Death of Security Appliances – Hype or Reality?

A Pragmatic Approach to Embracing Cloud Security

Keynote Guest Speaker
Jim Reavis
Co-founder and Executive Director
Logistics Help

• To send us questions during the sessions:
  Type the Question in the text box provided on the screen and click ‘Submit’. We will answer the questions submitted during the webcast.

  ▪ Any Technical Issues?
    Email:  webcast@zscaler.com

  Tip: Microsoft IE works better with Windows Media Player

Please complete the Feedback Form before you exit for a chance to win a $50 VISA GIFT CERTIFICATE.
Webcast Agenda

- **Death of Security Appliances – Hype or Reality?**
  
  *Jim Reavis, Co-founder and Executive Director of the Cloud Security Alliance (CSA)*

- **Simplifying Web Security Using Zscaler**
  
  *Manoj Apte, VP, Product Management, Zscaler*

- **Step-by-step Demo of Web 2.0 Exploits**
  
  *Michael Sutton, VP, Security Research, Zscaler*

- **Real-Life Customer Case Study**
  
  *Alfredo Pequeno, IT Sub Director, Banco Regional de Monterrey (BanRegio)*

- **Q&A Session**
Death of Security Appliances – Hype or Reality?

A Pragmatic Approach to Embracing Cloud Security

Jim Reavis, Executive Director

April, 2010
CSA Organization

• Global, not-for-profit organization
• Board of Directors
  • Jerry Archer, CISO Sallie Mae
  • Alan Boehme, EVP ING
  • Dave Cullinane, CISO eBay
  • Paul Kurtz, Good Harbor
  • Nils Puhlmann, Co-founder
  • Jim Reavis, Co-founder and Executive Dir

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”
40 Corporate Members, 10 Non-profit Affiliations
Defining Cloud

- On demand provisioning
- Elasticity
- Multi-tenancy
- Key types
  - Infrastructure as a Service (IaaS): basic O/S & storage
  - Platform as a Service (PaaS): IaaS + rapid dev
  - Software as a Service (SaaS): complete application
  - Public, Private, Community & Hybrid Cloud deployments
S-P-I Framework

You build security in

IaaS
Infrastructure as a Service

APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities

SaaS
Software as a Service

Presentation Modesty
Presentation Platform
APIs
Applications
Data
Metadata
Content

PaaS
Platform as a Service

Integration & Middleware
APIs
Core Connectivity & Delivery
Abstraction
Hardware
Facilities

www.cloudsecurityalliance.org
Defining Cloud Security

- Securing the Cloud: Securing IaaS and PaaS
- Cloud-Delivered Security or SaaS Security Services

Popular Cloud Security Services

Email Cloud Security

Web Cloud Security

www.cloudsecurityalliance.org
Drivers for Cloud Security

- Cloud adoption: enterprise applications and data hosted off-premises
  - Appliances do not secure it
- Ubiquitous mobility: many users & systems rarely in corporate offices
- Information perimeter NOT equal to physical perimeter
- Newer Web 2.0 threats
- Cloud is the only logical web security enforcement point

www.cloudsecurityalliance.org
New Threat Profile & Trends

• Web-delivered malware top threat vector
  • Web threats have transient characteristics
  • Botnet “platforms” mutate continuously
• High-tech criminals increasingly sophisticated
• Web 2.0
  • Social networks widely used by employees (Twitter, Facebook, etc.)
  • Creates inadvertent data leakage vector
  • Platform for malicious applets
• Insider threats on the rise (DLP, etc.)
• Need to leverage cloud trends to win
Leveraging Cloud Effect for Security

• Better threat detection
  • Wider and deeper view of traffic to spot threats
  • Real-time correlation of threats across the globe

• Cloud security always current
  • Keeps threat signatures updated
  • Appliances: User systems cannot keep pace with updates
  • Significant lapsed time: threat detection > signature release > deployment

• Trust Experts to keep security current
  • Customers often lack expertise to keep up with newer threats
Legacy URL Filtering is not Enough

• Traditional web security: Primitive egress inspection
  • Network port filtering, URL database
  • Ineffective in today’s Web 2.0 world
  • Cloud apps require policies (e.g., Google Docs – read vs. post)

