The Essential Guide to Cloud Security

With Practical Tips for CISOs and CIOs to Reduce Costs and Improve Security

Jay Chaudhry
CEO & Founder
Zscaler, Inc.
Contents

Introduction ................................................................................................................................................................... 3
1. The Changing Internet: Cloud Computing, Web 2.0, Mobility and New Threats ................................................... 4
2. Legacy Security Struggles...................................................................................................................................... 10
3. Coming to an Enterprise Near You: Cloud Security .............................................................................................. 14
4. Architecture of a Cloud Security Service............................................................................................................... 18
5. Security Threat Protection ...................................................................................................................................... 23
6. Web 2.0 Managed Access Policies ........................................................................................................................ 27
7. Data Loss Prevention via the Cloud ....................................................................................................................... 29
8. Reporting and Analysis .......................................................................................................................................... 33
9. Cloud Security Provider Assurance & Trust .......................................................................................................... 35
10. Incident Response & Forensics ............................................................................................................................ 37
11. Extending Cloud Security to Partners .................................................................................................................. 40
12. The Business Case for Cloud Security ................................................................................................................. 42
13. Recommendations for Transitioning to Cloud Security ....................................................................................... 45
References ................................................................................................................................................................... 48
Introduction

Like brakes on a car, information security is there to make the business go faster.

*Rhonda MacLean, Former Global CISO at Barclays Global Retail*

Welcome to *The Essential Guide to Cloud Security*. This guide was developed as the result of collaboration between several information security experts in order to provide CISOs with an understanding of how traditional security architectures are being disrupted by key trends such as Cloud Computing, Web 2.0 and Mobility. The guide provides a wealth of data points, definitions and statistics to address the key challenges that CISOs are facing as a result of the adoption of these trends.

There are many aspects to Cloud Computing that are being discussed widely in the media, at conferences and in the blogosphere. The main focus of this guide is to address the necessity of utilizing Cloud Computing as a component of a comprehensive security strategy. It explains how Cloud Security Architecture can mitigate new threats and enable organizations to better manage their business in a secure way.

When we say cloud security, we are not talking about securing the cloud computing platform such as Amazon or Google. We are talking about cloud-delivered security whereby internet bound traffic is filtered by a service in the cloud to make sure that the users are protected from the threats of internet. Other terms used for this are Security-as-a-Service (SaaS), On-Demand Security or Utility Service.

Today’s global economy demands maximum flexibility and agility on the part of businesses. New business opportunities, fast moving security threats and on-demand computing mandate the need for an on-demand approach to information security. We hope that this guide will provide you with insight and inspiration as to how you can incorporate Cloud Computing into your security strategy and enable a “future ready” organization.
The Changing Internet: Cloud Computing, Web 2.0, Mobility and New Threats

The New World of Cloud Computing
“The rise of the cloud is more than just another platform shift that gets geeks excited. It will undoubtedly transform the IT industry, but it will also profoundly change the way people work and companies operate.”


As enterprises have been leveraging the Internet for a decade and a half, its the organization’s information security function has played an evolving role to keep pace with, and protect the business. Internet-driven changes in business models and information technology do not take a predictable, linear path. Today’s Chief Information Security Officer (CISO) stands at the precipice of a generational shift in computing, catalyzed by the interplay between several significant trends, the most notable being Cloud Computing, Web 2.0 and Mobility. These trends both heavily influence and are heavily influenced by society’s drive towards globalization and a highly interdependent world economy. These trends in turn drive a computing ubiquity with far-reaching implications.

Cloud Computing
Moore’s Law has led to continued commoditization of computing power and bandwidth. At the same time, Operating System Virtualization and Service Oriented Architecture (SOA) technologies enable “just-in-time” data center growth and the logical separation of business applications from fixed hardware. This is fueling an explosion of on-demand computing capabilities typically referred to as Cloud Computing, of which Software-as-a-Service (SaaS) is the most well known offering.

Analyst forecasts for this market continue to be revised upward, with IDC predicting $42B in cloud computing spending by 2012. The practice of paying only for the amount of computing needed is not only changing the economics of information technology, but is also accelerating business. An enterprise can leverage Cloud Computing to move very quickly to launch new products, locations and business units without the traditional time to procure and provision information technology and enterprise applications. One must expect that any economic downturn will only accelerate the pressure to embrace Cloud Computing.

Consider Merrill Lynch’s analysis of Cloud Computing:
Cloud computing is the delivery of applications over the Internet. Cloud computing refers to the idea of delivering personal (e.g., email, word processing, presentations) and business productivity applications (e.g., sales force automation, customer service, accounting) from centralized servers. These servers share resources like storage,
processing and bandwidth more efficiently by a cost factor of at least 5-10X. Cloud computing is a relatively new method of software delivery that has been evolving for a number of years. Services are delivered over the Internet from shared servers, rather than from software loaded onto a personal computer or local server. The shared servers are likely located in a data center run by Google, Microsoft, Amazon or some other third party, and it is these data centers that are considered to be ‘the Cloud.’

The transition to the Cloud is analogous to the rise of utilities. Nicholas Carr has written extensively about the transformation currently taking place in the IT industry (see 'IT Doesn't Matter', HBR, June 2003, and 'The End of Corporate Computing', MIT Sloan Management Review, Spring 2005). He draws the analogy of how electricity went from being produced by in-house and private generating plants in the 1880's to large centralized utilities in the early 1900's. In his view, IT, like electricity, is a general-purpose technology that has the potential for considerable economies of scale if its supply is consolidated. Mr. Carr believes a fragmented supply is inherently wasteful. Centralized provisioning can achieve higher capacity utilization, and result in much cheaper supply.*

The characteristics of Cloud Computing are significantly different from those of Traditional IT infrastructures.

<table>
<thead>
<tr>
<th>Traditional IT</th>
<th>Cloud Computing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capital intensive</td>
<td>Operating expenses, pay as you go</td>
</tr>
<tr>
<td>Central planning</td>
<td>Business unit &amp; consumer procurement</td>
</tr>
<tr>
<td>Single purpose systems (appliances)</td>
<td>Virtualization</td>
</tr>
<tr>
<td>Capacity planning</td>
<td>On demand provisioning</td>
</tr>
<tr>
<td>Own infrastructure</td>
<td>Multi-tenant</td>
</tr>
<tr>
<td>Private VPNs</td>
<td>Granular user access</td>
</tr>
<tr>
<td>Operational control</td>
<td>Management Accountability</td>
</tr>
</tbody>
</table>

Attempts to taxonomize cloud computing are abound as experts seek to provide granular definitions of the variety of services that can be delivered via an on-demand model. One example of a framework for Cloud Computing by David Linthicum lists the following:

- Storage-as-a-Service
- Database-as-a-Service
- Information-as-a-Service
- Process-as-a-Service
- Application-as-a-Service
- Platform-as-a-Service
- Integration-as-a-Service
- Security-as-a-Service
- Management/Governance-as-a-Service
- Testing-as-a-Service

--

While these taxonomies are useful to understand the capabilities of Cloud Computing today, it is unlikely that these definitions will endure in the long run. The cloud is changing everything, and innovation is bringing to market new classes of services that defy easy categorization in our current mindset about information technology and the nature of business organizations.

**Web 2.0**

Web 2.0 is both a combination of technology, such as JavaScript, Flash, Really Simple Syndication (RSS), Service-Oriented Architecture (SOA), and an attitude of personal empowerment in using the Internet. These technologies are combined to create a wide variety of sophisticated applications, such as streaming multimedia, “mashups” and social networking. The end result is that users expect a rich, interactive internet experience from their web browser, and also expect to have no limitations in their access to information. In many cases, the Web 2.0 social networking sites are a primary vehicle for posting confidential enterprise information, much to the dismay of CISOs.

The first generation of web surfing very much resembled mainframe terminals, in which static pages consisting primarily of text and graphics were delivered to the user. CISOs previously had the ability to mandate secure browser configurations by, for example, disabling JavaScript or the Flash player within the browser. Today, such actions essentially “break” the functionality of the Internet, and enterprises are reduced to maintaining up-to-date versions of browser and plug-in software in order to reduce the risk of security vulnerabilities.

---

**What is Web 2.0?**

Web 2.0 is the business revolution in the computer industry caused by the move to the Internet as platform, and an attempt to understand the rules for success on that new platform.

*Tim O’Reilly, CEO, O'Reilly Media*

---

The impact of Web 2.0 is profound. In order to stay competitive, all popular web sites must use interactive Web 2.0 technology to attract business. The web browser, including Web 2.0-specific technologies, has thus become the default development platform for business and consumer applications.
Mobility

Mobility, achieved both through powerful mobile computing devices and pervasive high speed bandwidth, has unleashed workers from being tied to fixed locations. Users may consist of employees, contractors, consultants or business partners, united by their need for access to your enterprise’s information.

