What does the Cloud mean to Enterprise Security?

PREPARING YOUR COMPANY FOR MOBILE,
SOCIAL, AND CLOUD SECURITY

Table of Contents

Overview

The world of enterprise security has been undergoing a complete transformation as a result of rapid and sweeping changes that are remaking the way companies do business. New technologies and trends are changing the very definition of an enterprise, how and where we work, and the tools we use to do our jobs. The Everywhere Enterprise is not some future vision, it's today's reality for thousands of enterprises with operations that span the globe.

These technology trends include:

Mobility. The explosion of new mobile devices is changing the way we work, and dissolving the traditional corporate network perimeter in the process. Whether you embrace a "bring your own device" (BYOD) strategy today, or are standardizing on corporate-owned devices, mobility is a game-changing technology that affects every aspect of your business. CISOs are increasingly being asked to protect what they no longer own or control. Employees are working from home on laptops, connecting to corporate networks on public WiFi networks as they travel, and sending emails and texts across 3G and 4G networks on smartphones and tablets. In fact, an employee could be in the office, sitting at their desk, and accessing corporate resources on a personally owned device leveraging a 3G/4G network. This is a world where security appliances are blind.

Cloud Applications are transforming the economics of traditional enterprise software. Not only do today's employees expect to be able to use the devices they want to use, they expect to be able to purchase and use the applications they need directly from the Internet, without going through a centralized IT function. Whether it's a department head licensing a cloud-based marketing automation system, an employee storing files on Dropbox, or a contractor using a web application like Basecamp, the mentality of the empowered consumer is permeating the enterprise. As with the mobile example above, employees expect to be able to use these technologies to increase their productivity and innovate, and CISOs are being challenged to encourage these trends while protecting the company from the new dangers and exposure they bring.

Social Media has rapidly evolved from a consumer-only fascination to a business-critical enterprise application. Enterprises are increasingly unable to block access to social networks due to employee demand, but more importantly, they don't want to – social networks can be great business drivers. Marketing departments use Twitter, YouTube and Facebook to reach customers, partners and industry influencers. Sales organizations are finding sites like LinkedIn invaluable for prospecting and lead generation, and customer service centers are recognizing that customers are asking questions and looking for immediate answers on social sites and in private communities.

Security Threats Have Evolved

It should come as no surprise that cybercriminals are leveraging these technology trends in their attacks against corporations. Security threats have evolved from desktop-based viruses to browser-based threats, phishing attacks, and botnets. Mobility has made it even easier to breach corporate security measures, as employees increasingly access corporate assets over unprotected WiFi and cellular networks. As shown in the diagram below, in a post-PC world, these threats require a new approach to security, one that provides consistent policy, protection and visibility regardless of the user's device or location. This kind of protection cannot be achieved with traditional appliance-based security. A new approach is needed.

Consider three locations of users.



	OFFICE	COFFEE SHOP	AIRPORT
Device	PC	Laptop	Tablet/smartphone
Protection	IDS, IPS, FW, SWG, DLP etc.	Host based AV and firewall	none
Visibility	Location based reporting	none	none

We must seek security solutions that ensure consistent policy, protection and visibility, regardless of device or location. Cloud provides the opportunity to level the playing field.

Today, the Perimeter is Gone

In the mobile, Everywhere Enterprise, there is no longer a set perimeter. Business happens everywhere, on mobile devices and 3G/4G networks, in coffee shops and airports on public WiFi networks, and increasingly, even on airplanes. Users are going direct to Cloud, bypassing corporate gateway proxies and firewalls to access cloud and mobile apps, upload and download data, and send text messages and emails. Mobile devices are outnumbering PCs in the enterprise, and VPNs do not secure 3G/4G mobile traffic.

Given the growing abundance of user-owned devices with always-on network connectivity, we must shift enterprise security from a mentality of 'block vs allow' to 'manage and monitor'. Simply prohibiting access to Internet resources will simply encourage users to bypass enterprise controls, and they will succeed.

The truth is that the security vendors scrambling to update their software with patches to keep up with the latest malware or botnet attack are missing the point, leaving huge gaps in security that leave your users and your corporate data exposed, and put your company at risk.

