

## OVERVIEW

Enterprises are struggling with the consumerization of IT. With the proliferation of mobile devices like iPads and iPhones within the enterprise, IT administrators can no longer ignore these devices as outside their scope of responsibility. Smartphones and tablets are now as powerful as laptops. Employees can access corporate data and the Internet through wireless networks such as Wi-Fi hotspots or cellular 3G/4G that are not controlled by IT.

*“By 2013, mobile phones will overtake PCs as the most common Web access device worldwide.”*

- Gartner, 2010

With many corporate applications being hosted in the cloud, the risk is even higher. Ensuring the security of corporate data is no longer a matter of deploying adequate measures within the organization. It is imperative that security and policy travel with the employee wherever they are and whatever type of device they use.

Unlike the PC world that is dominated by a few main operating systems, the number of platforms and device form-factors for mobile devices is much higher, as is their churn rate. IT needs a solution that is easy to deploy, supports multiple mobile platforms and provides consistent user policy enforcement across PCs and mobile devices.

## MOBILE DEVICE SECURITY CHALLENGES

There are two primary challenges that affect IT organizations as the proliferation and adoption of mobile devices increases with enterprises.

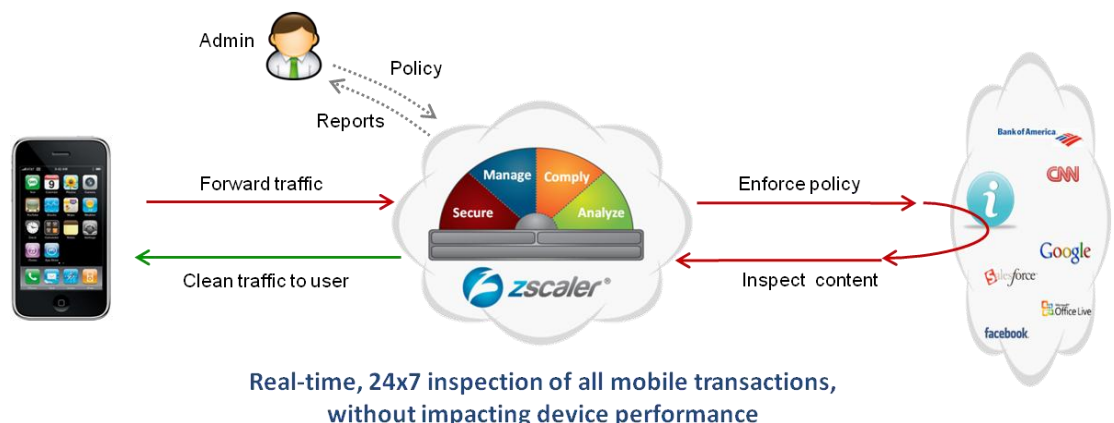
The first challenge is that the line between enterprise and personal usage is getting blurred on mobile devices. These devices run the gamut of applications, from Facebook, YouTube, Pandora, to enterprise apps like email and salesforce automation. Since the enterprise typically does not own the device, enforcing policies for acceptable usage or installing application controls like a traditional IT administrator would on a corporate PC is often not viable. There is an increased risk of exposing corporate data on mobile devices since they roam and connect to multiple Wi-Fi and cellular 3G/4G networks. Traditionally, web security protections have been enforced either by way of a gateway web proxy at an enterprise's egress to the Internet or via signature-based anti-virus protections installed on the user PC. With mobile devices, there is no obvious point of enforcement like an enterprise proxy. To complicate matters further, enterprise data is rapidly migrating to the cloud. As a result, an employee's mobile web transactions may never hit the enterprise network while accessing critical cloud-hosted data.

The second challenge is that security apps for mobile devices are expensive to develop and often ineffective. Unlike the PC world, which is dominated by Microsoft, there are several different mobile operating systems – Apple iOS, Android, Windows Mobile, Blackberry, Symbian, etc. Each platform has its own software development environment and a security vendor developing mobile security apps will have to replicate the effort across various platforms. Further, some platforms such as Apple iOS do not allow traditional anti-virus apps on their platform. Loading third party apps, not approved by the platform vendor may lead to violation of contract and often requires “jailbreaking” the device – definitely not an enterprise option. Even if security apps are allowed, they are a headache to deploy, require constant updates, and are easy to circumvent – the user can simply uninstall them if they dislike it. Worst of all, they impact device performance and degrade user experience by stretching the already limited processor and memory resources on the mobile device.



## ZSCALER MOBILE OVERVIEW

Zscaler Mobile adds a uniform way to secure mobile devices for small to large organizations. In tandem with Zscaler’s existing Web and Email cloud security services, Zscaler Mobile enforces the same policy for users wherever they go, across all their mobile devices. The new solution ensures protection for leading smartphones and tablets including iPhone and iPads. Over a billion web transactions from customers ranging from G2000 enterprises to governments to SMBs are secured by Zscaler daily. Zscaler Mobile leverages this proven infrastructure to extend protection to mobile devices.



Zscaler Mobile enforces policy in the cloud, not on the device. This means all network content is scanned, both browser and app generated web traffic, to ensure that malicious content is blocked in the cloud – long before it reaches the mobile device, or the corporate network.

*“I can instantly get access to web activity for all my employees and road warriors from a single, easy to use portal”*

- Security Director  
Financial Services Company

Zscaler Mobile provides two options to forward traffic to the Zscaler Cloud for security and policy enforcement. Users can forward traffic using a secure VPN tunnel or set an HTTP(S) proxy on the mobile device. In both of these scenarios, the administrator configures the device with the appropriate VPN or proxy server setting. Platforms such as Apple have enterprise configuration tools that facilitate the creation of mobile configuration files that can be signed and encrypted for secure delivery to the mobile device via the web or email for over-the-air configuration. Note that no new application needs to be installed on the user’s device.