*Mobility Changes (Almost) Everything*

As we equip more of the workforce with smart phones, they become less tethered to predefined locales and, thus, create an expanding boundary for us to address. The "little laptops" now attached to belt loops or in pockets and purses are rapidly gaining both increased processing power and, more important, new access pathways through third generation (3G) and fourth generation (4G), as well as WiFi and WiMAX, networks. Compounding the challenge is the parallel need to accommodate an ever-growing and frequently changing pool of temporary, contract and outsourced providers for many essential business services. So who is an "outsider" and who is the "insider" under these various arrangements? How would we define the boundary or perimeter of a network under this new paradigm?

*William Boni, VP IT Security Motorola, 2008*

Mobility has blurred the line between business and personal usage for these users. There is an equally significant blurring of the lines between the traditional corporate PC or laptop and the current generation of smart phones. Smart phones today have increasingly sophisticated corporate applications and fully implemented web browsers, which are often used to access sensitive business data. According to Morgan Stanley, a key tipping point in the growth of mobility will be reached in 2009. High speed data access with 3G or faster technologies will be employed by an estimated 21% of the 3.9B global subscribers, up significantly from 10% of the 3.2B global subscribers in 2007. This represents a critical mass of mobile devices with high speed capabilities, which creates a snowball effect such that businesses must make their services accessible to mobile devices and independent software vendors (ISVs) view this as a significant opportunity for application development.

Thinking of users and endpoint devices in cloud terms means the following:

- Many organizational users are not traditional employees
- Users have no barriers to procuring their own high functioning computing devices which they will attempt to use for business applications
- IT will not be guaranteed to have permission to maintain security control software on all endpoint devices and will need to instrument indirect endpoint controls
- IT cannot anticipate the IP address spaces their network-based controls must be applied towards

We can no longer make rigid assumptions about where users are located and which computing devices they choose to access the Internet, nor can we impede their demand for a rich internet experience.

Evolving Threat Profile

It should come as no surprise that cybercriminals are leveraging the latest technology trends, such as cloud computing, Web 2.0 and mobility, and turning hacking into big business. According to the Gartner group, by the end of 2007, 75% of enterprises will be infected with undetected, financially motivated, targeted malware that evaded their traditional perimeter and host defenses. Dave Cullinane, the CISO of eBay, puts it this way, “I used to say it’s not ‘The Sopranos,’ but today’s successful cybercriminals are primarily part of organized crime groups, and are extremely sophisticated in their business practices, social engineering techniques, as well as in the technology they employ.”
Security threats have evolved from desktop-based viruses to email-based worms, and now are largely becoming browser-based threats. Clearly the Web is now the primary attack vector for cyber crime. Malicious actors have embraced Web 2.0, and in order to defeat an enterprise, they only need to compromise a single user surfing the Internet within that enterprise. **Inbound security is irrelevant if outbound security is not robust.**

<table>
<thead>
<tr>
<th>Old threats</th>
<th>New threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking for fun</td>
<td>Hacking for profit, nation-state information warfare</td>
</tr>
<tr>
<td>Viruses</td>
<td>Distributed Botnets</td>
</tr>
<tr>
<td>Phishing</td>
<td>Spear Phishing, Whaling</td>
</tr>
<tr>
<td>Lost productivity</td>
<td>Data exfiltration, Data Loss</td>
</tr>
<tr>
<td>Email threat vector</td>
<td>Web 2.0 threat vector</td>
</tr>
</tbody>
</table>

Consider “Botnets,” for example. There has been much media attention to botnets lately—but what exactly are botnets, and why do they pose a threat? Botnets are specialized groups of installed software applications (called “bots,” short for “robots”) that can act in coordinated fashion with each other and usually at the beck-and-call of a controlling person (often dubbed the “master”). Current media use of the term botnets often assumes malicious intent on behalf of the bots or their creator(s).

Botnets first became very popular on IRC (Internet Relay Chat) channel over a decade ago. Over time, various intruders realized that they could effectively utilize botnets to perform “mass mischief,” particularly spamming and flooding attacks.

Today botnets are much more sophisticated, and are much larger. The Storm botnet was sensationalized throughout 2007. The size estimates of the Storm botnet vary widely, starting at 160,000 bots to projections surpassing many millions. But regardless of the actual size, everyone seems to agree that the Storm botnet is both large and poses a notable risk.

**The Hybrid Enterprise**

The convergence between these major trends has created a situation we call **“The Hybrid Enterprise.”** The Hybrid Enterprise is characterized by enterprise data and applications existing both within the organization’s perimeter as well as at popular internet sites and multi-tenant cloud computing service providers. It is also characterized by a heterogeneous user base, a “cloud of users” that comprises employees and a variety of consultants, contractors and other partners, which will have a wide variety of endpoint computing devices. All of these authorized users are accessing enterprise data from locations both inside and outside the enterprise. The critical digital assets of an organization can no longer be assumed to reside within the organizational boundaries and associated network perimeters. The computing devices accessing these digital assets will be under varying degrees of IT control – in some cases that will mean no control at all.

The data, user and device management problems are compounded by the increasingly complex and accelerated information security threats we now face. Simple, monolithic email-borne viruses are increasingly being replaced by sophisticated command and control malware mutating by the minute, infecting users through Web 2.0 applications. CISOs are in a no-win situation of choosing to either disrupt the user experience or letting the user become infected with new breeds of web-hosted malware.
A New Threat Response Needed

Cloud Computing, Web 2.0 and Mobility are creating another internet revolution, whose impact is reshaping businesses on a global basis. The rapid decoupling of data from organizational boundaries, the acceleration of business decision making and the sophistication of new security threats are creating a mandate for innovation on the part of the CISO. These trends are challenging long held information assurance strategies and causing CISOs and their key architects to re-think security in very fundamental ways.

Chapter Takeaways

- Cloud Computing, Web 2.0 and Mobility are high growth trends changing computing, business and society.
- The Cloud and Mobility have decoupled an organization’s digital assets from its traditional boundaries and controls.
- Web 2.0 has become the pervasive application delivery platform and primary channel for security threats.
- CISOs must re-think architecture and strategy in response to these trends.
## Legacy Security Struggles

Information security, by its very nature, requires ever evolving defenses. Best practices dictate a layered approach to information security, so that no single layer’s compromise will deal a fatal blow to the business. When dealing with a cunning criminal adversary and high rates of disruptive technology change, the threat vectors continually change. This strains traditional layers of defense, increasing overall risk for the enterprise. The following table shows key weaknesses typically observed in today’s organizations:

<table>
<thead>
<tr>
<th>Traditional Defenses</th>
<th>How New Trends are Breaking This</th>
<th>Impact on the Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus/IDS signature updates</td>
<td>High rate of new and mutating malware</td>
<td>Signature-based security defenses are perpetually outdated, increasing risk of infection</td>
</tr>
<tr>
<td>Fixed perimeter security controls</td>
<td>Business demands and mobility create an enterprise “information perimeter” that differs from a network perimeter</td>
<td>Perimeter security cannot protect sensitive data as it moves to new locations</td>
</tr>
<tr>
<td>Network layer security</td>
<td>Diverse applications all use single web protocol</td>
<td>Traditional Network security can no longer distinguish between and protect enterprise applications or enforce user access policies</td>
</tr>
<tr>
<td>Inbound security</td>
<td>Simpler for criminals to lure users to malicious websites rather than penetrating inbound defenses</td>
<td>Users infect their own enterprise by virtue of their web surfing habits, criminals have botnets that include virtually every enterprise connected to the Internet</td>
</tr>
<tr>
<td>Endpoint control</td>
<td>Network access by consultants and contractors, smart phone adoption, business unit PC procurement</td>
<td>IT no longer manages all endpoint devices on its network or owned by its enterprise, cannot enforce controls, establish standards, maintain desktop security software suite</td>
</tr>
<tr>
<td>Operational security management</td>
<td>More time required to manage above defenses via patching, signature updates, rule changes</td>
<td>Security department must devote more resources to operational security, less time solving business problems</td>
</tr>
</tbody>
</table>

There are basic limitations inherent in using signature-based technology and keeping its anti-threat content up-to-date. The graphic below depicts a statistical capture and represents a typical 24 hour reading of the performance of antivirus engines in providing comprehensive detection of new malware threats. This demonstrates the failure of AV signatures to keep pace with new malware.
It is important to note that not only is traditional antivirus having an increasingly difficult time in detecting infections, but that the infections themselves are becoming much more severe. The prevalence of rootkits and other malware which do not appear in a system process list cannot be removed by antivirus. More and more organizations are reporting that the only effective way to eradicate viruses in a system is through a complete and costly system rebuild plus data restore. Clearly, we must block viruses and malware before they reach our enterprise computing assets.