Why Your Appliance Based Security is Failing You

Although the advantages and ROI of cloud solutions has been well-documented, if your IT organization has been less than enthusiastic about the move to the cloud, you are not alone. Research shows that one of the primary reasons enterprises are hesitating to embrace cloud computing is due to security concerns. In fact, in a recent survey by LinkedIn, 54% of respondents cited Security as their top concern for transitioning to the cloud.

Their concerns are real. That's because the traditional appliance-based security products designed for yesterday's corporate network security are woefully unequipped for the challenges. 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:

TRADITIONAL DEFENCES	HOW TRENDS ARE BREAKING THIS	IMPACT ON THE ENTERPRISE
Antivirus/IDS signature updates	High rate of new and mutating malware	Singular-based security defenses are perpetually outdated, increasing risk of infection
Fixed perimeter security controls	Business demands and mobility create an enterprise "information perimeter" that differs from a network perimeter	Perimeter security cannot protect sensitive data as it moves to new locations
Network layer security	Diverse locations all use single web protocol	Traditional network security can no longer distinguish between and protect enterprise applications or enforce user access policies.
Inbound security	Simpler for criminals to lure users to malicious websites rather than penetrating inbound defense	Users infect their own enterprise by virtue of their web surfing habits, criminals have botnets that include virtually every enterprise connected to the internet
Endpoint control	Network access by consultants and contractors, smart phone adoption, business unit PC procurement	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
Operational security management	More time required to manage above defenses via patching, signature updates, rule changes	Security department must devote more resources to operational security, less time solving business problems

Today's sophisticated hackers understand this new world of enterprise IT, and are exploiting the gaps left by legacy security appliances with increasingly sophisticated, frequent and evolving threats. They are increasingly targeting mobile users, and using mobile devices as a beachhead to attack corporate environments. They are exploiting the trend toward employees going Direct to Cloud to access cloud applications, use mobile apps, and surf on public WiFi networks.

The gaps within traditional network security appliances described above are 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 technology and business shifts;
- They impede innovation, creating friction within the business.

Specifically, the limitations of the appliance-based model include:

Location Dependent: 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.

Performance Issues: The location dependence of appliances 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 simply go without corporate security protection.

Appliance overload: Appliances tend to be built for one security function only, creating an explosion of new appliances in the data center to keep up with each new threat, all of which must be individually purchased, installed, maintained and updated.

Spiraling Costs: Appliances require significant costs for acquisition, installation, regular patching, log file management, access control, and integration among several other costs. IT organizations simply cannot keep pace with the demand to update appliance signature files, resulting in inevitable security gaps.

Capacity Limitations: Appliances do not provide on-demand capacity, forcing IT organizations to "over-architect" a solution. For example, an appliance may be designed for 100, 500, or 2000 users. If you have exactly 2000 users, you either must spend more money to purchase excess capacity or purchase an insufficient solution that hinders business growth.

Single tenant: Appliances are designed for a single organization, not for the notion of multi-tenant configurations, limiting their usefulness with today's collaborative networks of contractors, partners, supply chains and vendors.

The simple fact is that today's security appliances simply can't meet the needs of today's rapidly changing, global, mobile, fluid enterprise. The solution to scaling your business securely is not to purchase ever more hardware and software, and hope that the gaps in your security strategy go undetected.

What does all this mean to enterprise security?

"In 2012, 80% of new commercial enterprise apps will be deployed on cloud platforms."

- IDC

"At year-end 2016, more than 50% of Global 1000 companies will have stored customer-sensitive data in the public cloud"

- GARTNER

The Case for Cloud

The same economic efficiencies and competitive advantages driving the shift to cloud computing and SaaS applications are now driving a similar transformation in the landscape of enterprise security. Of course, the idea that cloud computing can transform a market is not new. Companies like Salesforce.com, Workday, Rackspace and NetSuite have already proven that the cloud can disrupt a market, making companies that use these applications more competitive, efficient, and innovative, while dramatically lowering costs.

Over the last ten years, the move to the cloud has gained momentum and continues to accelerate, with more and more traditional bastions of on-premise enterprise hardware and software infrastructure giving way in favor of the economies of scale, superior functionality and sheer convenience that cloud computing provides.

In 2012, Salesforce.com passed SAP as the lead vendor in the worldwide customer relationship management (CRM) software market (Gartner).

Companies are less and less likely to build vast datacenters to store their corporate information and host their applications and web sites, instead relying on cloud alternatives like Rackspace or Amazon. Web applications like Gmail and Microsoft 365 are gaining ground in the enterprise over more traditional office applications.

