WHITE PAPER

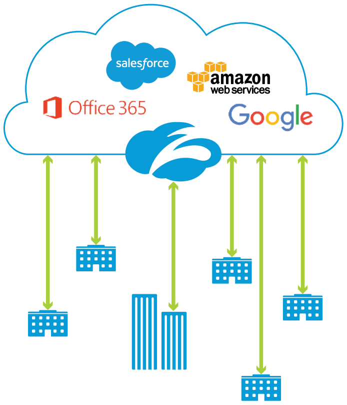
What does the cloud mean to enterprise security?

Preparing government and education for mobile, social, and cloud security

OVERVIEW

Enterprise security has undergone a complete transformation as a result of rapid and sweeping changes that are remaking the way public sector organizations 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. These trends include:

Mobility and the use of mobile devices have changed the way we work, and have all but dissolved the traditional enterprise network perimeter in the process. Because of BYOD, CISOs are increasingly being asked to protect what they no longer own or control. Increasingly employees are working remotely on laptops, connecting to enterprise networks using public Wi-Fi, 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 a desk with a PC connected to the enterprise network, and be accessing enterprise resources on a personally owned device leveraging a 3G/4G network. This is the reality in today's world, and it's a world to which traditional security appliances are blind.



Cloud applications, such as Office 365, Salesforce, and Workday have introduced enterprises to the collaboration and productivity benefits enabled by the cloud. But these applications have also created challenges for the traditional hub-and-spoke network model, as they place far greater demands on nework resources. In addition, the cloud-based app market makes applications available to consumers direct from the Internet, so users are downloading them in high numbers without going through IT. Whether it's a department head licensing a cloud-based CRM 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. CISOs are being challenged to encourage these trends while protecting the organization from the potential risks and exposure they introduce.

Social media has rapidly evolved from a consumer-only fascination to business-critical enterprise applications. In addition to the well established use of Twitter, YouTube, LinkedIn, and Facebook for communication and collaboration purposes, an increasing number of enterprised-based collaboration tools in the social media style have been introduced with resounding success, such as Yammer and Slack.

SECURITY THREATS HAVE EVOLVED

It should come as no surprise that cybercriminals are leveraging these technology trends in their attacks against agencies and municipalities. Security threats have evolved from desktop-based viruses to browser-based threats, phishing attacks, and botnets. Mobility has made it even easier to breach enterprise security measures, as employees increasingly access organizational assets over unprotected Wi-Fi and cellular networks. These threats require a new approach to security, one that provides consistent policy, protection, and visibility, regardless of the user's device or location.

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.

> “Cloud delivery of an integrated security platform provides big opportunities for CISOs to reduce latency and costs, while at the same time improving their security posture.”
>
> *– Forrester Research*
>
> FORRESTER®