Security Appliances: Designed for Yesterday’s Problems

In order to tackle these newer challenges, enterprises have been deploying security point products or appliances. Many of the problems with traditional security defenses can be revealed when examining our current dependency upon security appliances as a core part of our architecture:

- **Legacy enterprise view.** A security appliance is tied to legacy location concepts: dictating limitations to the business rather than enabling it. It forces business activities to be tied to locations or for traffic to be redirected to monitoring network segments in order to implement security controls. This creates performance, point-of-failure and security vulnerability issues. For example, an organization with a central URL filtering appliance forces poor architectural decisions upon other locations and mobile users. A remote user may be required to access the Internet via slow VPN connections or be denied corporate security protection.

- **Single purpose.** Appliances tend to be built for one security function only, creating an explosion of new appliances in the data center or in an organization’s DMZ (De-Militarized Zone) to keep up with each new threat, all of which must be individually integrated with the corporate directory.

- **Cost of ownership.** Appliances require significant costs for acquisition, installation, regular patching, log file management, access control, and integration among several other costs.

- **Trail the threats.** IT shops cannot keep pace with the demand to update appliance signature files resulting in false sense of security.

- **Appliances are not “on-demand,” and force “over-architecting” the solution.** An appliance may be designed for 100, 500, 5000 users, etc. If you have exactly 2000 users, you either must spend more money to purchase excess capacity or acquire an insufficient solution that hinders business activity. You also have hardware shipping and provisioning delays.

- **Single organization.** Appliances are designed for a single organization, not for the notion of multi-tenant configurations, limiting their usefulness with supply chains and business partners.

As the following figure shows, the proliferation of single-purpose security appliances creates several management problems, while only being able to protect a stationary constituency and leaving several protection gaps in the enterprise.
Traditional Appliances: Designed for Yesterday’s Problems

Current point products are expensive, inefficient and incomplete.

The security appliance has had a useful life in improving the TCO of security solutions, however, its usefulness is declining for the same reason that cloud computing itself is ascending: the business demands for security on demand and from anywhere.

Conficker: A Case Study in Legacy Security Defense Failures

The worldwide Conficker Worm outbreak provides a case study in security management and why our current defense strategies fail us. It has been a while since we've seen a fast spreading worm affect a significant volume of victims. In January 2009, however, a new variant of Conficker (aka Downadup) reportedly infected millions of Windows machines. Why was Conficker suddenly so successful? Not surprisingly, the answer relates to weaknesses in enterprise defenses and ingenuity on the part of the attackers.

- **Patch Management**: It would appear that patch cycles aren’t so foolproof after all or at least there are still adequate numbers of end users that are not patching machines in a timely fashion.

- **Network Shares**: Should vulnerability exploitation not succeed, Conficker then looks for network shares with weak passwords. While enterprises have significantly locked down the network perimeter over the years, the LAN itself is typically wide open.

- **Multi-faceted**: Conficker is a hard working worm. It attempts to exploit machines vulnerable to MS08-067, spread via network shares and even connected removable storage devices.
Enterprise Defenses: Adapt or Fail

The gaps within traditional layered security defenses described above are today exposing enterprises to significant risk. While many statements can be made about these failings, the following three statements tend to be universally accurate within today’s enterprise:

- Traditional defenses cannot be updated quickly enough to counter evolving threats
- They lack architectural flexibility for new enterprise organizational concepts and business shifts
- They impede introduction of new technology, creating friction within the business

It is critical to understand that the cybercriminals understand these failings very well. By constantly probing traditional defenses and testing security technologies, they have learned how to achieve a high degree of success in exploiting their targets. They understand how to create subtle payload changes to evade antivirus detection, and can even predict how long it will take until AV signatures catch up. They understand how to hide attacks within web applications and setup a command-and-control infrastructure that bypasses firewalls and Intrusion Detection Systems.

The arms race between cybercriminals and the information security defenders is never ending. As it currently stands, the balance of power has shifted decidedly in favor of the malicious actors. While it will not be feasible to provide perfect protection, it is incumbent upon enterprises to evolve the current generation of signature-heavy and statically-architected defenses into dynamic, on-demand security that raises the bar for enterprise protection. Taking these steps will cause the cybercriminals to move their attacks to the targets with simpler legacy defenses.

<table>
<thead>
<tr>
<th>Chapter Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security technology weaknesses: perpetually outdated malware signatures, fixed perimeter locations and lack of application visibility</td>
</tr>
<tr>
<td>Endpoint security software has an expensive cost of ownership and dubious security benefits</td>
</tr>
<tr>
<td>Heavy reliance on security appliances inhibit organizational ability to operate “on-demand”</td>
</tr>
<tr>
<td>Operational security investments preclude focus on solving business problems</td>
</tr>
</tbody>
</table>
Coming to an Enterprise Near You: Cloud Security

A key strategy shift that must occur as a result of cloud-based trends and the limitations of existing security practices is the adoption of a Cloud Security Architecture. This strategy allows an enterprise to have access to on-demand, point-of-use security perimeters in order to consistently enforce organizational policies and provide advanced threat management capabilities that keep pace with an enterprise’s dynamic adoption of cloud computing and user mobility. An important consequence of this shift is a strategic migration away from security appliances, which create location-based architectural limitations, high capital costs and critical points of failure.

In this architecture, the cloud security service provider is essentially taking over responsibility for the burdens associated with security device management: patching, signature updates, user management, log file maintenance and backups – duties which are not core to most businesses. This frees up your internal resources to think more strategically about how security capabilities can enable the business and how granular policies can be crafted that support compliance mandates while helping employees be more productive.

Natural Evolution of Security Delivery

A Cloud Security service can logically be seen as the next generation in a Security Capability Maturity Lifecycle. Initially, there is a manual process to solve a security problem. Next, it becomes automated through software. Then, it becomes easier to manage through a turnkey appliance. Finally, the solution becomes on-demand and available pervasively in the Cloud.

Security Capability Maturity Lifestyle

Cloud security is a natural evolution of security deployment from software and appliances
In addition to providing an elegant solution to the arcane and cumbersome security appliance overload, the Cloud Security Architecture also augments endpoint security. While we are not advocating removing the security software on a desktop PC or laptop yet, the cloud security service can protect the endpoint from critical web-borne threats and protect the enterprise from data loss with a **Zero Footprint Deployment** – no expensive-to-maintain software agent on the desktop. Cloud endpoint protection is provided on the “first hop” into the cloud, before the user reaches any web destinations.

**Various Architectures for Managed Security**

True Cloud Security should be differentiated from Managed Security Service Providers (MSSP) and Hosted Applications by CISOs seeking to procure the right solution for their enterprise.

**MSSP**: Outsourced management of on-premise equipment. Essentially the organization is attempting to shift labor costs to a service provider, but retains the appliances and all the associated costs, architectural and scalability limitations and points of failure. An example of MSSP is a vendor managing your distributed deployment of firewalls or desktops.

**Hosted Applications**: Provider acquires and manages single-tenant appliances. This architecture is not designed from the ground up for cloud operations. Boxes are essentially co-located, with no economies of scale gained from architecture with dangerous points of failure and troublesome performance issues. An example of Hosted Applications is a vendor deploying Squid web proxies in a data center and performing web filtering by routing your internet-bound traffic to the data center.

As clean water and electricity saw a natural move to professionally managed services, enterprise security is moving from a cottage industry to a professionally managed service.
**True Cloud Security:** Provider delivers a service with virtualized multi-tenant infrastructure designed to be resilient, redundant and high performing. An example of true cloud security is Zscaler which has a multi-tenant platform with a distributed global network.

*True Cloud Security from the Ground Up*
There is a reason why Salesforce.com became the killer app of cloud computing and Seibel Systems did not. Salesforce.com was built from the ground up to be Software-as-a-Service.

**Inbound versus Outbound Security**
Most of today’s security products—such as firewalls, VPN, IDS/IPS—protect corporate networks and servers from threats coming from the Internet. Newer threats infect end users accessing internet resources by using bots, phishing, and malicious active content, all of which subsequently infect corporate networks. Other than deploying caching and URL filtering products, corporations have done very little to inspect user-initiated traffic and protect their users.

With threats emerging from the Internet trying to compromise enterprises well under control, the new focus needs to be outbound security – protecting users while they are accessing the Internet.

The focus of this book is outbound security and outbound security in the cloud. When we say cloud security, we are not talking about securing the cloud computing platform such as Amazon or Google. We are talking about cloud-delivered security whereby internet bound traffic is filtered by a service in the cloud to make sure that the users are protected from the threats of the Internet. We are also not talking about replacing firewalls which do a fine job for inbound security threats. The focus of this book is newer threats which require monitoring internet-bound traffic.

