happen at the application."

  - Gartner "Security at the Application Level"

- "64 percent of developers are not confident in their ability to write secure applications."

  - Microsoft Developer Research

How much effort would the “fix” require ?

What are the vulnerability costs?

- The average custom business application has 150k to 250k lines of code

  -- Software Magazine
- Every 1k lines of code averages **15 critical security defects**

  -- U.S. Department of Defense
- That means there are an **average of 2.25k security defects** in every business application
- The average security defect takes **75 minutes to diagnose and 6 hours to fix**

  -- 5-year Pentagon Study
- That's **2.8k hours to diagnose** the defects **and 13.5k hours to fix** them
- Average worldwide cost of programmer = $40 per hour -- F5 Networks
- That's a cost of **$112k to diagnose** the defects and **$540k to fix** the defects

k=1,000

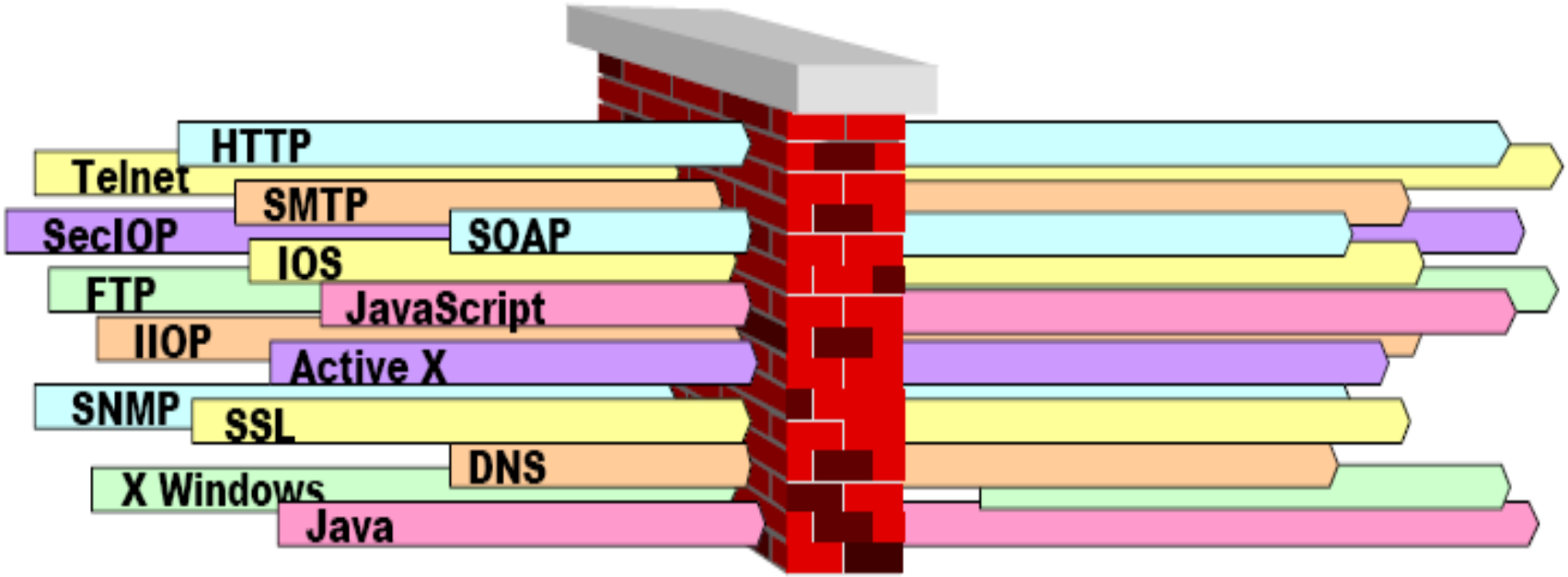
How long to resolve a vulnerability ?

Figure 6. Average number of days for vulnerabilities to be resolved (sorted by class)

[Website Security Statistics Report]

The standard way

Applications Tunnel Through Traditional Firewalls



Encryption leaves network firewalls blind

Challenges of traditional solutions

- HTTP attacks are valid requests
- HTTP is stateless, application is stateful
- Web applications are unique
  - there are no signatures for YOUR web application
- Good protection has to inspect the response as well
- Encrypted traffic facilitates attacks…
- Organizations are living in the dark
  - missing tools to expose/log/report HTTP attacks

Traditional Scan and Fix and Audits

- Scan and Fix
  - Scanners can't find all vulnerabilities
  - Scanners can't reverse engineer the code
  - Scanners can't find business logic vulnerabilities
  - When something is detected, it requires an immediate code change
  - Not a pro-active solution
- Security Code Audits
  - Extremely expensive ($25,000 for medium to small app)
  - Requires preparation and availability of the dev team.
  - Requires iterations of audit and fix
  - Each fix may add more bugs to current application or may add another vulnerability…

"We only protect from what we know,
We never protect from what we
don't know"

The way to have your web application secure

Web Application Firewall

Traditional Security Devices vs. WAF

	Network Firewall	*IPS*	*WAF*
Known Web Worms	Limited	✓	✓
Unknown Web Worms	X	Limited	✓
Known Web Vulnerabilities	Limited	Partial	✓
Unknown Web Vulnerabilities	X	Limited	✓
Illegal Access to Web-server files	Limited	X	✓
Forceful Browsing	X	X	✓
File/Directory Enumerations	X	Limited	✓
Buffer Overflow	Limited	Limited	✓
Cross-Site Scripting	Limited	Limited	✓
SQL/OS Injection	X	Limited	✓
Cookie Poisoning	X	X	✓
Hidden-Field Manipulation	X	X	✓
Parameter Tampering	X	X	✓
Layer 7 DoS Attacks	X	X	✓
Brute Force Login Attacks	X	X	✓
App. Security and Acceleration	X	X	✓

Value of a web application firewall ?