• Advanced threat protection
  • AV is important at the web gateway, but not enough
  • Most threats are malware, malicious active content, botnets
  • Requires full inspection of web pages

• Data Leakage, a growing concern
  • A single click can send sensitive docs via Webmail, IM
  • Trojans can capture every key stroke – passwords, CC numbers
Legacy Security Appliances Model Broken

• Appliances are better than deploying software
• Suited for protecting physical perimeters, not information perimeters
• Lots of egress points = Lots of appliances
• Provisioning delays, Mgt & patching intensive
• Scaling limitations at high-end (performance) and at the low-end (price)
• Capacity planning: Hard to adjust increase/decrease
Comparing TCO of Appliances vs. SaaS

- No OpEx
  - No hardware or software to purchase
- No Deployment Cost
  - Eliminates significant cost to deploy appliances
- Little on-going administrative cost
  - Saves IT cycles needed to manage and update appliances
- Save Bandwidth
  - No cost to backhaul traffic to HQ
  - No latency due to backhauling
- Reduced cost of fixing infected PCs
  - Better security = fewer infections = Lower cost of fixing PCs
Why Cloud Web Security?

• Optimal threat coverage
  • Protect entire “information perimeter”
  • Protect against all threats: Data loss, AV, Web 2.0

• Superior security architecture
  • Reduce redundant threat updates and latency
  • Uniform protection across all locations

• Economic
  • “On-demand”, per seat pricing
  • Flexible cost center accounting

• Business enabler
  • Immediate service, no product provisioning delays
  • Secure new business initiatives immediately
Enterprises Embracing Cloud Security

• CISOs see cloud-delivered security as inevitable next generation model
• Various migration strategies
  • Location by location
  • Business unit specific
  • Full enterprise – one security service at a time
  • Complete
• Crucial to prepare for further enterprise cloud adoption
Benefits & Lessons Learned

• Reduced cost of ownership
  • Reduced capital outlays
  • No appliance maintenance
  • Fewer management consoles
• Greater visibility into IT assets and usage
• Leverage with business partners and customers
• Redeploying resources to solve business problems
  • Make them business security analysts
Summary

• Cloud computing is the future of IT
• Enterprise information perimeters difficult to track
• Legacy security appliance model broken
• Cloud is only the logical web security enforcement point
• Enterprises finding flexible deployments and surprising ROI with SaaS Web Security
Simplifying Web Security Using Zscaler

Manoj Apte
VP, Product Management
Zscaler: Cloud Security without Compromises

Singular Focus

Always secure: Policy-based web security from any device, anywhere.
Security simplified: No hardware, No software needed!

Benefits

- Mitigate business risk: Improve security
- Simplify IT administration: Consolidate point products
- Reduce cost: Superior functionality at half the price
Drivers for Cloud Delivered Web Security

IT Applications are moving to the Cloud. Appliance protecting the perimeter are not sufficient

- Everyone has a Laptop
  Office, Coffee-shop, Airports, In-flight.
- Work-At-Home Employees
- Branch offices
- Mobile Devices Blackberry, Iphone, Android …

Mobile and Distributed Work Force
Drivers for Cloud Delivered Web Security

IT Applications are moving to the Cloud. Appliance protecting the perimeter are not sufficient

- Everyone has a Laptop Office, Coffee-shop, Airports, In-flight.
- Work-At-Home Employees
- Branch offices
- Mobile Devices Blackberry, Iphone, Android ...  

- Complex Web2.0 Attacks: XSS, XSRF, APT, Clickjacking and more
- Browser Vulnerabilities without patches
- Data protection challenge with Webmail and Social Networks

Complex Threat Environment
Drivers for Cloud Delivered Web Security

IT Applications are moving to the Cloud. Appliance protecting the perimeter are not sufficient

- Everyone has a Laptop
  Office, Coffee-shop, Airports, In-flight.
- Work-At-Home
  Employees
- Branch offices
- Mobile Devices
  Blackberry, Iphone, Android ...

