

## Seven Reasons to Embrace Cloud Security

### ABSTRACT

Cloud computing is rapidly transforming the enterprise IT landscape. Enterprise applications, infrastructure and platforms are steadily migrating into the cloud and are being offered by several vendors as a service. Traditional IT capital expenditure and system maintenance is giving way to services that can be turned on or off on demand, can scale elastically with evolving business needs, and are priced based on a subscription model. Enterprise security, particularly web and email security, is rapidly being adopted as a cloud based service. This white paper describes seven key benefits of cloud based security and outlines salient requirements that enterprises should focus on when considering a cloud security solution.

Why Should You Embrace Cloud Security? .....	3
1. Mobility: Cloud Can Protect Multiple Devices Across Different Networks .....	3
2. Gap Free Security: Cloud is Pervasive and Up-To-Date on Security Threats .....	4
3. Distributed Enterprise: Cloud Protects Branch Offices and Road Warriors .....	4
4. Agile Deployment: Cloud Provides Quick Rollout and Zero Maintenance .....	5
5. Reliability: Cloud is Inherently Resilient with No Single Point of Failure .....	6
6. Elasticity: Cloud Can Secure a Few Users Today and a Few Million Tomorrow .....	6
7. Lower Cost: Cloud Based Security Lowers TCO Substantially .....	7
Selecting the Right Cloud Security Vendor .....	8
Conclusions .....	9

## Why Should You Embrace Cloud Security?

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing is rapidly changing several enterprise IT paradigms. Software-as-a-service, delivered through the cloud, has already reduced the cost and simplified deployment for applications such as customer relationship management (e.g. salesforce.com) and email (e.g. gmail.com). Infrastructure-as-a-service has reduced the capital expenditure and maintenance overhead for enterprises on servers, allowing them to spin up computing and storage resources on demand (e.g. Amazon Web Services). The agility, reliability, scalability and cost benefits of cloud computing are being realized for enterprise security applications as well. According to Gartner, secure web gateways and email security are good candidates for delivery through a cloud based infrastructure<sup>1</sup>. The following sections outline seven key benefits of cloud based security for enterprises.

### 1. Mobility: Cloud Can Protect Multiple Devices Across Different Networks

The adoption of smartphones and tablets by consumers and enterprises is happening at a staggering rate. In the fourth quarter of 2010, smartphones out-shipped PCs for the very first time. According to [Morgan Stanley](#), the worldwide annual shipment of smartphones will exceed that of desktops and laptops combined by 2012. Analyst firm [Gartner](#) estimates that by 2013, mobile phones will overtake PCs as the most common web access device worldwide. The combined installed base of smartphones and browser-equipped phones will exceed 1.82 billion units, and will be greater than the installed base for PCs thereafter.

Employees are frequently bringing their own smartphones and tablets to work. 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 want to access corporate data and the Internet through wireless networks such as Wi-Fi hotspots or cellular 3G/4G networks that are not controlled by IT.

The line between enterprise and personal usage is getting blurred on mobile devices. These devices run the gamut of applications, from Facebook, YouTube and Pandora, to enterprise applications like email and CRM. Since the enterprise typically does not own the device, enforcing policies for acceptable usage or installing application controls as 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

“Web gateway SaaS provides opportunities to protect roaming devices, such as mobile devices and laptops that typically are not protected by on-premises gateways without heavy clients.”

Gartner, April 2011

networks. Traditionally, web security protections have been enforced either by way of a gateway web proxy at an enterprise’s Internet egress point, or via signature-based antivirus software installed on the user’s PC. With mobile devices, there is no obvious point of enforcement like an enterprise proxy. Additionally, on mobile devices where CPU cycles and battery life are at a premium, background processes, such as antivirus, are less than desirable; and due to more tightly controlled operating systems, antivirus apps are often not an option at all. To complicate matters further, enterprise data is rapidly migrating to the cloud. As a result, an employee’s mobile web transactions may never cross the enterprise network when accessing critical cloud-hosted data.

Cloud based web security allows IT administrators to define a consistent policy for any user and have that policy seamlessly enforced, regardless of the device with which the user is connecting, or the user’s location. Administrators no longer have to deal with multiple point products to secure PCs, smartphones and tablets. Unlike traditional mobile security solutions that require platform-specific apps to be installed on every device, a cloud

---

<sup>1</sup> *Moving E-Mail and Web Security to the Cloud*, Peter Firstbrook, Gartner, April 2011

based solution works seamlessly across a variety of mobile platforms, including iPhones, iPads, and Android devices.