*Web 2.0 is creating many risky backdoors; firewalls, IPS and anti-virus software on desktops is helpless to newer threats.*
In the following chapters, we will outline the major capabilities that Cloud Security must provide in order to offer complete protection to the enterprise as it enters the Internet:

- Architecture of a Cloud Security Service
- Security Threat Protection
- Policy Management
- Data Loss Prevention
- Reporting and Analysis

<table>
<thead>
<tr>
<th>Chapter Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Security Architecture protects organization when accessing internet</td>
</tr>
<tr>
<td>Dynamic, point-of-use perimeter created for each user and location</td>
</tr>
<tr>
<td>Zero Footprint on endpoint – protection provided at “first hop” into internet</td>
</tr>
<tr>
<td>Reduction in security appliances, endpoint software and associated costs</td>
</tr>
</tbody>
</table>
Architecture of a Cloud Security Service

Adopting a “Cloud Security Controls Architecture” shifts the balance of power back in favor of the CIO and CISO. It requires solutions that allow them to regain control of all computer-based business activity, including computing between an increasingly dynamic and mobile user community and enterprise digital assets, both of which are located both internally and on the Internet.

This is accomplished by replacing the notion of fixed enterprise network perimeters, which are easily bypassed and creating On-Demand Security Perimeters to protect users whenever they seek to access the Internet, either from enterprise or remote locations.

Companies simply define their corporate security, control and compliance policies by accessing the SaaS service. The web traffic leaving the network firewall is easily redirected to one of the data centers in the SaaS provider’s global infrastructure. Based on an organization’s policy, traffic is blocked, throttled, or allowed to access the Internet. As the browser retrieves the web pages, the service scans it for a range of malware threats and delivers clean traffic to the end user.

A cloud-delivered security service for the Web sits between the Internet and the user, offering a filtering and policy enforcement service to protect users. It can provide all key services including security, managed access, compliance, reporting and analysis.
Secure & Managed Access to the Internet – Key Functionality

The on-demand perimeter enables comprehensive protection against network and application layer threats, providing the following capabilities:

- **Visibility.** A Cloud security control point has a comprehensive vantage point over the entire Cloud of users, which provides a foundation for enforcement of organizational policies.

- **Comprehensive outbound security analysis.** Malicious actors have learned that rather than trying to bypass inbound security defenses (firewalls and IPS), the path of least resistance is to lure corporate users to infect themselves while visiting malicious websites. This simply bypasses firewalls and IPS defenses. Many of the latest active content attacks, such as Flash exploits, require no action on the part of the user other than visiting the wrong site. By inspecting outbound web requests and responses, it is possible to prevent users from infecting themselves from malicious web pages and also detect connection requests to nefarious sites owned by criminals. Without comprehensive outbound security, inbound security is ineffective.

- **Web granularity.** This means the ability to map web traffic into discrete applications and manage accordingly. For example, your organization may want to allow access to certain groups to specific public social networks, and disallow others. Or perhaps you want to allow all social networks at certain times of the day, or allow webmail applications but block file attachments.

- **Realistic Web 2.0 security policies.** The aforementioned web granularity will enable the CISO to define usage and security policies that protect the enterprise, yet recognize that users will expect reasonable access to Web 2.0 applications that are not core business applications.

- **Focus on user-centric security.** In the Hybrid Enterprise, the notion of trusted versus untrusted locations is severely undermined. Network-based security controls should be deemphasized in favor of directory-integrated security that authenticates and authorizes granular user activities.

- **Cloud-based web access control (WAC).** Network admission control is growing in popularity as a network-based security technology to assure endpoint integrity. Cloud-based WAC makes sure that the user has a clean browser environment before accessing enterprise information, whether in-house or in the cloud.

- **Focus on Data Loss Prevention.** A consequence of the rise of mobility is the ability to take data anywhere in large quantities using tiny devices. Cloud-based enforcement points should be instrumented to perform data loss prevention pervasively rather than merely at a single enterprise egress point.

- **Cloud-based attack detection.** Identify and block malware in the cloud rather than within your enterprise or on your users’ computing devices. This reduces the risk of successful security attacks on your assets by keeping detection at arm’s length, and also reduces the amount of computing resources you must devote to attack detection and remediation. The bots and other malware in the wild today are so resistant to traditional endpoint defenses that most organizations report that a costly full system rebuild is the only way to remove many types of malicious code. **It is cost effective and an important risk reduction strategy to keep the fight on foreign battlefields.**

A “Cloud Security Controls Architecture” is a design to deliver the appropriate amount of security on demand. The ability to create a dynamic, cloud-based, point-of-use perimeter around users and enterprise office locations is an essential foundation to provide a consistent security baseline unaffected by business changes, such as user mobility, office expansion and contraction due to corporate mergers & acquisitions.
It is useful to visualize a Cloud Security Framework as depicted in the following graphic. The service provider’s cloud platform must provide the subscribing customer the ability to fully protect its enterprise based upon the notion of a unified policy. A unified policy construct should support all necessary elements simultaneously: User, Device, Application and Data, allowing for extremely granular controls that support business needs. It should also support concepts such as Time (time-of-day, day-of-week, etc.) as well as Location, whether a true physical office or a virtual location.

By leveraging a unified policy capability, it becomes possible to deliver comprehensive security capabilities, organized within the following major domains:

- Threat Protection
- Managed Access to all resources
- Compliance to all relevant regulations, standards and corporate policies
- Analyze all usage and activities, creating a feedback loop to improve policies and management practices

*By leveraging a unified policy, a cloud service should be able to provide comprehensive functionality eliminating the need to buy multiple point products.*

**Architecture of Cloud Security**

In evaluating a cloud security service, it is important to recognize the radical shift that cloud computing represents. It is critical to select security solutions built from the ground up to exist in the cloud, rather than migrating legacy security solutions into the cloud.

**Mesh versus hierarchical architecture.** The redundancy and effectiveness of a cloud security service is optimized by a mesh architecture, which essentially follows the design that has made the Internet itself so resilient and popular.

- **Multi-tenant architecture.** The ability to create on demand perimeters requires pervasive security control devices located throughout the fabric of the Internet, bringing performance close to the user and corporate network, rather than requiring inefficient roundtrips to a relatively small number of data centers. This is illustrated in the diagram below.
Security “points of presence” should be pervasive within the fabric of the Internet, bringing performance to the user and corporate network.

- **Inline performance.** Unlike applications such as email which are “store and forward,” protecting the “Cloud of Users” must be done without perceptible latency. This requires next generation high performance capabilities. Combined with the overall architecture, this must deliver high performance on a global scale for any location as users become more mobile.

- **True web application granularity.** Not only must web applications be individually identified for granular control, but also specific activities within an application must be explicitly articulated for unique policy-based controls.

- **Real-time security.** Cloud security solutions should update the protection capabilities and policy changes for every user and business location in real-time.

- **Comprehensive Logging.** The ability to log all internet traffic activities occurring on behalf of the enterprise but outside its perimeter is one of the most critical capabilities a cloud security service must deliver. Robust and comprehensive logging should be available to provide CIOs and CISOs with regulatory, forensics and management accountability.

- **Heterogeneous support.** The cloud security service should be agnostic to different endpoint devices and data center computers. It should provide uniform security protection to different operating systems, laptops, mobile devices, etc.
Chapter Takeaways

- In-The-Cloud Security Architecture calls for “on demand security perimeters” to block threats and enforce policies
- Design requires extreme granularity in user, application and device management
- Redundancy architecture should mirror best practices of internet itself
- Must be designed from the ground up as a cloud-delivered service, rather porting of legacy security devices into the cloud

An example of a state-of-the-art, cloud-delivered, distributed security architecture
Security Threat Protection

Let us dig deeper into what cloud security means from a threat protection perspective. By definition, users today are going “out” into the cloud in order to access data and applications to solve business problems. This means that cloud security service and its dynamic point-of-use perimeter is directly managing the security of outbound traffic, whether leaving corporate firewalls, PC desktops, smart phones or the notebook computers of your road warriors.

All internet bound traffic passes through the cloud security inspection on their “first hop” in order to apply organizational policies prior to reaching any web destinations. Policy is the foundation for this architecture, as the user experience and levels of protection must be set at the discretion of the CISO to align with business needs and risks. Because the sophisticated malware of today and the future uses bi-directional “command and control” traffic, cloud security is indirectly managing inbound security as well, and is thus capable of providing broad security protection to the enterprise.

Protecting the HTTP Channel against Viruses

Virus detection is not new: combined with the firewall, antivirus (AV) represents the oldest defense employed by enterprises to protect their computing assets. Existing antivirus products are designed to look for viruses on the desktop and within email messages at the email gateway level. Web traffic typically has no virus protection within enterprises, primarily because this has been a difficult technical problem to solve. Some readers may argue that desktop AV running in protective “shield” mode provides an indirect protection against viruses within web traffic. We would disagree. Based upon the high rate of new malware introduction, and the difficulty to mitigate viruses post-infection, viruses have a clear path via web channels.