As cloud applications have become more trusted and more prevalent, these economies of scale have become too compelling to ignore, and ties to legacy on-premise hardware and software are increasingly viewed as a competitive disadvantage. Why pay for all those capital investments and the resources to manage them, when you could redeploy those dollars and resources to more strategic projects? Whereas appliance-based security products require enterprises to make purchases based on anticipated demand, cloud-based security allows enterprises to scale purchases up and down based on their actual consumption.

However, cost savings is not the only reason companies are moving data and applications to the cloud. Increasingly, CIOs are thinking of cloud computing in terms of flexibility, agility and competitive advantage:

In the same way, the cloud offers not only dramatic economies of scale, but a significant leap forward in advanced security capabilities that simply can't be achieved using traditional, appliance-based security.

"The reason to go to cloud is no longer price but being able to move fast — deploy, re-deploy, and un-deploy workloads as needed without having to buy servers and software that could become shelfware next week or next month "

- GIGAOM

The Next Generation of Security: Direct-to-Cloud Network

Securing business in the cloud requires an entirely new approach to enterprise security, one that is built from the ground up to address the new realities of the mobile, social, Everywhere Enterprise. It requires solutions that allow CIOs and CISOs to regain control and visibility into all of the enterprise's digital assets and user activity, whether located internally or externally on the Internet. Visibility is a key factor, equally if not more important than the notion of traditional security. In today's complex IT environments, the ability to see clearly every user, device, and application accessing your corporate network is no longer a "nice to have," it's a business imperative.

The next generation of enterprise security will be about much more than blocking threats. Although threat detection will continue to be critical, the next generation of security will also serve as a business driver and competitive advantage for companies looking to embrace innovation, be more agile and flexible, and outmaneuver their competition, without being held back by outdated capital and operating cost structures that must be planned and invested years in advance.

Zscaler calls this approach the Direct-to-Cloud Network.

Fuel New Business Initiatives

Today's CIOs are being challenged to shift their focus from basic infrastructure projects to strategic initiatives that drive business value with transformational practices. Moving security to the cloud is just such a transformational practice that can increase business agility and generate ROI. This approach frees up the CIO's and CISO's resources to think more strategically about how security capabilities can enable the business, and use funds formerly allocated to security infrastructure to fuel those initiatives.

Accelerate Innovation

New technologies and processes can deliver enormous gains in productivity, efficiency that drive real business metrics like revenue generation and customer satisfaction. However, the proliferation of new mobile and cloud technologies has shifted the center of gravity toward the user, leaving security professionals struggling to keep up. Moving security to the cloud shifts the balance of power back in favor of the CIO and CISO, allowing your company to embrace innovation securely, while providing the visibility and controls needed to ensure compliance with corporate policies.

Increase Competitiveness

The ability to innovate, and adopt new technologies and processes that accelerate innovation, is what separates market winners from their followers, and allows new competitors to challenge established players. Moving your security infrastructure to the cloud makes your company more nimble, allowing you to quickly adapt not only to evolving threats, but to changes in the market that threaten slower competitors.

When is a Cloud not Really a Cloud?

There are many products and vendors on the market claiming to be "cloud" security solutions. With each vendor claiming their solution solves all issues, it can quickly become confusing separating reality from the hype.

To be clear:

MSSPs: Provide 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 Appliances: The 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.

Key Requirements of a Direct-to-Cloud Network

A Direct-to-Cloud Network is very different from other security architectures. The two key attributes that characterize a Direct-to-Cloud Network should be:

1. **Elasticity:** The enterprise is charged based on actual consumption of the service, as opposed to anticipated demand.
2. **Multi-tenancy:** This is how economies of scale are achieved – every CPU cycle is utilized, allowing for a competitively priced service to be delivered

In contrast with the above approaches, a true Direct-to-Cloud Network is built from the ground up to be resilient, redundant and high-performing. Instead of building perimeters around people, devices or organizations, it provides a dynamic perimeter that moves with the user.

This means no matter where a user is, they should be able to access the Internet locally, but only after going through a gateway that ensures that good traffic is allowed, and bad or malicious traffic is kept out. Creating a dynamic perimeter is not measured in the ability to standup five, ten or even 20 gateways, but rather a 100 or more local access points around the world. This requires a global cloud infrastructure built from the ground up to ensure that no matter where you are, you have a local, fast, secure, and policy based connection to the Internet.