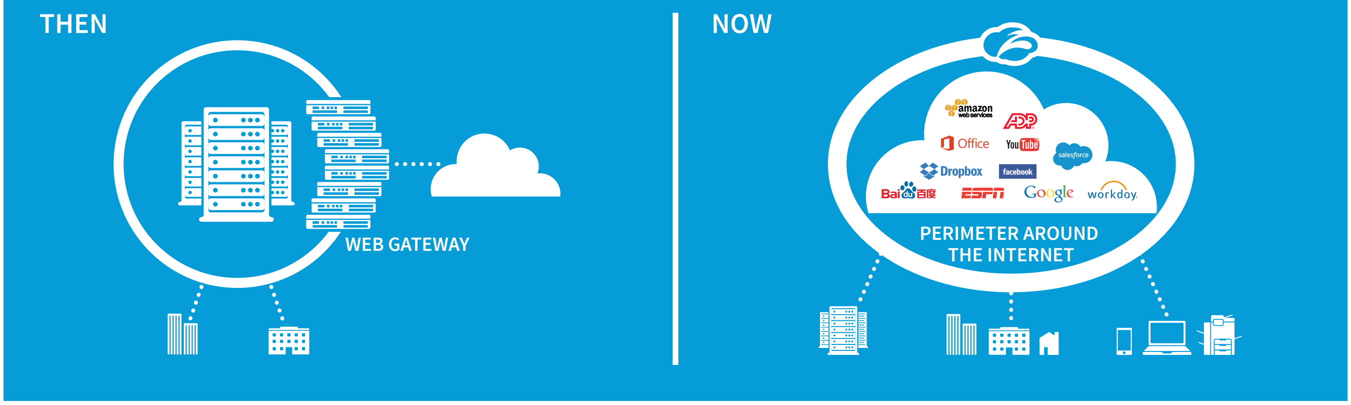
The perimeter is gone

In the mobile 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 Wi-Fi networks, and increasingly, on airplanes. Users are going direct to cloud, bypassing enterprise 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.” Prohibiting access to Internet resources opens you up to the risk that users will simply bypass enterprise controls.

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 expose your users, your data, and your organization to risk.

In the old days, you protected servers in the data center. But now, you must protect people, cloud applications, and a range of internet-connected devices.



Why appliance-based security is failing you

Although the advantages and ROI offered by cloud solutions have 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 have been hesitant to embrace cloud computing is due to security concerns.

Their concerns are well founded, based on the security measures they have in place. That's because the traditional appliance-based security products designed for enterprise network security are woefully ill-equipped to protect users and resources in the cloud. Many of the problems with traditional security defenses are revealed by examining our current dependency upon security appliances as a core part of our architecture:

TRADITIONAL **DEFENSES**	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 enterprise environments. They are exploiting the trend toward employees going direct to the Internet and using public Wi-Fi networks to access cloud and mobile apps and to send and receive email.

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 enterprise 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 2,000 users. You're frequently in the position of overspending in order to purchase excess capacity, or purchasing an insufficient solution that hinders business growth.

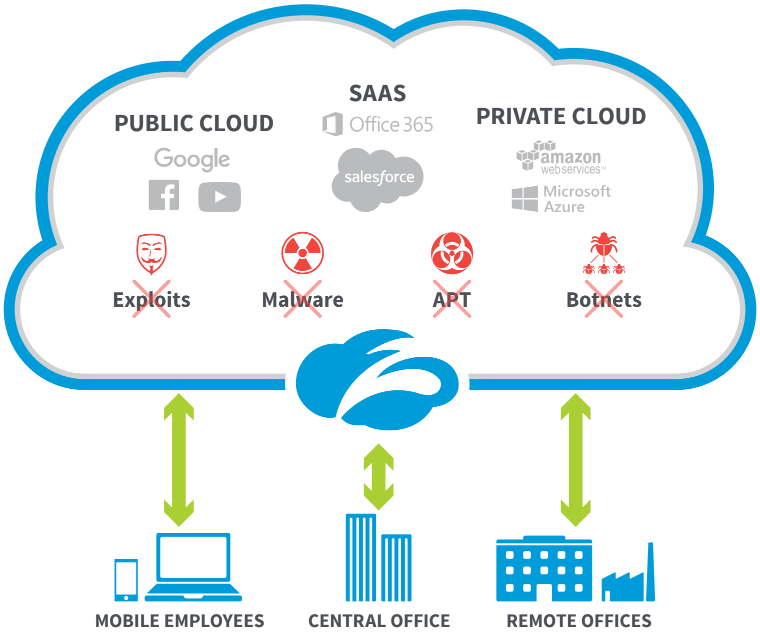
Single tenant: Appliances are designed for a single organization, not for the notion of multi-tenant configurations, limiting their usefulness with today's collaborative networks of contractors, partners, supply chains, and vendors.

Security appliances simply can't meet the needs of today's agile, global, mobile enterprise. The way forward for 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?

THE CASE FOR CLOUD

The same economic efficiencies and business imperatives driving the shift to cloud computing and SaaS applications are now driving a similar transformation in enterprise security. Of course, the idea that cloud computing can transform a market is not new. Office 365, Salesforce, Workday, and others have proven that the cloud can disrupt a market, making organizations that use these applications more agile, efficient, and innovative, while dramatically lowering costs.



Over the last 10 years, the move to the cloud has gained momentum and continues to accelerate, with the bastions of on-premises enterprise hardware and software giving way to cloud computing's economies of scale, superior functionality, and sheer convenience. Public sector is shifting away from building vast data centers to store information and host applications and websites, instead relying on cloud alternatives like AWS or Azure.