As was mentioned previously, the malicious actors well understand this enterprise weakness. They have moved to Web 2.0 sites as the primary launching pad for new malware, as they know this is the most difficult threat vector to defend. The primary reason that web traffic has never been protected is due to the performance degradation this would cause with traditional AV. Users will revolt against security solutions that impede performance. A cloud defense, which can aggregate processing power, is the only solution specially designed to look for viruses within HTTP (web) transactions without introducing perceptible latency. The performance is not strictly due to carrier grade equipment and sophisticated scanning technology, but is also a function of the cloud-based visibility. Antivirus protection that is specifically built for a cloud service operation has the capability to tag infected files and block every subsequent download of the same tagged file – immediately, regardless of source or destination and without scanning it first.
Beyond being fast, the cloud-based malware detection must be accurate, using a combination of AV signatures, content analytics and site reputation. Although signature-based protection has clear challenges in responding to new threats in a timely manner, it is important to note that it is not obsolete. Once a defense like AV is well known, it becomes a permanent defense, as cybercriminals would shift tactics and return to deprecated viruses if signature defenses were omitted. The trick is to optimize the value of signature defenses. A large enterprise may have literally hundreds of thousands of signature files to maintain, and must compromise between the frequency of updates and other tasks. A cloud security provider will have a few signature files to maintain, and can devote significant time to real-time updates, and can even perform customized updates to improve signature accuracy. Simply put, virus protection is a core requirement for cloud security threat protection.

Advanced Threats: Malicious Active Content, Botnets and more...

Advanced threats represent the next generation of malware and are likely the most important threat protection a cloud security service can deliver. Botnets, peer-to-peer applications (P2P) and other threats that leverage Web 2.0 scripting technologies have such sophisticated distributed architectures and dynamic deployment capabilities that they are completely immune to traditional layered defenses. Cloud security has a distinct advantage in defending against advanced threats by employing multiple content inspection capabilities, understanding the full context of distributed malware activities via end-to-end visibility, and leveraging analytics across a global network to detect the movement and changes in the malware behavior. A cloud security service will inspect internet bound traffic and identify advanced threats before the return traffic can infect the user. In some cases the detection may be due to malicious active content, such as ActiveX, Ajax, Flash, or JavaScript, which is identified during content inspection. In some cases, the cloud security service will protect the user based upon the destination of the request, which may be a cybercriminal’s command-and-control website, or a phishing site designed to capture sensitive personal information.

With the prevalence of Web 2.0 technology in all leading websites, we are seeing an increase in the phenomenon of popular commercial websites being used as attack launch points. For example, a popular news website can host malicious cross site scripting (XSS) attacks within the user comment sections of each story. Users may become infected by simply accessing a respected site they assume to be trustworthy. A cloud security service with sophisticated content scanning capabilities can deconstruct the session traffic to identify this and many other web-hosted threats. An appropriately architected cloud security service can also detect and block peer-to-peer applications (P2P), which can consume internet bandwidth and create security as well as liability risks for your organization.

Full content inspection is required to effectively detect newer, more sophisticated web threats.
Key to Advanced Threat Protection – Full Content Inspection

The key to effective detection of web threats is inherent in the ability to provide full content inspection. For performance reasons, most security solutions will perform header detection only, or partial content inspection. By leveraging carrier class equipment, it is possible for the cloud security provider to perform full content inspection with no noticeable latency to the user.

Web Access Control

Cloud security that is managing outbound traffic can recognize and classify web browsers based on their User-Agent signature. Policy management capabilities can specify which web browser vendors and versions should and should not be allowed for use. This provides granular control over the use of outdated browsers in your enterprise, effectively reducing risk by preventing them from accessing the Internet. This on-demand version control capability is especially helpful in combating new malware arising from reverse-engineered browser patches.

Outdated Browser Threats

The general threats posed by outdated browsers:

- Outdated browsers can contain the same vulnerabilities as discovered in their newer brethren
- Due to discontinued vendor support, vulnerabilities will not be patched nor will there likely be any public notification even if vulnerabilities do exist
- Newer security-related features (integrated phishing warnings, extended SSL verification, security-conscience dialog popup options, etc.)

Security threats caused by web surfing habits rank as the top threat to an organization’s information systems. Furthermore, the ability to contain and remove these threats is virtually non-existent once the malware is present within your systems. These threats are extremely fast moving, and are beginning to attack new platforms such as mobile devices, likely in advance of your ability to employ appropriate endpoint security solutions. Leveraging a cloud security service to provide virtual endpoint protection at the “first hop” into the Internet, in order to block advanced threats off premises and provide on-demand protection to new endpoint devices as they appear, represents key cloud-based functionalities that can greatly improve your organization’s risk posture.
## Chapter Takeaways

- High-performance cloud-based processing provides uniform endpoint protection on “first hop” into cloud, agnostic to endpoint device type or operating system
- Detect traditional viruses in the HTTP channel
- Block advanced Web 2.0 threats such as botnets, malicious active content, P2P that currently evade all other defenses
- Web Access Control: manage access according to browser type, version and patch level
Web 2.0 Managed Access Policies

Web 2.0 trends - from social and business networks to user-generated content - create both opportunities and challenges for today’s organizations. Users are no longer just the consumers of web content; they are now the creators. This provides marketing opportunities and increased productivity. However, without appropriate controls, this can also create liabilities for organizations when their employees publish inappropriate or confidential content on blogs and social networks. Furthermore, the use of rich multimedia applications, such as audio and video streaming technologies, can negatively impact the network performance of the entire office - instantly affecting productivity.

What is Web Access used for?

- Firewalls see web traffic as one application; Web 2.0 policy management solutions identify thousands of different applications embedded in normal web traffic
- According to several studies, nearly 50% of web traffic is streaming audio and video
- YouTube consumed as much bandwidth in 2006 as the whole internet did in 2000
- P2P applications now use HTTP tunneling to bypass corporate firewalls and evade ISP traffic throttling techniques

It is helpful to think of these managed access capabilities in three main categories:

URL Filtering

In this case, we are blocking websites or sections of websites via their domains. This is not used to protect against malicious technical threats which undergo rapid address changes, but rather liability to the business based upon the content of the site. For example, these sites could be gaming, inappropriate content, competitors and other sites which could impact productivity or create legal consequences for the enterprise. As with AV signatures, a cloud provider has the advantage of being able to rapidly update its URL databases on all points of presence. At the same time, you should be assured of the ability to create customized lists of URLs to block based upon your own business needs.
**Web 2.0 Application Control**

Cloud Security provides unique opportunities to manage access to Web 2.0 applications. The answer is not to block access completely, nor is it to allow unrestricted access. The solution lies in providing managed access. Organizations should create flexible and granular web access policies by action (e.g. reading versus posting), location, and group.

Below are some examples of all three areas of managed access capabilities:
- Allow selected Webmail applications, but block users from attaching files, which usually risks data leakage
- Allow all employees to access and view social networks for an hour a day, with the exception of marketing, which can view and publish on social networks such as Facebook to promote communities of interest
- Prohibit pornographic websites which violate company policy and local obscenity laws
- Allow employees to view videos & listen to audio on streaming media sites for a maximum of 50 megabytes per day, but prohibit uploading content during office hours
- Allow certain instant messaging (IM) applications for chat, but prevent file transfers using IM
- Allow employees to read blogs, but not post to them
- Block competitors’ websites, except for groups doing competitive research

**Bandwidth Optimization**

As mentioned above, applications such as YouTube have exploded in their popularity and bandwidth consumption, potentially disrupting critical business applications and leading to increased telecommunication costs. The ability to throttle these applications or place some time limits on usage can increase user productivity, business application performance and decrease costs.

*Application-level control can enforce the appropriate allocation of bandwidth and reduce costs. For example, the use of rich multimedia applications, such as audio and video streaming technologies, can negatively impact the network performance of the entire office.*
The optimal Web 2.0 policy management solution combines the following features:

- Extensive catalog of web applications (Facebook, Google Docs, etc.)
- Rules based upon specific web application functions (file attachments, posting, etc.)
- True user and group management (directory versus IP address)
- True location management (dedicated IP versus assumptions of user behavior)
- Time-based restrictions (off hours versus peak hours)

### Chapter Takeaways

- CISOs must be aware of the thousands of different applications that appear to be web traffic to your firewall
- Rich multimedia applications may inhibit line-of-business application performance
- Provide granular access and subtle throttling to Web 2.0 applications as opposed to simplistic deny or allow rules
- Support granular policy criteria such as User, Specific Application, Time-of-Day, Bandwidth Consumption, Action (Reading versus Posting)
Preventing Data Loss with Cloud Security

As the traditional perimeter is vanishing and enterprises are connecting to their customers and partners, data leakage is becoming an expensive, burdensome problem. Employees, whether innocent or malicious, can easily send a Webmail or instant message with confidential information. Information can be posted on social networks and blogs instantaneously. Customer’s private information, such as Social Security and credit card numbers, is protected by government regulations and leakage creates legal liabilities which can damage a company’s brand reputation. Further, leaks of sensitive company information risk financial loss.