Mobile and Distributed Work Force

- Complex Web2.0
  Attacks: XSS, XSRF, APT, Clickjacking and more
- Browser Vulnerabilities
  without patches
- Data protection
  challenge with Webmail and Social Networks

Complex Threat Environment

- Cluttered DMZ to
  provide complete
  web protection
- Backhaul or buy a
  thousand boxes.
- Monitoring overhead
  Manage, Consolidate, Correlate

Cost

IT Applications are moving to the Cloud. Appliance protecting the perimeter are not sufficient
Largest Cloud Delivered Security Provider

Putting a Fence around the Internet…
Delivers Rapid Response Time & High Reliability
Current point products are expensive, inefficient and incomplete

- Acquisition & deployment Cost: X boxes
- On-going Management Cost: Multiple UI/policies, log files
Enable IT to focus on Strategic Security: Policy & Architecture
Providing Deep Inline Web Security

Knowledge of Destination
- URL Categorization

Knowledge of Payload
- Anti-Virus
- Anti-Spyware

Knowledge of Application
- Protocol Tunneling
- Unauthorized Applications

Knowledge of Content
- XSS
- Vuln ActiveX
- Botnets

Complexity

Security

Block Lists

Static Signatures

Protocol Analysis

Dynamic Content Inspection
Zscaler Web: Comprehensive, Integrated, Best-of-Breed

Eliminates the need to buy multiple point products; Reduces cost

Zscaler Global Network
Cloud Architecture Designed Ground Up

1. **Brain/Nervous system, Policy, Updates, Health of the Cloud**

2. **Onramps to Internet, Traffic processing, Policy execution**
   - Each Zen capable of scaling to 10Gbps

3. **When user moves from city A to city B, the policy follows him, her traffic is directed to the nearest ZEN**
   - Logs Compressed 50:1

4. **Logs from all locations go to NanoLog (real-time consolidated reporting)**
   - **15 million logs per second**

---

**Delivers Rapid Response Time (ultra-low latency) & High Reliability**
Customers around the world trust Zscaler

- Zscaler is truly Scalable

  Securing web traffic from more than **140 countries**

  Most traffic sent by a single Customer: **2 TB every day**!

  Biggest global reach for a single customer: **49 countries**

  Most number of branch offices covered: **>1000 offices**

- For every Microsoft Browser Vulnerability this year:

  Zscaler cloud protected its users within **1 hour**!
Step-by-step Demo of Web 2.0 Exploits

Michael Sutton
VP, Security Research
Apache.org hit by targeted XSS attack

April 13, 2010
Angela Moscaritolo

The open-source Apache Software Foundation recently suffered a cross-site scripting (XSS) attack against its infrastructure that resulted in users' passwords being compromised.

The targeted attack allowed hackers to break into the server hosting Apache.org's issue and request tracking software, Atlassian JIRA, and steal encrypted passwords, the Apache Infrastructure team revealed in a blog post Tuesday. Hackers carried out the attack on April 5 by sending an error report to Apache and including a TinyURL link containing an XSS exploit. Several Apache administrators clicked on the link, compromising their sessions.

The attack was crafted to steal the session cookie from the user logged-in to JIRA
- https://blogs.apache.org/infra/entry/apache_org_04_09_2010
What is XSS?

**Cause**
- Improper input validation
- User supplied data embedded in dynamically generated web page
- Attacker injects active script – typically JavaScript

**Risk**
- Authentication – steal access credentials (e.g. cookies)
- Privacy – screen scraping
- Obfuscation – Overwrite page content
- Non-repudiation – force unintended user actions

**Attack**
- Persistent
  - Injected active script stored on vulnerable site (e.g. forum, comments, reviews, etc.)
  - Popular sites targeted or spam used to direct traffic to injected content
- Reflected
  - JavaScript embedded in link clicked on by user
  - JavaScript typically embedded in link within spam email message

---

Copyright © 2009-2010 Zscaler CONFIDENTIAL
Reflected XSS

http://tinyurl.com/XXXXXXXXX

Vulnerable JIRA Web App

Malicious link posted

Attacker

Victim
Reflected XSS

1. Malicious link posted

2. Admin clicks on link – sends malicious JavaScript

```
<script>
</script>
```
Reflected XSS

1. Malicious link posted
2. Admin clicks on link – sends malicious JavaScript
3. Malicious JavaScript embedded in response