Application Security

- Virtually patch vulnerabilities in minutes without changing application code
- Reduce operation costs –
  - Ensure high application availability by stopping attacks
  - Reduce the expenses of meeting PCI security compliance requirements by showing clean scans
- Streamline application delivery
- Cut your infrastructure costs - consolidation
- Get out-of-the-box application security policies with minimal configuration
- Improve workforce efficiency
- Application visibility and reporting
- Handle changing threats with greater agility

Comprehensive Application Security

Integrated architecture with application protection and performance

Attack protection from the latest web threats

PCI compliance reporting

Protects valuable intellectual property

Smarter security and access control

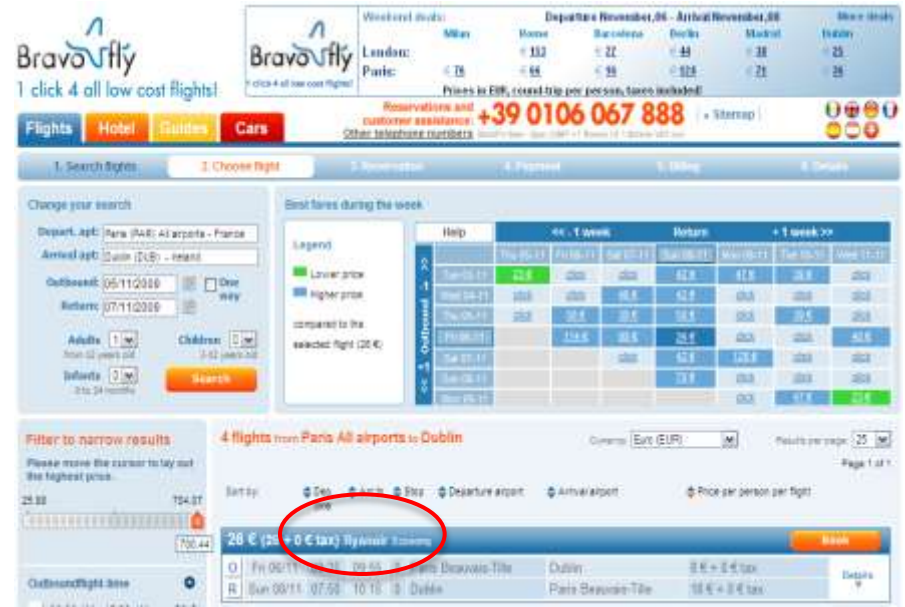
Visibility into attacks

Examples

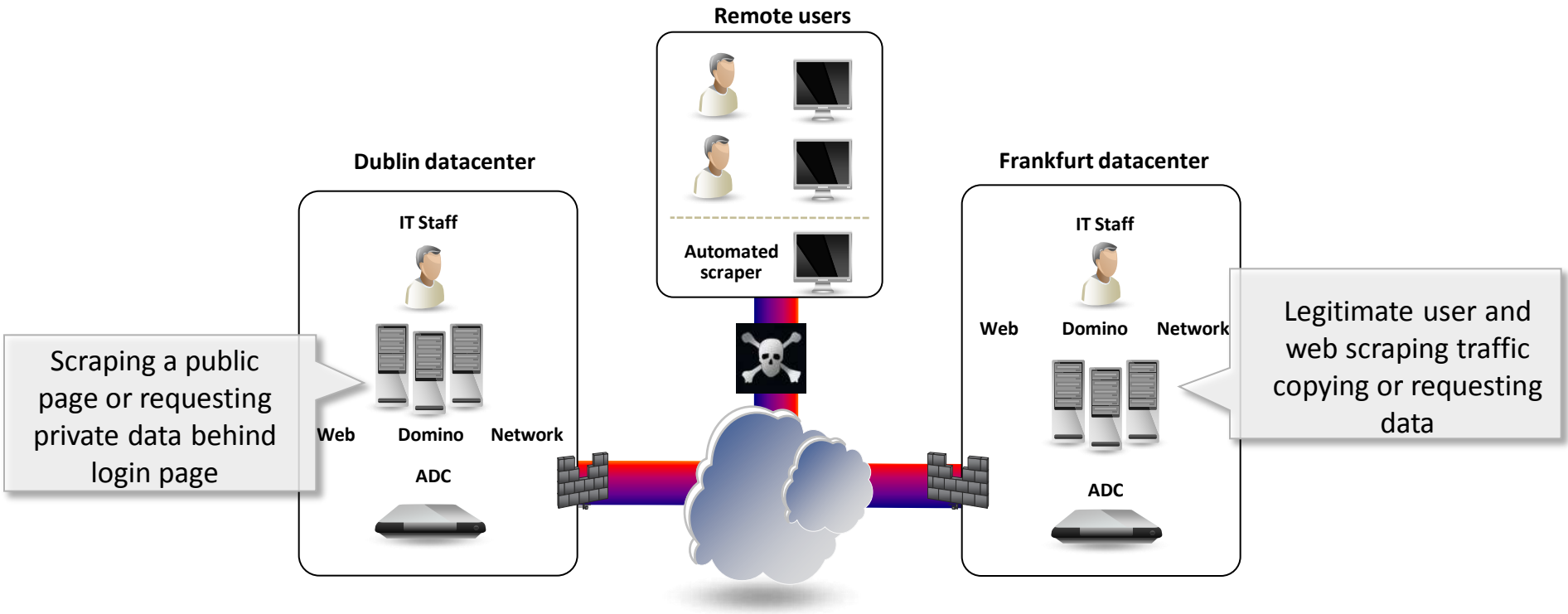
Airline Inventory Vulnerable to Web Scraping