**Ponemon Institute: 2008 U.S. Cost of a Data Breach Study**

- Average $202 cost per customer record
- Average total per-incident costs in 2008 were $6.65 million, compared to an average per-incident cost of $6.3 million in 2007
- Third-party organizations accounted for more than 44 percent of all cases in the 2008 study and are also the most costly form of data breaches due to additional investigation and consulting fees
- More than 88% of all cases in this year’s study involved insider negligence

<table>
<thead>
<tr>
<th>Date</th>
<th>Records</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jan 2009</td>
<td>100,000,000</td>
<td>Heartland Systems (record loss still being verified at publication time)</td>
</tr>
<tr>
<td>Jan 2007</td>
<td>94,000,000</td>
<td>TJX Companies Inc.</td>
</tr>
<tr>
<td>June 2005</td>
<td>40,000,000</td>
<td>CardSystems, Visa, MasterCard, American Express</td>
</tr>
<tr>
<td>July 2004</td>
<td>30,000,000</td>
<td>America Online</td>
</tr>
<tr>
<td>May 2006</td>
<td>26,500,000</td>
<td>U.S. Department of Veterans Affairs</td>
</tr>
<tr>
<td>Nov 2007</td>
<td>25,000,000</td>
<td>HM Revenue and Customs, TNT</td>
</tr>
<tr>
<td>May 2008</td>
<td>12,500,000</td>
<td>Archive Systems Inc, Bank of New York Mellon</td>
</tr>
<tr>
<td>Sept 2008</td>
<td>11,000,000</td>
<td>GS Caltex</td>
</tr>
</tbody>
</table>

* Source: Open Security Foundation
Why Traditional DLP Solutions Have Failed

Traditional security architecture calls for a gateway appliance solution to prevent data leakage. These products often require extensive implementation and consulting services. Because of performance limitations, these solutions only inspect email communications and completely miss the more common web vector. This is unacceptable, as Facebook, blogs and webmail have become top threat vectors for data leakage.

The best way to ensure proper inspection for DLP is to have proxy gateways inspect the traffic. This works for email proxies since SMTP email is a store and forward protocol and does not care about latency of a few minutes. The Web is an interactive protocol. If web proxies take users’ response time from half a second to few seconds, users will revolt. Traditional web proxies are too slow to perform inspection of outbound web content. Some customers have found a work around by using DLP point products in “tap” mode. In this mode, the DLP appliance does not sit in-line and hence does not introduce latency. It tries to identify policy violations and send a reset connection. This works reasonably well for proof of concepts but if you are running heavy traffic, this approach becomes unreliable. The traffic with sensitive data may have passed before the reset command is sent. This approach is akin to sitting on the side of a highway and trying to shoot at suspected vehicles.

Not surprisingly, less than 5% enterprises have deployed data leakage prevention (DLP) solutions today. Those organizations which have deployed DLP solutions can typically afford to protect only one network egress point out of the hundreds they may have. If an employee takes the data on the road with a laptop computer, the company has no preventative controls. Considering the Ponemon Institute finding that 88% of the data breaches studied in 2008 were the result of insider negligence as opposed to master criminals, it is less important to have a highly sophisticated DLP solution monitoring a single network exit that it is to have broad DLP coverage everywhere.

Pragmatic Approach to DLP

Organizations have a critical mandate to protect regulated and other sensitive information; one of the top five priorities of CISOs based upon recent surveys. Data leakage prevention begins with policy. Translating business policy and rules into a data protection policy creates the following process cycle:

- **Define.** Create a data protection policy based upon regulatory and business risks.

- **Detect.** Enable a detection mechanism to identify policy violations.

- **Enforce.** Determine level of active blocking versus notification or logging based upon the sensitivity of the data and importance of the business activity using the data.

Define a DLP Policy based on Intellectual Property or regulatory compliance, enable a detection mechanism, and apply different policies for different user groups.
The detection and enforcement processes should be consistently reviewed through dashboard reporting and log files in order to tune the policy definitions.

Data loss prevention is an area where cloud security truly shines. By moving the content inspection point off premise and into the cloud, IT is able to immediately activate a DLP policy that protects the entire enterprise, and sensitive data will be blocked on the first hop into the cloud, before it can fall into the wrong hands.

The risks of data breaches spur organizations to perform full inspection of all HTTP and HTTPS traffic leaving the organization, looking for two main categories of violations:

- Regulatory compliance by state or federal governments, or other standards bodies, often pertains to personal or private consumer information. Examples include regulations such as HIPAA, GLBA, PCI, or SOX.
- Company sensitive information may include sales data, pricing information, or intellectual property such as source code.

### Chapter Takeaways

- Data leakage is a high priority pain point for CISOs – tremendous liability and compliance issue
- Studies show most data breaches related to insider negligence and broken processes
- Conventional data loss prevention solutions are comprised of email gateways or endpoint software – incomplete and unrealistic in the cloud-enabled and mobile enterprise
- Leverage cloud security to block data leakage from all organizational egress points – HQ, remote offices, mobile devices
Fundamental to a productive, metrics-driven security program is a robust reporting capability. Any time a new approach to solving security problems is implemented, reporting becomes even more important to understand the impact and effectiveness of the new controls. This is especially true for off-premise security protection, where the management console and reports may be your only direct interaction with the solution.

We believe three broad principles must be inherent in a cloud security solution:

- **High level presentation of information** – the ability to capture broad trends, to understand the “big picture” and potentially predict future events
- **Drill down** – being able to quickly move to progressively more detailed and granular information, down to a specific transaction in a log file
- **Real-time** – immediate access to current activity to be able to respond more quickly to incidents

Among the broad functional reporting needs related to security:

- Executive dashboards
- Policy & Compliance
- Operational management
- Baselines/metrics geared towards continuous improvements
- Analytics, situational awareness
- Cost center accounting
- Risk/vulnerability assessment
- Incidents
- I/R & forensics
- Usage

A key challenge inhibiting the production of timely and accurate reports is the ability to collect, normalize and present the data. The previously referenced security appliance conundrum exacerbates this problem. Log files are scattered throughout the enterprise, using different file formats and capturing different data elements. Aggregating log files after the fact is an extremely difficult challenge, typically providing incomplete answers too late to be useful.

There are technological innovations happening in log management whereby the log size can be reduced by a significant factor without losing any information. This enables cost effective storage of logs and faster retrieval of information. This will also allow cloud security providers to offer log retention for several years rather than a few months.

Cloud Security has the potential to radically alter information security reporting, and with it significantly change the productivity of the business. By combining all of the above mentioned security functions into a single integrated service, a single log file can provide a tremendous amount of useful information in real time.
Comprehensive and integrated functionality enables integrated reporting. For example, see specific web usage or security risks across all locations, all users, or all departments. Moreover, see powerful trending metrics.

**Chapter Takeaways**

- Reporting is key functionality for security program improvement, attestation and compliance
- Broad reporting principles: High Level Trending, Granular Drill Down and Real Time Accuracy
- Timely and accurate reporting dependent upon quality of underlying data – centralized log file information
Cloud Security Provider Assurance & Trust

Today’s modern enterprise can leverage partners to outsource a great deal of non-strategic operations. However, it is not typically possible or even advisable to outsource accountability. As global organizations leverage more cloud computing service providers, regulatory compliance is an important issue to address. Perhaps even more important are your own organizational risk tolerances and the assurance that your cloud security provider is lowering risks, increasing availability and protecting assets, while providing this service at a lower cost than could be done internally. Fortunately, the assurance and attestation tools are available to meet both external and internal mandates.

**PCI DSS: Service Providers Included**
The Payment Card Industry / Data Security Standard provide guidance on managing service providers, such as those operating in the cloud, in section 12.8. Requirement 12.8.2 states:

"Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess."

Currently, the standard for cloud service provider attestation is the SAS 70 Type II audit. SAS 70 stands for Statement on Auditing Standard 70. It was created by the American Institute of Certified Public Accountants (AICPA), and was developed to provide standards for auditing service providers. The Type II audit adds a section for the auditor to attest to the effectiveness of the controls in place. Any party reviewing a SAS 70 report or requesting a new audit should ensure that the scope of the audit is appropriate for their own assurance needs.

**U.S. Federal Government Getting into Cloud Security?**
NIST has announced that a Special Publication will be created in FY09 to address cloud security, covering the following main issues:

- Overview of cloud computing
- Cloud computing security issues
- Securing cloud architectures
- Securing cloud applications
- Enabling and performing forensics in the cloud
- Centralizing security monitoring in a cloud architecture
- Obtaining security from 3rd party cloud architectures through service level agreements
- Security compliance frameworks and cloud computing (e.g., HIPAA, FISMA, SOX)
In addition to the security features, key assurance concerns expressed by clients of cloud security providers include high availability and reliability in the provider architecture. When developing a relationship with a cloud security provider, consider the following:

- Service provider company practices and policies
- Management team
- Service level agreements
- Transparency in system operations
- Robust logging
- Frequent testing of controls
- Global coverage
- Strong authentication, authorization and access control practices
- Liberal use of encryption

In the future, we can expect all information security and IT audit frameworks such as ISO 27001, COBIT and others to be applied more specifically to cloud security.