Attacker

Vulnerable JIRA Web App

Victim
Reflected XSS

1. Malicious link posted
2. Admin clicks on link – sends malicious JavaScript
3. Malicious JavaScript embedded in response
4. JavaScript executes – cookie stolen
Zscaler Protections - XSS

**Challenge**

- Limited solutions available for XSS
- Lack of visibility into attacks

**Protections**

- Pattern matching – identification of malicious JavaScript embedded in requests
- Cookie stealing – watermarked cookies identified/blocked in requests to 3rd party servers
Fake AV

Threat

- Top social engineering based attack
- Often combined with SEO, social network/blog spam
- Highly effective

Detection

- Limited detection due to continually changing nature of attacks
- Zscaler approach – full content inspection leveraging pattern matching, combined with offline data mining
Fake AV Attack

Google search results for "didi index indicator"

1. **didi index indicator (from metatstock) @ Forex Factory**
   - 6 posts - 3 authors - Last post: Nov 6, 2008
   - i need a indicator called "didi index" created for metatstock platform, ...
   - www.forexfactory.com › Forums › Programming Discussion - Cached - Similar

2. **DIDI Index - MQL4 forum**
   - 11 posts - 3 authors - Last post: Dec 9, 2008
   - There is an indicator called DIDI INDEX, which was developed by a trader called Odir Agular.
   - The indicator is very powerful, works very well ...
   - forum.mql4.com/17782 - Cached - Similar

3. **Metastock Indicators Index - investors trading strategies**
   - Didi Index. Displace Indicator Forward, displaced moving average, Dunn-Type 1. Dunn-Type 2. Fibonacci Trader - Dynamic Balance Point ...
   - www.brave.net.au/ms/list_indicators.php - Cached - Similar

4. **Wealth-Lab NET - Forum Topic: DIDI index - Code for Wealth Lab**
   - Please, I do use a great indicator combined with ADX called DIDI Index. You can find a screen pic at this link http://forum.mql4.com/c/forum/2008/12/tlwz3. ...
   - www.wealth-lab.com/community/forum/Posts.aspx?id... - Cached

Message from Didi:

Feb 24, 2010 ... didi index indicator (from metatstock) Programming Discussion. Priyaa didi... sapko janamdi ki bahot bahot ShubhakaamayeN .. meri hameShaa ...
- consultedem.com/seriously/didi.html - Cached
Fake AV Attack

LOL didi, i thought the same BUT if you take into consideration that there is a circus there, petting zoo and rides then i guess the entrance.

Priyaa didi.. aapko jannahin kii bahot bahot ShubhakaanaanyeN . meri hameshaa se duaa yahee rahiN hai kii aap ki har khwahishen poori hoN.

Please help us honor "Didi" in this small way. Let's let him know how very much he was appreciated and how terribly he will be missed by all.

I found "Didi's Magic lake" on the site and thought it might save a bit of time and .. I'm pretty sure you get at least between 1-4x more with Didi's than ..

I corrected, Didi will be on soon! NT 03/23/10 06:33 PM AddThis Social Bookmark Button. Edit, Reply, Quote. I am not related or jealous.

Met Didi a few years ago he was in Jalons on Smithdown Rd. having a scrum with Babel and he walked in the bathroom as I was walking out just

mama mami ke saath hi rohte the aur meri majhi didi Babli jo ki . ko mub lagakar choos rahe the aur iski samay mami didi ki patticoat . Contestant Didi Benami recently impressed judges with her rendition of "Terrified"

during Hollywood Week -- but is there more to the ..

Dr. Didi Harries Chilliwack, BC Gender: F Specialty: Pediatrician Webpage: Hospital Answers Email: Online Appt. Scheduling: N.

Didi is going to the Powry competition > Comments welcomes > Freindly Sylvan I was looking for your picture in the list of entries and was ..


AND you cannot get on DIDI Daves forum now for the same reason I mentioned, if you have to register one is SOL so everyone that uses ..