- Ryanair – Forbids screen-scraping as commercial use. Major business problem
- Unister online travel site: Duesseldorf to London
  - Ryanair 93.25 Euros vs. Unister 111.86 Euros, **a 20% increase in price**
- easyJet warns Expedia: 'Hands off our flights'
  - Tried to block IP address but Expedia uses **millions** of IP addresses

- Alternatives: Litigation and legal letters
  - Ryanair sent cease and desist letters to 300 sites
  - Ryanair wins injunction against Vtours GmBH



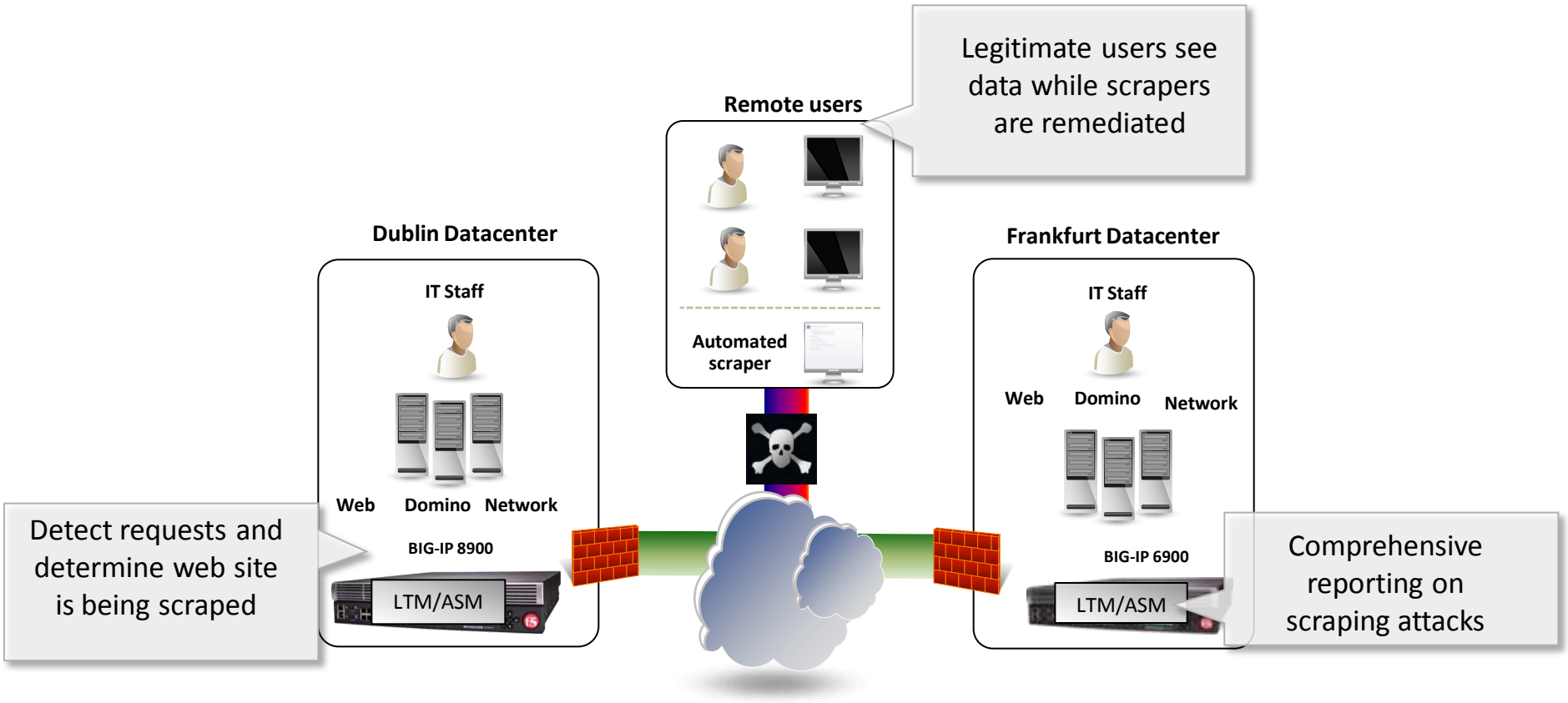
Automated scanner and BOT programs



Problem

- Entire web site is being scraped of valuable IP information
- Scrapers fail to provide company's terms and updates
- Sites copying content end up ranking above company's for keywords
- Need logging and reporting on Web scraping