<table>
<thead>
<tr>
<th>Chapter Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud provider assurance standards are new and evolving</td>
</tr>
<tr>
<td>SAS 70 Type II is most prevalent</td>
</tr>
<tr>
<td>Level of due care dependent on type of service provided and whether provider is hosting regulated data</td>
</tr>
<tr>
<td>Align assurance with organizational risk tolerance and commonly available best practices for information security management systems</td>
</tr>
</tbody>
</table>
Incident Response & Forensics

As is the case with compliance and accountability, CISOs have a key responsibility in incident response and forensics, regardless of the degree to which the organization uses contractors, consultants and service providers.

Information security’s extensive experience with outsourcing provides guidance on some of the likely key issues in resolving incidents and conducting investigations in conjunction with a cloud service provider:

- **Legal jurisdiction.** Is there any impact on the relevant laws based upon how the cloud provider is organized?

- **Data retention policies.** What types of data are they storing and what are their policies?

- **Cloud Service Provider’s role.** It is important to understand what role your Cloud Service Provider will play in an incident. In an ideal situation, your organization is provided with transparent access to log files, reporting and management control to give you flexibility in managing incidents based upon their sensitivity. In any case, Service level agreements (SLAs) should be established.

While it is important to assure that your cloud computing providers have the capabilities and SLAs to assist with incident response and forensics, cloud security services can actually be a boon to investigations. The comprehensive visibility into the entire organization’s web traffic, whether occurring on premises or remotely, can create insights to solve problems more rapidly and effectively than before. Examples may include:

- **Data exfiltration.** An insider may download...
Sensitive data in the office, take it on the road and attempt to send it to an inappropriate location from a remote internet connection. An administrator will be able to track all activities conducted by the suspicious user, regardless of location.

**Serial Spear Phishing.** Criminals may attempt to methodically compromise an organization location by location, leaving a pattern of attack discernable by an administrator with a broad view of the enterprise.

---

**Collaboration on Incident Response**

By taking advantage of the “Network Effect,” cloud security providers can accelerate information sharing and analysis and reduce the overall number of incidents any participating organization suffers. The following groups may also be appropriate to collaborate with on incidents:

- **Information Sharing and Analysis Centers (ISACs)**
  - Electric: www.nerc.com
  - Financial Services: www.fsisac.com
  - IT: www.it-isac.org
  - Oil & Gas: www.energyisac.com
  - Telecom: www.ncs.gov
  - Water: www.amwa.net/isac/
  - Multi-State: www.msisac.org
- **Government Forum of Incident Response and Security Teams**
  - www.uscert.gov/federal/gfirst.html
    - InfraGard: www.infragard.net
    - SANS: www.sans.org
    - US Cert: www.uscert.gov

---

**e-Discovery**

It is predicted by many experts that we will soon see an explosion in e-Discovery requests that significantly impact IT and information security. Cloud Computing and its superior storage management capabilities will likely be a large beneficiary of the e-Discovery boom. Google is among the companies that have already begun offering services to archive data and offer e-Discovery services.

---

**Key Findings of SANS 2008 Log Management Survey**

- 78 percent of respondents said their reason for collecting log data was “Detection and Analysis of Security and Performance Incidents.”
- The number one log analysis pain point reported by 51% of respondents was the basic task of collecting logs
- Average Global 2000 firm spends $190,000 annually on log file analysis

However, it is important to realize that the legal profession is being trained to take a holistic perspective to vetting the trustworthiness of electronic information, and seek to have it admitted or invalidated based upon
their interests. Key to this is understanding **metadata** that provides critical context to the information itself. The most important metadata to obtain and protect are log files, which in theory should provide non-repudiated evidence of actions and intent. **Log file management is likely the most important service your cloud security provider can offer as it relates to e-Discovery and Forensics in general.**

### The mandate for robust logging

- That which was not recorded did not happen
- That which is not documented does not exist
- That which has not been tested is insecure

*Jeffrey Ritter, noted e-Discovery attorney and CEO of Waters Edge, LLC*

### Chapter Takeaways

- Cloud security providers are a partner in your Incident Response and Forensics strategy
- Key issues include legal jurisdiction, data retention policies, Service Level Agreements
- Broad coverage of web traffic is strategic in “connecting the dots” for managing incidents
- Provably secure and consistent log file management is critical to e-Discovery and related forensics activities
Extending Cloud Security to Partners

In our highly interconnected global economy, business partners play an increasingly important role in our organization’s success. Gone are the days when a manufacturer would own every aspect of its supply chain, from the raw materials to the finished product.

_Supply Chain Security Woes_
A recent study by Aberdeen Group shows that few companies can afford to ignore supply chain risks. Almost 99 percent of the 138 companies surveyed suffered a supply chain disruption and 58 percent suffered a financial loss.  

Information security within a supply chain has been historically problematic. We have a mandate to share our data with selected partners; however, we may not trust our partners’ security controls and ability to protect our data once they have it. On the other hand, we do not have the ability to dictate their architecture, or if we do it may come with an unwanted responsibility to provide operational support.

_In-The-Cloud Supply Chain Protection_

Cloud security providers offer tantalizing possibilities to be the arbitrators of trust and protect supply chains with acceptable, non-intrusive security baselines to all partners. In this scenario, a partner needs to gain access to databases located at your headquarters datacenter. In order to trust inbound network traffic from the partner, we can direct them to go through our cloud security protection before reaching our datacenter. In this example, we may have our IT admin configure three security checks:

- Antivirus/Antispam detection
- Advanced threat detection, such as botnets
- Web browser version, to only allow the partner to connect to our site with the most recent browser

This extra layer of protection would require no hardware or software installation by the partner, and would likely be as simple as a single firewall rule.

Large organizations that are characterized by a high number of small partners are ideal targets to investigate cloud security for their partners. In many cases, these large organizations have already shouldered a significant amount of operational security for these partners that could not otherwise justify it. A common example is a healthcare cooperative, where large hospitals foot the bill for security at small affiliated medical clinics and doctors’ offices. Another example of this will be an organization using salesforce.com may require its users to come through a cloud security provider. An internet portal may require the same thing from its users.
<table>
<thead>
<tr>
<th>Chapter Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Security assurance among business partners is an ongoing challenge</td>
</tr>
<tr>
<td>▪ Inability to dictate security standards to partners or encumbered with partner operational security</td>
</tr>
<tr>
<td>▪ Cloud security offers non-intrusive, “zero footprint” means to assure partners have an acceptable baseline of security before accessing supply chain</td>
</tr>
<tr>
<td>▪ Organizations with a large number of small partners are an ideal candidate to evaluate cloud partner security</td>
</tr>
</tbody>
</table>
The Business Case for Cloud Security

Cloud computing in general is able to provide organizational ROI by both increasing the business agility and reducing costs. According to Forrester Research, cloud-based servers have 5 to 10 times greater utilization than enterprise servers, while cloud administrators have similarly improved efficiencies due to improved processes and the benefits of specialization. The resultant cost reductions experienced by cloud computing customers include:

- Hardware capital costs
- Software licenses
- Maintenance contracts
- Labor costs for managing IT infrastructure
- Energy costs

Below is a TCO calculator from a cloud security provider, which drives home the cost savings that can be achieved by leveraging cloud security as opposed to traditional approaches.

<table>
<thead>
<tr>
<th>Total Cost of Ownership (TCO) Computation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Appliances</strong></td>
</tr>
<tr>
<td><strong>Upfront Costs</strong></td>
</tr>
<tr>
<td>Purchase boxes and software</td>
</tr>
<tr>
<td>Deployment cost</td>
</tr>
<tr>
<td>Training Cost</td>
</tr>
<tr>
<td><strong>Total Up-front Cost (Capex)</strong></td>
</tr>
<tr>
<td><strong>Recurring Costs</strong></td>
</tr>
<tr>
<td>Annual Maintenance (appliance) or Subscription Fee (SaaS)</td>
</tr>
<tr>
<td>Annual On-going Administration Cost:</td>
</tr>
<tr>
<td><strong>Total Costs</strong></td>
</tr>
<tr>
<td>Three Year Recurring Cost</td>
</tr>
<tr>
<td>3 Year Total TCO: Upfront &amp; Recurring</td>
</tr>
</tbody>
</table>

In addition to the above cost savings, cloud security service also achieves ROI in the following areas:
- Eliminate multiple single-purpose security appliances performing URL filtering, antivirus, data leakage protection, botnet prevention, P2P and IM control, Web threat management and bandwidth savings
- Appliance signature updating and patch management
- Integration costs
- Unexpected benefit of web policy management reducing telco costs

Go Green with the Cloud

Studies estimate up to 2% of the United States’ electricity powers data centers, whose servers are idle 85% of the time. Using cloud computing, including cloud security providers, reduces the need to purchase security appliances, resulting in lower power consumption.

Web Usage Policy Management: A Hidden Cost Saver

Businesses typically absorb large telecommunications costs to provide internet service. While all executives are aware that much of the bandwidth used is for non-business uses, such as streaming video and audio, attempting to block this traffic is challenging and decreases organizational morale.