## 2. Gap Free Security: Cloud is Pervasive and Up-To-Date on Security Threats

Traditional enterprise security is delivered as a host based and/or network based solution. In the host based security model, endpoint agents are installed on the users' PCs. The endpoint agent may provide antivirus and malware protection, firewall capabilities, IDS/IPS functionality, etc. The agent itself needs constant updates in the form of new threat signatures to keep up with evolving vulnerabilities. In a large organization, updates are managed by IT and there is a delicate balance between stability and security: too frequent updates may reduce employee productivity and increase support calls, too few updates may result in security gaps arising from outdated threat signatures. Network based security is typically delivered through an appliance – a dedicated piece of hardware running custom security software designed to provide features such as firewall, IDS/IPS, web proxy, etc. As with endpoint agents, threat signatures as well as the appliance software have to be kept up-to-date in order to provide protection against constantly evolving threats.

The traditional enterprise security model is reactive and often entails significant latency between the time a security event is discovered and when protection is made available for users. As new vulnerabilities are discovered, patches and signature updates are created and a cumbersome process of distributing and updating individual user machines and enterprise appliances follows. This results in significant gaps in security coverage.

Cloud based security eliminates the gap between threat discovery and protection being available. Unlike the appliance and endpoint models, there is only one instance of the product – the cloud. Enterprises leverage the multi-tenant cloud to get security delivered as a service.

Since the cloud sees traffic from a variety of sources, it has real-time and granular visibility of new security outbreaks. As new vulnerabilities are discovered, a single update to the cloud offers instant protection to *all* users seamlessly. If one user uncovers a new vulnerability, all others are instantly protected against it.

*“Cloud-based providers should have better real-time telemetry of global events and the ability to respond to these events rapidly by modifying the solution.”*

**Gartner, April 2011**

This real-time updating is a paradigm shift in the security delivery model, and perhaps the best way to see the difference is to consider the following analogy: Imagine a town that does not have a municipal water supply. All its citizens have private wells that they use to extract their water. If there was contamination in the ground water supply, the information will first have to be disseminated by town authorities, individual households will have to buy some recommended filtration system for their private wells; many of them may run into compatibility issues given the differences in well and pump design. This situation is very similar to what happens when individual enterprises have their private security appliances and endpoint agents. Now imagine the same town with a municipal water supply. Households buy water as a service. If there was any contamination, the appropriate filters and containment would be deployed centrally and clean water would be instantly available to all households. The municipal water system guarantees clean water and is able to provide the service cost-effectively at the necessary scale.

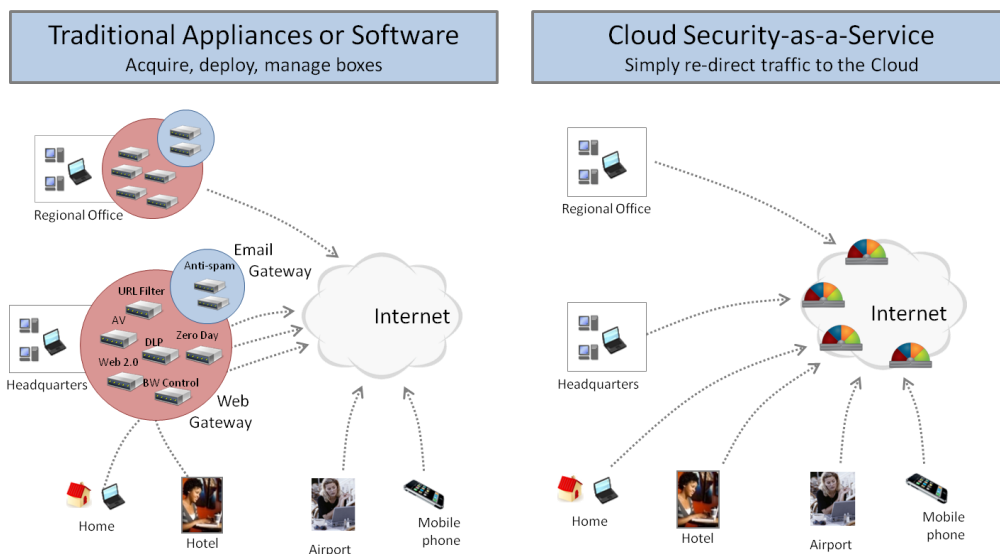
## 3. Distributed Enterprise: Cloud Protects Branch Offices and Road Warriors

Enterprises today are getting more and more decentralized, with office locations across the world and an increased acceptance of telecommuting. In fact, according to [Nemertes Research](#), 91 percent of employees in most organizations work in locations outside of traditional headquarters. This decentralized enterprise increases challenges for IT when it comes to managing appliances in lots of different locations. In the appliance based security model, a “box” is typically deployed at each office location. As the number of offices increase, more boxes need to be deployed and managed. The appliance management problem gets compounded at smaller branch offices which may not have IT resources on-site. Add telecommuters that work from home offices, and the appliance based model quickly becomes untenable. As such, enterprises frequently force users to VPN to

headquarter locations to leverage on-premise security appliances. This leads to unnecessary traffic backhaul with increased bandwidth cost for the organization and added latency for users. Further, as users adopt mobile devices that go straight to the Internet, appliances that enforce security and policy compliance are often circumvented completely.