Protection from Web Scraping

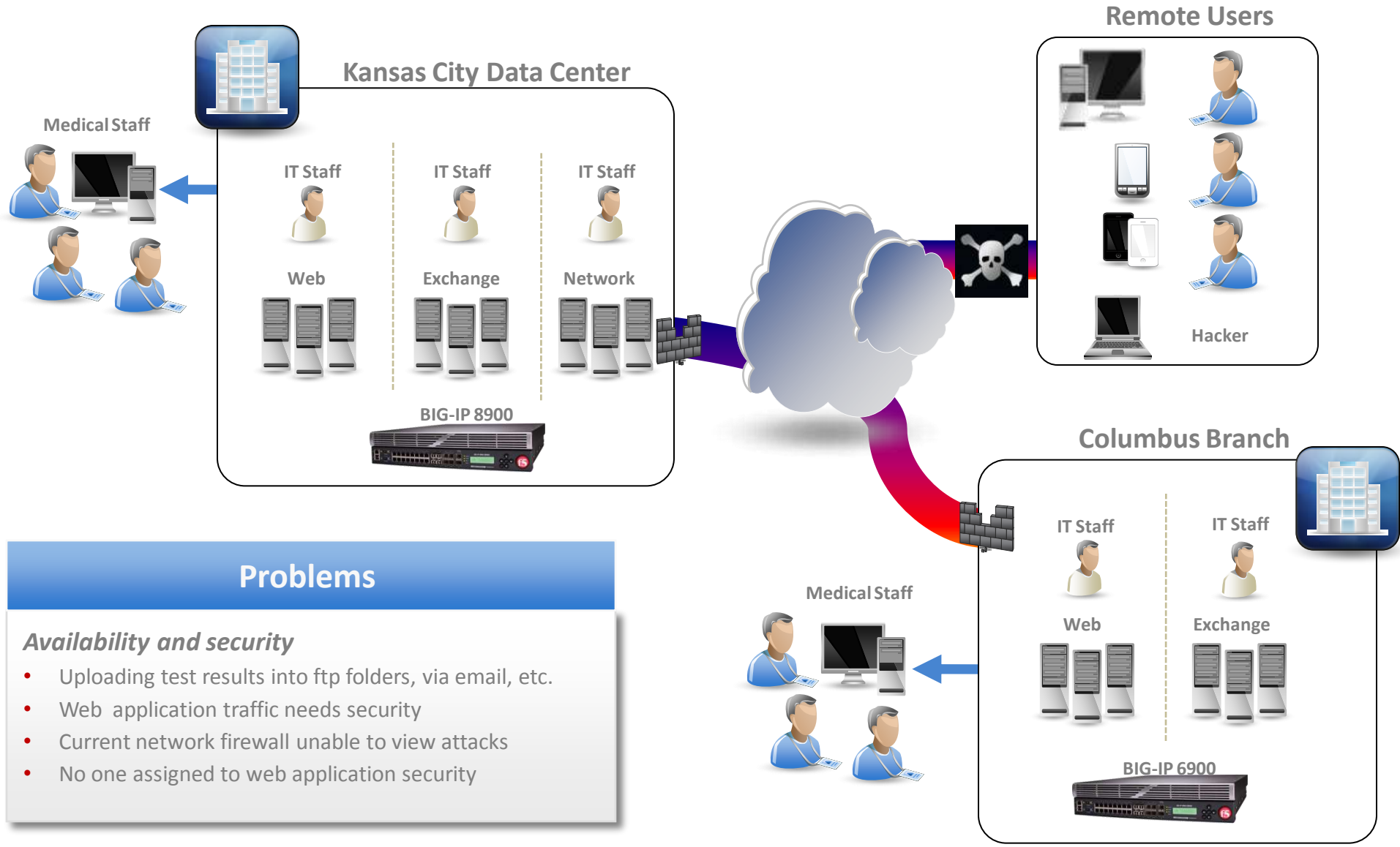


Solution

- Protects valuable intellectual property
- Prices are controlled and users see airline approved inventory
- Integrated scrape reporting for PCI compliance
- Avoid litigation drastically reducing legal costs