With Zscaler’s global footprint, the solution provides users a seamless Internet experience as users’ traffic is tunneled to a data center locally within the region they are visiting. Centralized policy management and reporting enables administrators to enforce policy regardless of which network or device the employee may use.

Zscaler provides user-based policy across security, access management and data loss prevention. Enterprise administrators define the policy once and it is applied consistently regardless of the employee’s location or device. Zscaler’s Nanolog technology enables globally aggregated reporting, providing administrators accurate Internet activity report on any user, on any device, anywhere in the world and at any time.

## ZSCALER MOBILE BENEFITS

**Uniform policy for users** - Zscaler allows IT administrator to define a uniform policy for any user and have it seamlessly enforced regardless of the device the user is connecting with. Administrators no longer have to deal with multiple point products to secure PCs, smartphones and tablets.

**Global footprint for near-zero latency** – With over 40 strategically located data centers worldwide, Zscaler minimizes latency associated with inspecting traffic in the cloud.

**No extra software to install on mobile device** – Unlike other mobile security vendors that require platform-specific apps to be installed on every device, Zscaler Mobile works seamlessly across mobile platforms, including iPhones, iPads, and Android devices.

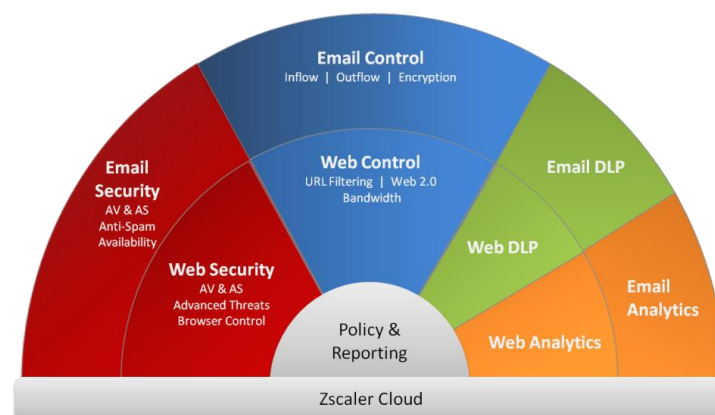
**Up-to-date 24x7 mobile security** – Zscaler Mobile requires no signature updates and provides real-time inspection in the cloud for every web transaction, regardless of whether it came from a browser or from an app installed on the device.

**No degradation of device performance** – Zscaler Mobile runs in the cloud and has no impact on device performance, battery life, or processing resources.

**Centralized reporting and administration** – Zscaler provides real-time logs and reports for any user, from any location, on any device, at any time.

## ZSCALER CLOUD SERVICES OVERVIEW

Zscaler offers four cloud-based subscription services that help customers secure and manage every aspect of their employees' internet usage.



*“In my 30 years of IT, I have never seen such a powerful technology that is so simple to deploy”*

- CTO  
Global 2000 Company

Web and email have become the preferred channels of communication for businesses. Organizations are able to effectively secure their users against today's dynamic email and web threats with Zscaler's services. Browser control and dynamic inspection of content is necessary to protect against more complex threats.

Maintaining control over mail flow and access to web resources is critical. Zscaler offers the ability

to granularly control access to websites and applications as mandated by corporate policy.

Users may accidentally or maliciously leak sensitive corporate data using a number of methods including email, webmail, social networks, blogs, or instant messaging. Zscaler can prevent organizations from incurring liabilities due to data loss by scanning all outbound traffic against predefined engines.

Traditional log consolidation from multiple locations and correlation of data is cumbersome. Zscaler's centralized policy and reporting simplifies administration and reduces IT operational costs for organizations.

Traditional security vendors will tell you that they have embraced the cloud, but look deeper. Building and running a cloud is complicated. Zscaler is the largest company in the world focused solely on cloud security. Our R&D centers span three continents, our cloud operates at four 9s availability and our cloud specific patents stand at 30 and growing. Join the companies from 140 countries, who have thrown away their hardware and software, and moved to the Zscaler Cloud. **Security made simple!**

***"It's truly real-time reporting. I can see any web transaction from anywhere in the world, within three seconds."***

- IT Director  
Global 2000 Company

## MORE INFORMATION

### USA & Canada

+1-408-533-0288  
usc-info@zscaler.com

### Latin America

+52-1811-2551670  
latam-info@zscaler.com

### Middle East & Africa

+33-1-4561-3272  
mea-info@zscaler.com

### Japan

+81-3-6206-8535  
jp-info@zscaler.com

### Northern Europe

+44 (0)7799 038043  
neur-info@zscaler.com

### Central Europe

+49-89-954499820  
ceur-info@zscaler.com

### Southern Europe

+33-1-4561-3272  
seur-info@zscaler.com

### Eastern Europe

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

### South East Asia

+65-9796-5851  
sea-info@zscaler.com

### Australia & New Zealand

+613-9653-9088  
anz-info@zscaler.com

### India

+91-80-26672127  
india-info@zscaler.com

### Greater China

+65-9796-5851  
china-info@zscaler.com

*Zscaler®, and the Zscaler Logo are trademarks of Zscaler, Inc. in the United States. All other trademarks, trade names or service marks used or mentioned herein belong to their respective owners.*