As cloud applications have become more trusted and more prevalent, cloud economies of scale have become too compelling to ignore, and ties to legacy on-premises hardware and software are increasingly viewed as a barrier to achieving business objectives. 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 public sector organizations are moving data and applications to the cloud. Increasingly, CIOs are thinking of cloud computing in terms of flexibility, agility and the ability to deliver improved citizen services.

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 next generation of security

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, and 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 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 for organizations looking to embrace innovation, be more agile and flexible, and enable enhanced citizen services, without being held back by outdated capital and operating cost structures that must be planned and invested years in advance.

THE ZSCALER™ CLOUD: SECURE, SIMPLIFY, AND TRANSFORM YOUR ENTERPRISE

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 mission, and use funds formerly allocated to security infrastructure to fuel those initiatives.

FULL INLINE CONTENT INSPECTION

All bytes, all ports, all protocols, including SSL — no compromises.

REAL-TIME THREAT CORRELATION

Correlation of risk indicators — destination to content — to predict and block zero-day attacks.

UNIFORM SECURITY FOR EVERYONE

CLOUD INTELLIGENCE

Over 100M+ threats blocked every day — once a new threat is detected, it's immediately blocked for all users. 175K+ security updates a day.

40+ INDUSTRY THREAT FEEDS

Threat sharing partnerships, commercial deals, open source, private working groups.

Microsoft PhishTank Google CYBER THREAT ALLIANCE

Accelerate innovation

New technologies and processes can deliver enormous gains in productivity and 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 organization to embrace innovation securely, while providing the visibility and controls needed to ensure compliance with organizational policies.

Increase responsiveness

The ability to innovate, adopting new technologies and processes that accelerate innovation, is imperative for public sector organizations under pressure to do more with less. Moving your security infrastructure to the cloud makes your organization more nimble, allowing you to quickly adapt not only to evolving threats, but to changing stakeholder requirements.

When is a cloud not really a cloud?

There are many products and vendors in 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: A managed security service provider offers outsourced management of on-premises equipment. Essentially, they allow an organization to shift labor costs to a service provider, while retaining the appliances and 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.

Hybrid security: Many appliance vendors now have a "cloud" offering to complement their box sales. But these solutions offer none of the benefits of a true cloud solution, like the intelligence, economies of scale, and performance that are only possible with a multi-tenant cloud architecture.

In a hybrid solution, your security appliances are essentially co-located in the cloud, so they can provide services to your branch offices without backhauling traffic. But, if you have performance issues or you've detected points of failure in your on-premises appliances, they won't go away with a hybrid approach. And your mobile users remain unprotected.

Key requirements of true cloud network

A cloud is very different from other security architectures. The two key attributes that characterize a pure-cloud solutions include:

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 cloud solution 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 users go, 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, 10, or even 20 gateways, but rather 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.

> “ It's one of those few products that actually does what it says on the tin. Zscaler was born in the cloud. It lives in the cloud. Therefore, it's much easier for them to maintain and grow their service. ”
>
> – ***Tony Rimmer,*** *Chief Security Officer, Fugro*

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 pure-cloud security platform is the next generation of IT security that provides the economies of scale, advanced security, and elasticity required to achieve your mission objectives in today's mobile, social world.

A true cloud architecture enables organizations to leverage a whole new way of securing their users, devices, and data that can scale and adapt to the needs of their organization for the next 10 years. While cloud security is a key strategy, 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 organization's future adoption of cloud computing. To find out more about how you can begin to transition to a cloud enabled-enabled enterprise, contact Zscaler today.

To learn more, contact us for a personalized demonstration, or sign up for a live, online demo or one of our on-demand webinars at **www.zscaler.com**.

ABOUT ZSCALER

By 2008, Zscaler founders could see that business was transforming, moving away from the corporate network and into the cloud. Believing that the only way to deliver security for the cloud would be in the cloud, we set out to build a global, multi-tenant platform with comprehensive, integrated security services and access controls to protect organizations from cyberattacks and prevent data loss. Today, Zscaler operates a massive, globally distributed cloud security platform, helping thousands of leading organizations make the secure transformation to the cloud. Learn more at **www.zscaler.com**.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

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