Healthcare Organization Example

Need application security with SharePoint



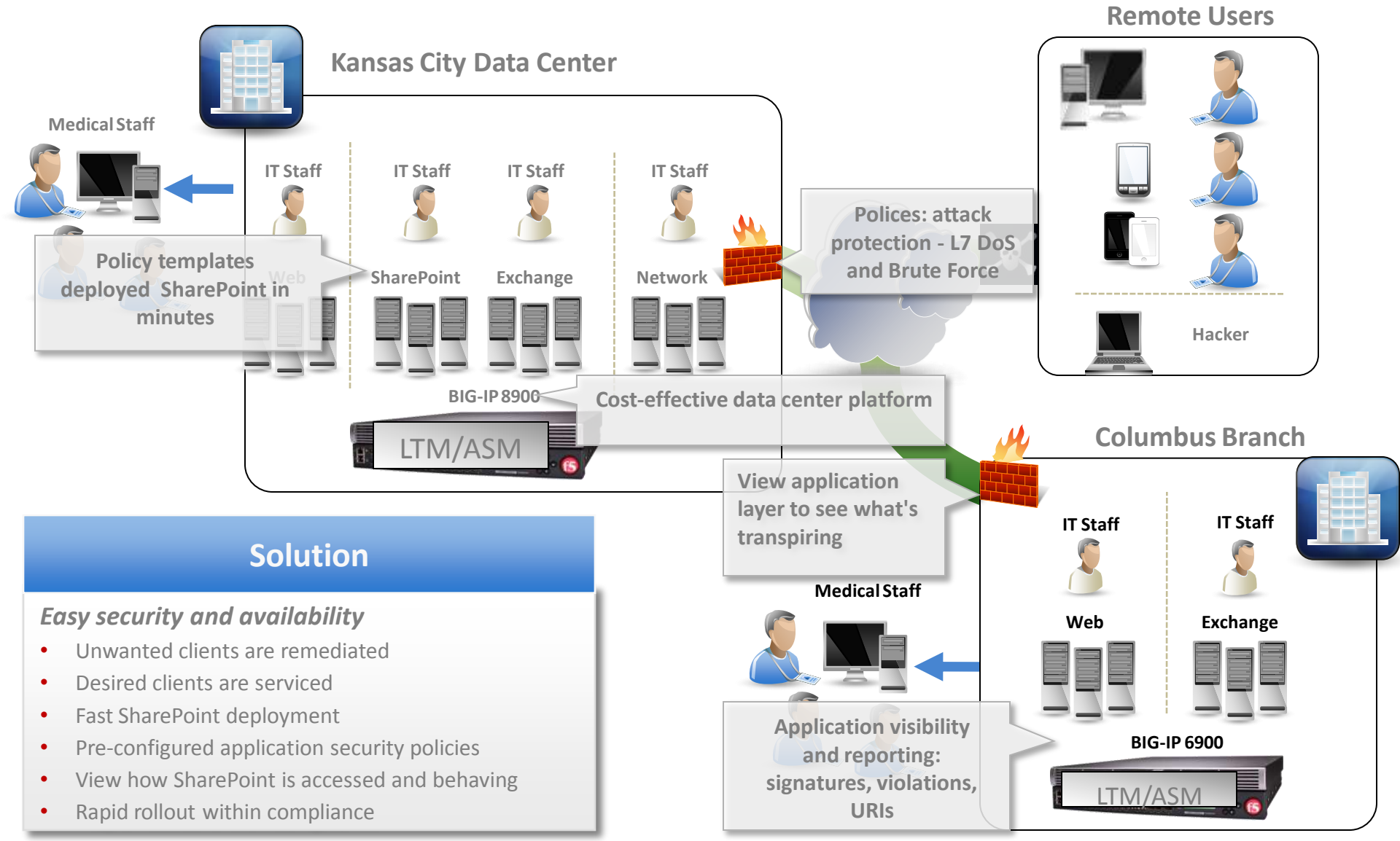
Problems

Availability and security

- Uploading test results into ftp folders, via email, etc.
- Web application traffic needs security
- Current network firewall unable to view attacks
- No one assigned to web application security