A cloud based offering eliminates these problems. Traffic from headquarters, branch offices, home offices and mobile devices is redirected to the cloud. Security and policy is enforced by local nodes in the cloud, avoiding expensive backhaul and minimizing service latency. User based policies are defined by the administrator once; they then get enforced across the cloud – regardless of user’s location or access device, as illustrated in Figure 1.

Web and email security solutions are prime candidates for a cloud based security offering. Internet and email have become the preferred channels of communication for businesses. Maintaining control over mail flow and access to web resources is critical. Cloud based security offers the ability to granularly control access to websites and Internet based applications as mandated by corporate policy.



**Figure 1: Cloud simplifies deployment and protects the distributed enterprise**

#### 4. Agile Deployment: Cloud Provides Quick Rollout and Zero Maintenance

Appliance and endpoint security products frequently come with deployment headaches. Appliances need to be shipped to various locations, configured appropriately, installed and tested. Endpoint security agents need to be installed on user machines. A large rollout can take several months, and often requires complex project

management and lots of resources working in tandem.

“[Security-as-a-service solutions] are faster to implement and easier to maintain. Full cloud-based SaaS solutions benefit from eliminating the maintenance of the hardware and data center rack space, power and cooling. They also benefit from eliminating the need to maintain the solution software, such as upgrading to the latest version, backing up configuration files and, in the case of software-based solutions, maintaining and securing the underlying operating system.”

Gartner, April 2011

Just as cloud based software-as-a-service offerings have eliminated the need for on-premise software deployment and maintenance, cloud based security-as-a-service can eliminate the need for on-premise hardware and software. Eliminating additional hardware automatically cuts down any rack-space, power, cooling and asset management requirements. Deploying complex endpoint agents is a headache most enterprise IT professionals would gladly avoid if possible. So what exactly needs to be done for a cloud based security rollout?

Let's take a look at a cloud based web security. Enterprise IT needs to configure their edge routers to redirect traffic to the cloud. Traffic redirection is accomplished using a variety of techniques – GRE tunnels, VPN, proxy chaining, port forwarding, etc. These are typically simple configuration changes on routers and firewalls. If user-based policies are desired, the enterprise needs to sync their Active Directory with the cloud based solution. Road warriors connecting to the Internet from third party networks will need local proxy settings. Typically this is centrally provisioned with features such as Group Policy. Similarly, smartphones and tablets are centrally provisioned using Mobile Device Management (MDM) solutions. Note that no new software needs to be deployed on these mobile devices and PCs; only a configuration push is needed to redirect traffic to the cloud.

## 5. Reliability: Cloud is Inherently Resilient with No Single Point of Failure

If you were to power your home with a local generator, the chances of being out of power would be much higher than if you bought power from a reliable grid. The generator might malfunction or run out of gasoline. Sure, you can have redundant generators, but that will significantly increase upfront cost and require additional maintenance. The electrical power grid, in contrast, has much higher resiliency, balancing electrical supply and demand at a massive scale. Even if one power plant is out of commission, the grid sustains itself. As such, there isn't a single point of failure. Yes, entire grids do fail, but that happens very infrequently.

In a similar fashion, cloud based security is significantly more resilient than an on-premise appliance. An enterprise buys SaaS with SLAs around uptime, latency, protection coverage, etc. A well-designed cloud security solution ensures that every component in the infrastructure is designed for fault-tolerance. Cloud vendors simply cannot afford service downtime because of a single component failure. The lateral scale of cloud based security provides significant redundancy if a few nodes or data centers go offline. A properly designed solution will distribute processing across hundreds of nodes deployed in redundant data centers across the globe. If a few nodes are down, traffic processing is automatically redistributed across the active nodes. All this is completely transparent to the end user. In the power grid analogy, the user simply gets reliable electricity, oblivious of the power plant it came from – the grid abstracts those details. System health monitoring, upgrades, fault management are all done centrally by the vendor. Economies of scale provide a highly reliable security service to the enterprise at a fraction of the cost it would take to implement it on-premise.

## 6. Elasticity: Cloud Can Secure a Few Users Today and a Few Million Tomorrow

As a business scales, IT requirements and cost rise in proportion. Referring to the power grid analogy again, if you have a 2 kW generator today and tomorrow your power requirement goes to 10 kW, you will have to invest in a bigger generator. Security appliances work in the same fashion. It is hard to balance future requirements and immediate cost. Most enterprise IT professionals plan for some headroom when they invest in security appliances. If they need to protect 100 users today, they may invest in an appliance that is capable of processing 250 users. As the business grows, they may have to re-invest in bigger appliances without having fully depreciated the cost of the original purchase.