We are seeing 20% to 30% savings in bandwidth by applying bandwidth control policies.

Zscaler, Inc.

While a business may choose to absorb this cost, the penalties accrued when exceeding committed information rates often leads to expensive telco bills, based upon the arcane billing rules devised by telecommunications providers.

CISOs have a rare opportunity to create immediate cost savings via granular web usage policy management. Sophisticated cloud security services enable users to access rich applications, but can limit the amount of bandwidth that is consumed for streaming media. Using subtle throttling techniques, users can still access streaming web sites, and are unaware of the bandwidth controls being enforced. CISOs can also employ more overt restrictions, such as allowing social networking sites during specific hours, such as during lunch or after normal business hours. The lower internet connectivity bills can be dramatic, in some cases paying for major security projects. The ability to reduce telecommunications costs with granular web policy management is one of those perfect storms where good security and tangible ROI are aligned!

Sharethis: ROI

Sharethis, a social media company, reported using cloud computing to scale from 100 to 3,500 machines in a single day for less than $200.

CIO.com, October 2008
<table>
<thead>
<tr>
<th>Chapter Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Businesses adopting a cloud security stand to reduce capital expenditures for hardware and software</td>
</tr>
<tr>
<td>- Businesses also save on operating expenses such as labor, maintenance contracts and energy costs</td>
</tr>
<tr>
<td>- Granular Web 2.0 usage management may result in greatly reduced telecommunications costs</td>
</tr>
</tbody>
</table>
Recommendations for Transitioning to Cloud Security

It is the objective of every CISO to operate the highest quality and most efficient information assurance program in alignment with the company’s risk tolerance and governance practices.

A high quality security program is often characterized by the ability to innovate, and drive business value with transformational practices. Cloud security is just such a transformational practice that can increase business agility and generate ROI. In fact, the more an organization adopts progressive technology, the greater the mandate is for cloud security. As an additional benefit, its adoption allows the CISO to employ business analysts as opposed to operational security experts. Instead of fostering competencies related to operational security, such as firewall and web proxy management, business analysts can focus on policy and architectural issues, as well finding innovative ways for security to enable new business initiatives.

While cloud security is a key strategy and even a business differentiator, its on-demand nature means that it can also be employed to solve tactical problems and even be utilized as a data gathering tool to help justify a broader adoption of cloud computing. It is trivial to subscribe a single computer or a small location to a cloud security service. We believe that CISOs should evaluate cloud security now, both to prepare their organization for its future adoption of all forms of cloud computing as well as to provide feedback to providers.

The Evolving Role of the Security Organization

In an era when the business environment is very dynamic, how do you distribute the resources where they’re needed?... How does the security team guess how many resources they’re going to need in order to manage all of the requirements across the organization? Instead of building a security empire, have the organizations own the incremental assets. Security provides the standards and has a governance program.

William C. Boni, CISM, VP IT Security Motorola, Inc.
As you begin the process of evaluating cloud security, we recommend that you ask the following questions to appropriate stakeholders:

- Do we have a detailed breakdown of the usage of our internet connections and how that relates to our business needs?
- What are the costs of the Internet security appliances our organization has? Do they adequately protect against emerging threats and do they cover all user constituencies?
- Where are we using Software-as-a-Service, and what other internet-based services may potentially be storing organizational data?
- Can we currently prevent a user from leaking sensitive or regulated information, either at headquarters, remotes offices or on the road?
- How many internet connections/network egress points are used by our enterprise, including mobile workers?
- What endpoint devices are used by our organization (laptops, PCs, iPhones, Blackberrys, etc.)?
- Which popular Web 2.0 sites are used by employees, such as Facebook, MySpace, LinkedIn, etc.?
- Do we manage access to web-based email services?
- Do employees and partners access business systems from home?
- What are our data communications costs related to internet activity?

<table>
<thead>
<tr>
<th>A Possible Cloud Security Implementation Roadmap</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable service in passive monitoring mode</td>
</tr>
<tr>
<td>Use monitored data in risk assessment to identify prioritized risks</td>
</tr>
<tr>
<td>Adjust security and internet usage policies as needed</td>
</tr>
<tr>
<td>Determine cloud security services to enable</td>
</tr>
<tr>
<td>Pilot service with a department (IT is a great test group)</td>
</tr>
<tr>
<td>Add additional departments, locations</td>
</tr>
<tr>
<td>Continue transitions</td>
</tr>
</tbody>
</table>

By analyzing your business and asking the right questions, it is highly likely that you will find an avenue to at least partially implement cloud security in a way that is neutral or positive to your current fiscal year budget. More importantly, you are creating an architectural blueprint to allow your business to reap future rewards from the global trends towards Cloud Computing, Mobility and Web 2.0.
## Chapter Takeaways

- Create an internal strategic shift from operational security competencies to business analytics: policy, architecture and business enablement
- Because cloud security is by nature “on-demand,” there are virtually no barriers to evaluating solutions and beginning pilot programs today
- Building competencies towards developing a Cloud Security Architecture best positions the organization to take advantage of the business-changing trends in Cloud Computing, Mobility and Web 2.0
References

Chapter 1


Chapter 2


Chapter 3


Chapter 5

Chapter 6

Chapter 7
Open Security Foundation Data Loss DB
http://datalossdb.org/
http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9127376
Washington Post, “Data Breaches Up Almost 50 Percent, Affecting Records of 35.7 Million People”
http://www.washingtonpost.com/wp-dyn/content/article/2009/01/05/AR2009010503046.html

Chapter 9
NIST, “Perspectives on Cloud Computing and Standards”
Tech-Faq, “What is SAS 70?”
http://www.tech-faq.com/sas-70.shtml
IT World, “Cloud computing and compliance: be careful up there”
SearchSecurityAsia, “Cloud compliance: How to manage SaaS risk”
http://www.searchsecurityasia.com/content/cloud-compliance-how-manage-saas-risk?page=0%2C0

Chapter 10
NIST, “Guide to Integrating Forensic Techniques into Incident Response”
e-Discovery 2.0, “Google moves E-Discovery to the Cloud”
http://www.clearwellsystems.com/e-discovery-blog/2008/05/19/google-moves-e-discovery-to-the-cloud/
CIO.com, “CIO Cyberthreat Response & Reporting Guidelines”

Chapter 11
Industrial Market Trends, “Shoring up Supply Chain Security”

Chapter 12
CIO.com, “Who is getting ROI from Cloud Computing Now”

James Hamilton, “Cost of Power in Large Scale Data Centers”

Sumit Datta, “Go Green by Adopting Cloud Computing and Virtualization”

CSOOnline.com, “Acceptable Use Policies for Web 2.0”
http://blogs.csoonline.com/acceptable_use_policies_for_web_2_0
About the Author

Jay Chaudhry

Jay is a seasoned entrepreneur and experienced technology executive with a track record of success. He is an innovator and trendsetter in the high-tech industry who has founded several successful companies including AirDefense, CipherTrust, CoreHarbor, Air2Web and SecureIT. Jay’s 25 years of sales, marketing and engineering experience also includes leadership roles at leading companies such as IBM, NCR and Unisys.

Jay is considered an industry thought-leader in cyber-security and has been honored for his entrepreneurial leadership and management success by numerous organizations. He received E&Y’s Entrepreneur of the Year award in 2004 for South East USA. Catalyst, South East’s entrepreneurship magazine, named Jay among the Top 50 Entrepreneurs several years in a row. He is the founding president of TiE Atlanta Chapter and has been on the Board of Trustees of TiE Global.

In 2002, he launched AirDefense which pioneered the wireless security market and was the market share leader, with over 35% of the Fortune 100 as its clients. It had a successful merger with Motorola in 2008. Jay founded CipherTrust in 2000, creating the industry’s first email gateway security appliance and led its successful merger with Secure Computing. In 2000, he founded CoreHarbor, the first ASP for e-procurement solutions, which was acquired by USi/AT&T. In 1999, he launched Air2Web, a provider of mobile internet applications for enterprises, which connects more than 500 carriers in 200 countries.

In 1997 Jay founded SecureIT, the first pure-play internet security services company, which experienced exponential revenue growth. As a self-funded company, SecureIT was acquired by VeriSign in July 1998, where he served as Vice President and General Manager of the Security Services Division.

Between 1995 and 1997, Jay served as Senior Vice President of Worldwide Marketing at IQ Software, a public company that specializes in database reporting tools. Previously, he was the Vice President of Sales and Marketing for the Software Products Division at Unisys. Prior to that, Jay was Director of Marketing for NCR handling Latin America, Middle East and Africa division. He has also held various sales positions at IBM.

Jay holds a Masters in Computer Engineering, Masters in Industrial Engineering, and Masters in Business Administration from The University of Cincinnati. He has attended executive management programs at Harvard Business School, Wharton Business School and IBM.