Healthcare Organization Example

Fast web application security implementation

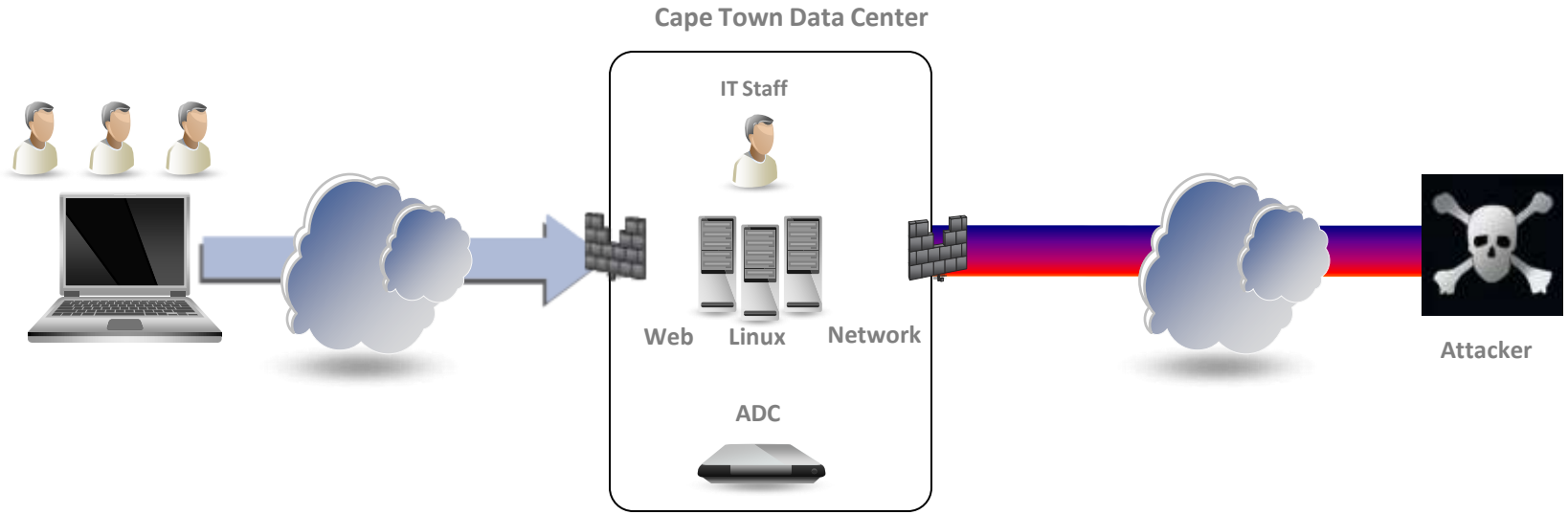


Solution

Easy security and availability

- Unwanted clients are remediated
- Desired clients are serviced
- Fast SharePoint deployment
- Pre-configured application security policies
- View how SharePoint is accessed and behaving
- Rapid rollout within compliance

EMEA Customer Website

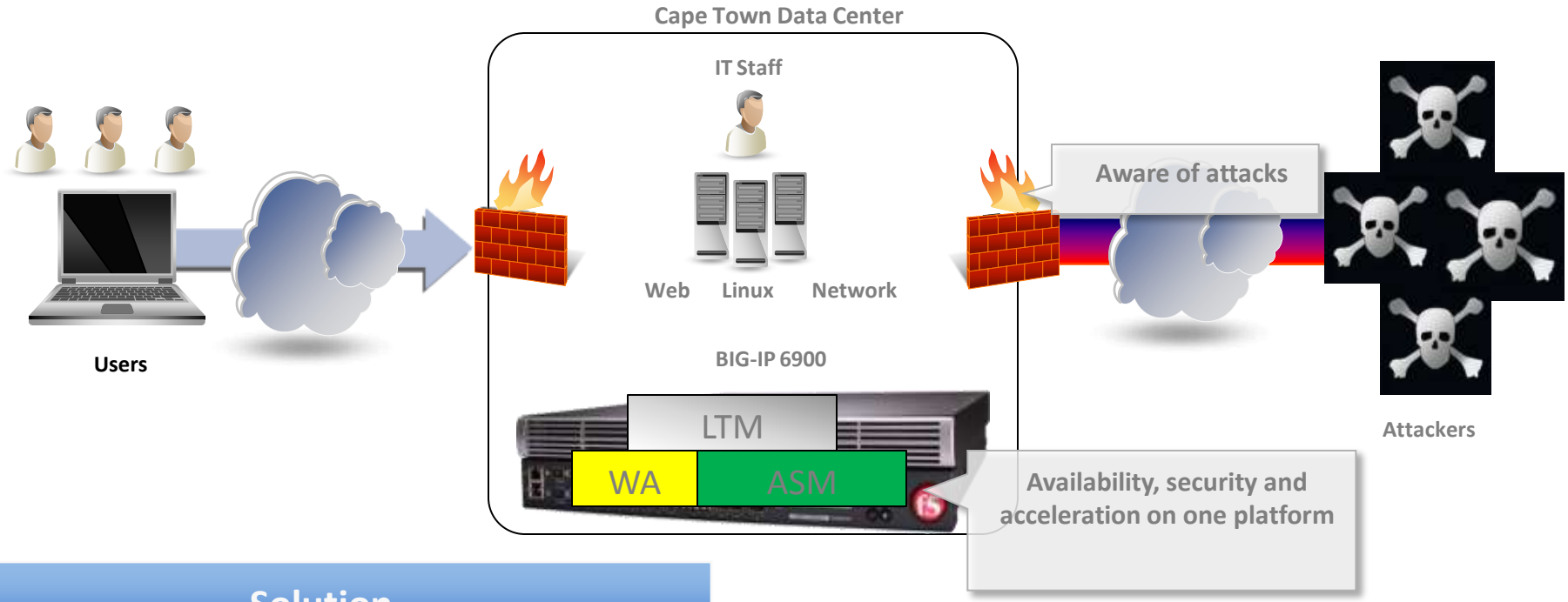


Problems

- Unaware of attacks nor ability to block them
- End user performance is declining
- Current network firewall unable to view attacks
- Separate solutions for acceleration and security were difficult to manage

EMEA Customer with WAF

"We didn't even know we were being attacked…"