From an architectural point of view, a true Direct-to-Cloud Network will have the following key elements:

1. **Device Agnostic:** The Direct-to-Cloud Network should be independent of the network gear, employee devices and operating systems used in your enterprise. As long as you send your traffic through the Direct-to-Cloud Ne work, your users should be protected and your security should "just work".

2. **No Hardware, No Software:** There should be no investment in infrastructure required to host or run your security solution. That means no hardware, no software, no operating system, and no agents.

3. **Location Independent:** A global service is useful only if any user can use any data center any time. Your security solution should need no pre-knowledge of where your users may show up in order to provide security, it should follow the user wherever they go.

4. **Gap-free**: No compromises. It's not enough to maintain a list of blacklisted sites, or deliver software patches every few weeks. The only way to protect users is to scan every byte traffic that comes in and goes out of your organization, and match it against millions of signature, behavior patterns and heuristics in real time.

5. **Multi-tenant:** True multi-tenancy, an architecture where each user is treated with individual policy. So regardless of where the HQ is, they can travel anywhere, be on any device and yet get their company's policy locally.

6. **Inline:** You can no longer trust that a site is clean by reputation alone. Inline security that sits between the user and the Internet is the only way to verify that content is clean and users are secure.

7. **SSL Aware:** Most online communications today are SSL encrypted. Any viable security solution must be able to scan SSL content inline to verify that the content does not contain security threats. While many security appliances claim to do this, they either only inspect content "headers," and not the full content, or they introduce unacceptable latency to the user experience.

8. **Granular**: 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.

9. **Real-time:** The Direct-to-Cloud Network should update the protection capabilities and policy changes for every user and business location in real-time.

10. **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 Direct to Cloud service must deliver. Robust and comprehensive logging should be available to provide CIOs and CISOs with regulatory, forensics and management accountability.

11. **Single Sign On/ID Federation**: Enterprises will not be able to live without. Too many applications to manage without it.

12. **Detailed Visibility:** Detailed logs are critical to finding malicious behavior and forensics. Your Direct to Cloud service should always be able to collect logs, correlate them across the world, sequence them and present them to your administrator in real-time. Logs should never be written to disk (even encrypted) outside the jurisdiction of choice. If a Swiss company wants logs in Switzerland. We must be able to do that no matter where their employees are.

13. **Continuous Trust:** For every transaction, make sure nothing changed, and dynamically verify the identify of the user. Change your authentication level and assign a risk level based on the new information. Block the botnet call home and change user access permission.

14. **Behavioral Analysis – detecting zero day threats.** Being able to detect virus signatures is not enough, you need to be able to analyze the behavior of a transaction and detect when it behaves differently than expected in order to protect against completely unknown threats.

15. **Layered Security – There is no silver bullet when it comes to security**. A layered approach must be taken whereby all network traffic is assessed from multiple angles, leveraging various techniques to ensure that threats are not missed.

16. **Big Analytics:** Lastly, you need powerful analytics and reporting that is extremely versatile. This is essential for organizations with strict privacy and other legal reporting requirements. For example, you need the ability to determine which web sites John Smith visited on Jan 5th at 3pm. How long would it take for you to do that with your current architecture ?

Summary

The forces of mobility, cloud apps and social media are challenging traditional notions of enterprise network security. In the new world, business is dynamic, users are mobile, and protecting your network perimeter is only the beginning. The Direct-to-Cloud Network is the next generation of IT security that provides the economies of scale, advanced security and elasticity required to remain competitive in today's mobile, social world.

A true Direct to Cloud architecture enables large global organizations to leverage a whole new way of securing its users, devices and data that can scale and adapt to the needs of their business for the next ten years. 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. We believe that CISOs should evaluate a move to the cloud now, both to prepare their organization for today's rapidly evolving security challenges, and to prepare for the company's future adoption of cloud computing. To find out more about how you can begin to transition to a Direct to Cloud strategy, contact Zscaler today.

To learn more about Zscaler's Direct-to-Cloud Network, contact Zscaler today for a personalized demonstration, or sign up for one of our on-demand webinars.

CONTACT US

Zscaler, Inc.
110 Baytech Drive, Suite 100
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/groups/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com