This photo from the TrekEarth travel gallery is titled 'Pawnee Buttes - for Didi Photo'.

http://seattletimes.nwsource.com/ABPub/2006/05/13/2002992853.jpg
Fake AV Attack
Zscaler Protections – Fake AV

**Challenge**

- Strong social engineering tactics fool many victims
- Sites are moving targets – quickly emerging and disappearing

**Protections**

- Inline anti-virus
- Pattern matching within web content to identify common elements of fake AV pages
Real-life customer case study

Jose Alfredo Pequeno Contreras

IT Sub Director

Webcast with the Cloud Security Alliance (CSA)
Founded in 1994, Banco Regional de Monterrey (BanRegio) is a leading financial services institution in Monterrey, Mexico

- 100 branch locations
- 2000 users
- Expertise in retail, small and medium business, factoring, leasing, consumer finance and private banking services
- Rapid business growth leading to proliferation of branches
## Challenges and Requirements

<table>
<thead>
<tr>
<th>CURRENT SOLUTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Central proxy-based URL solution</td>
</tr>
<tr>
<td>No network-based anti-virus solution</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHALLENGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>High bandwidth costs due to traffic backhauling from 100 locations to central site</td>
</tr>
<tr>
<td>High operational costs resulting from maintaining large pre-approved URL list</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection against new advanced threats</td>
</tr>
<tr>
<td>Reduced management complexity</td>
</tr>
<tr>
<td>Reduced backhaul infrastructure cost</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OPTIONS EVALUATED</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appliance-based solutions</td>
</tr>
<tr>
<td>Did not want to backhaul traffic by installing point products</td>
</tr>
<tr>
<td>High setup and administration cost to install appliance per location</td>
</tr>
<tr>
<td><strong>Zscaler cloud delivered Web Security Solution was selected</strong></td>
</tr>
<tr>
<td>Only SaaS provider with local data centers in Mexico</td>
</tr>
<tr>
<td>Easy to manage due to centralized administration</td>
</tr>
</tbody>
</table>
Deployment Experience

- Easy, quick, smooth deployment at 50 branch locations
- Significant bandwidth savings
- Instant malware detection
Zscaler Benefits for BanRegio

NEXT STEPS: Immediately redirect traffic to Zscaler cloud from remaining 50 branches

Benefits to Organization
- Bandwidth cost savings
- Better utilization of IT resources
- Protection against more advanced threats

Benefits to Administrator
- Easy central policy management of users across 50 locations
- Savings from URL list maintenance
- Better visibility of organizational security with real-time reporting

Benefits to User
- More flexible access to websites
- Lower latency – no traffic backhauling
Summary: Superior Security at Half the Price

- **Consolidate point products**
  - Integrated
  - Comprehensive
  - On-demand

- **Reduce cost, low TCO**
  - No CapEx
  - Rapid ROI

- **Simplify Security**
  - Easy to deploy & manage
  - Enable IT to focus on strategic issues

- **Game Changing cloud service**
  - Jet engine vs. propeller engine
  - Near-zero latency
  - Reliability

A Trusted & Reliable Partner
With commitment to quality & customer success
Next Steps

- Online Personalized Demo
- Free Service Evaluation

Contact Zscaler at:

**US, Canada and Latin America**
1-866-902-7811 or +1-408-533-0288
info@zscaler.com

**UK and Ireland**
+44 (0) 845 009 9531
uk-info@zscaler.com

**Southern Europe & ME**
+33 1 45 61 32 72
seur-info@zscaler.com

**Central Europe**
+49 89 954499820
ceur-info@zscaler.com

**Eastern Europe**
+7 495 287 13 61
eeur-info@zscaler.com

**India**
India-info@zscaler.com
+91 984 552 6361

**South East Asia**
sea@zscaler.com
+65 979 65 851

**Australia**
pacific-info@zscaler.com
+613 985 95 266

Please complete the **Feedback Form** before you exit for a chance to win a **$50 VISA GIFT CERTIFICATE.**
Q&A Session

Submit your Questions using the on-screen text box.

- Jim Reavis – Co-founder and Exec Dir. of CSA
- Manoj Apte – VP Product Management, Zscaler
- Michael Sutton – VP Security Research, Zscaler

Please complete the Feedback Form before you exit for a chance to win a $50 VISA GIFT CERTIFICATE.