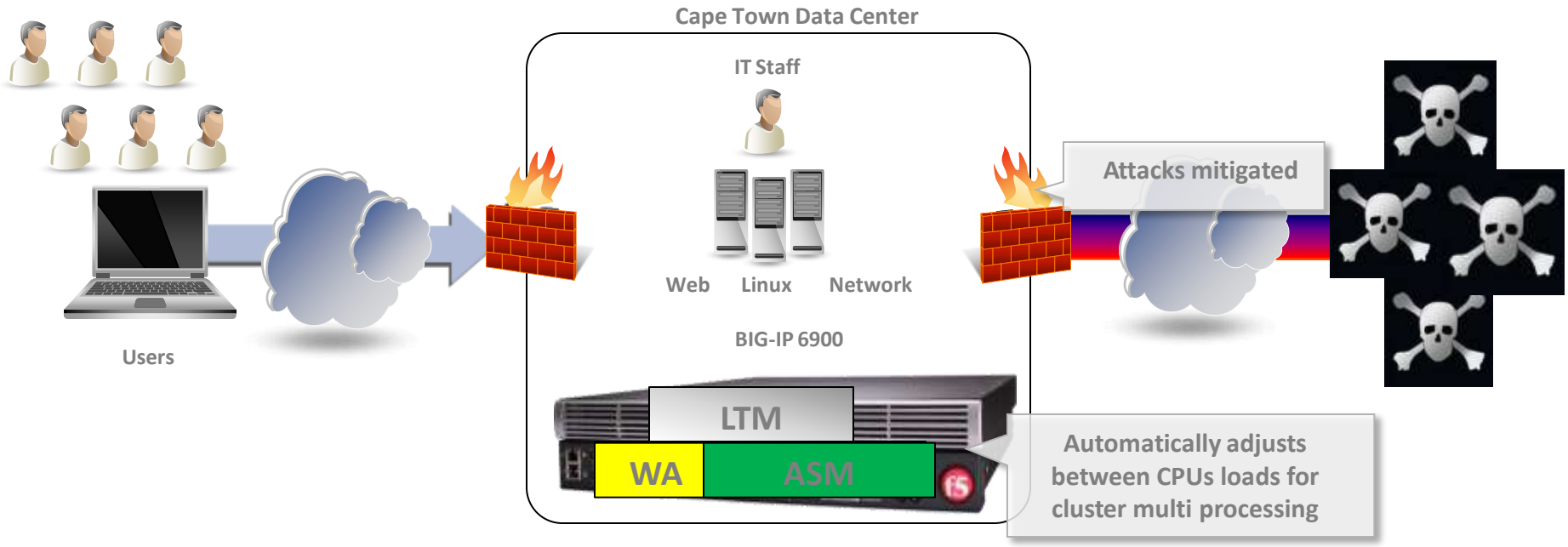
Solution

Unified application delivery

- 10x user performance increase
- 50% bandwidth reduction
- Attack and threat protection (SQL Injection, signatures)
- Visibility into attacks
- Provisioning resources to ASM during large attacks

EMEA Customer with WAF

Fast and secure

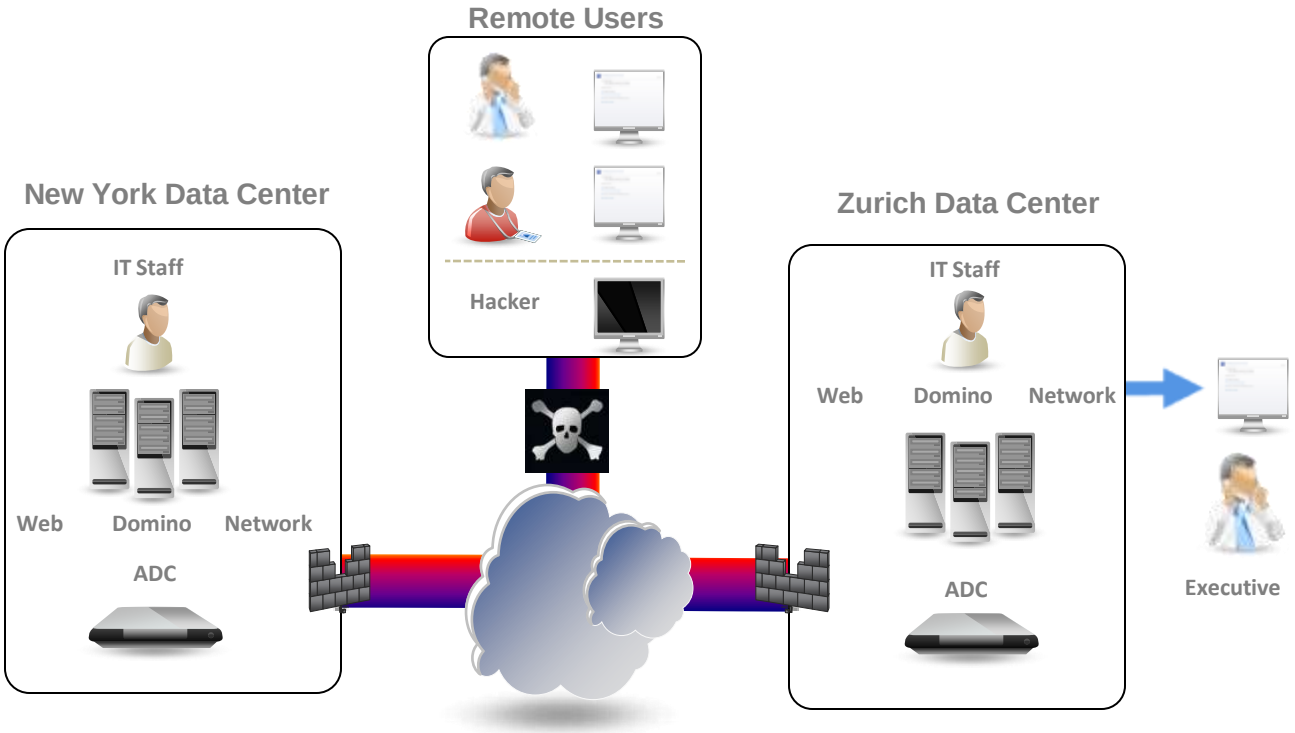


Solution

On Demand service provisioning

- Allocate resources to other application delivery services
- Attack and threat protection (SQL Injection, signatures)
- Burst and accelerate applications to meet user demands
- Dynamic Content Caching 80 - 90% of page loads
- ASM and WA pre-configured policies

Fortune 500 Financial
Web applications are vulnerable

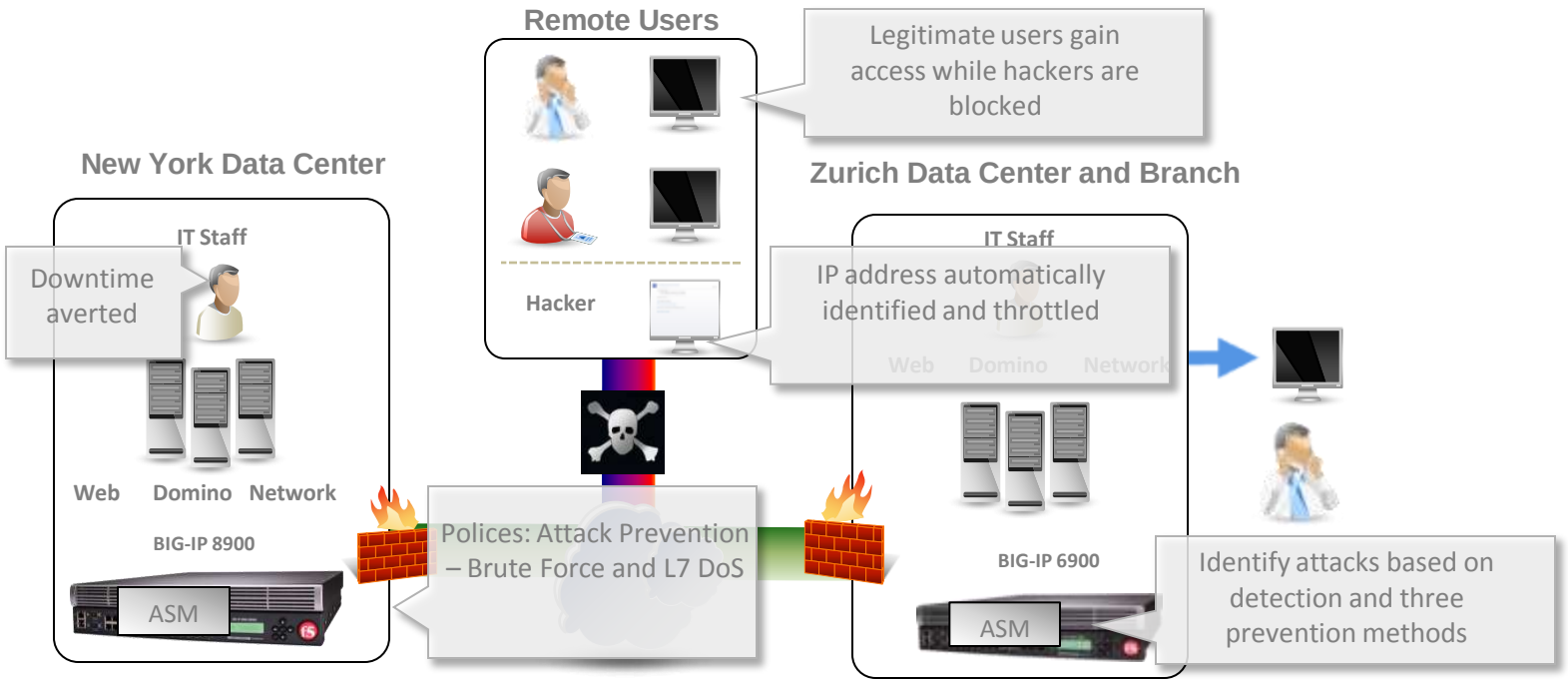


Problem

- Banking Web services are important but….
- Brute Force login attacks are rendering our web sites ineffective
- Inability to access information due to Layer 7 DoS attacks
- Slow response times from attacks overloading web servers
- Unable to view the attack source or slow the requests

Fortune 500 Financial

Application protection from attacks



Solution

- Unwanted clients are remediated and desired clients are serviced
- Improved application availability
- Focus on higher value productivity while automatic controls intervene
- Helps companies achieve security standards compliance

SECURITY 2011

19. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Radovan Gibala
F5 Networks
r.gibala@f5.com