Much like the power grid, cloud based security solutions offer enormous elasticity and scalability on demand. The pay-as-you-go model is perfect for businesses that do not want to be forced into an upfront capital expenditure based on anticipated future requirements. Enterprises also go through Mergers & Acquisitions (M&A). Entities locked into different appliance vendors often create integration challenges for IT post M&A. On the contrary, cloud based security is a service that can be switched on or off as needed and can scale overnight as business requirements change. The deployment agility and elasticity offered by the cloud is perfect in today's IT environment, when budgets are being slashed and operational expenses are preferred over heavy upfront capital expenditure.

*"SaaS costs are also more aligned with business metrics, such as number of employees and business strategy, and growth by acquisition or divestiture. Costs are based on a per-seat, per-feature basis. SaaS solutions are also capable of growing or shrinking with business demands."*

**Gartner, April 2011**

## 7. Lower Cost: Cloud Based Security Lowers TCO Substantially

In addition to all the benefits outlined above, cloud based security significantly reduces the Total Cost of Ownership (TCO) for enterprise security. Security appliances incur both Capital Expense (CapEx) and Operation Expense (OpEx). CapEx components include equipment procurement costs, deployment cost, personnel training costs, etc. OpEx costs include annual maintenance charged by the appliance vendor, IT administration cost, etc. On the contrary, cloud based solutions virtually eliminate CapEx and lower the normalized OpEx per user with economies of scale.

Figure 2 illustrates a TCO comparison between cloud based security and comparable appliance based solutions. As

“SaaS secure Web and e-mail gateways frequently provide efficiency and cost advantages, and a growing number of offerings are delivering an improved level of security that exceeds what most organizations can achieve with on-premises software or appliances.”

Gartner, April 2011

security threats become more complex, protection costs rise. Appliances are typically dedicated to a particular security feature. If an enterprise wants to protect its users on the web, filter email spam and implement a Data Loss Prevention (DLP) system, they would have to deploy three separate appliance based solutions. There is significant CapEx involved and OpEx scales as IT resources need to be trained to manage, maintain and correlate alerts from separate appliances. Well-designed cloud based

solutions offer consolidated security – enterprises can enable features on-demand. There is no upfront CapEx for new security features. Opex is reduced thanks to an integrated management console and the elimination of box maintenance. Overall, web security TCO can be reduced 60% with cloud based as compared to appliance based solutions.

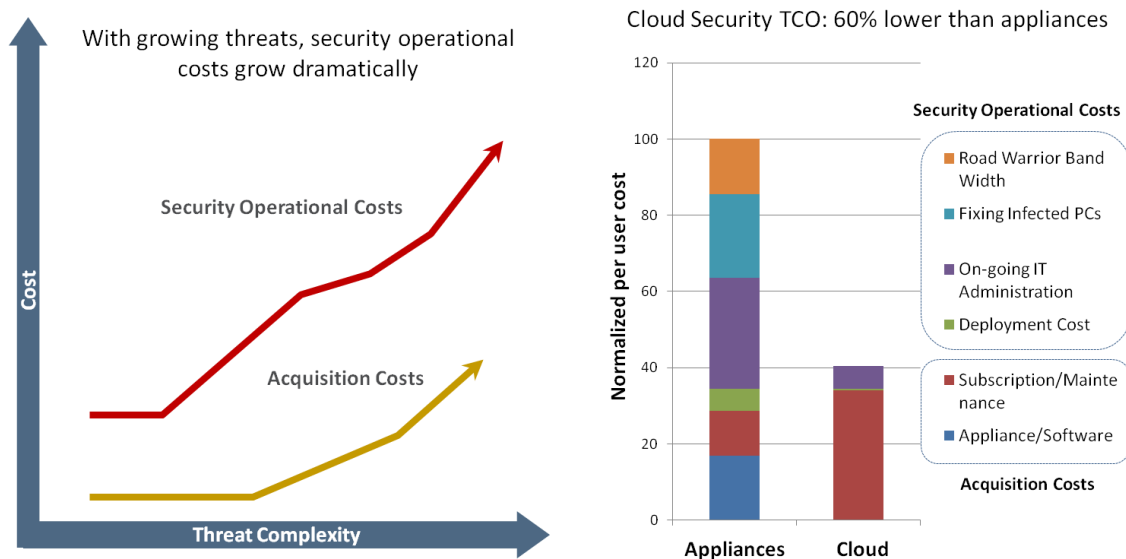


Figure 2: Cloud based solution reduces web security TCO and enables a simple subscription model



## Selecting the Right Cloud Security Vendor

All cloud based security solutions are not created equal. The benefits of cloud based security are quickly lost if the vendor's architecture has limitations. Figure 3 summarizes key criteria that enterprises should consider when evaluating a cloud based solution, focusing on web and email security.

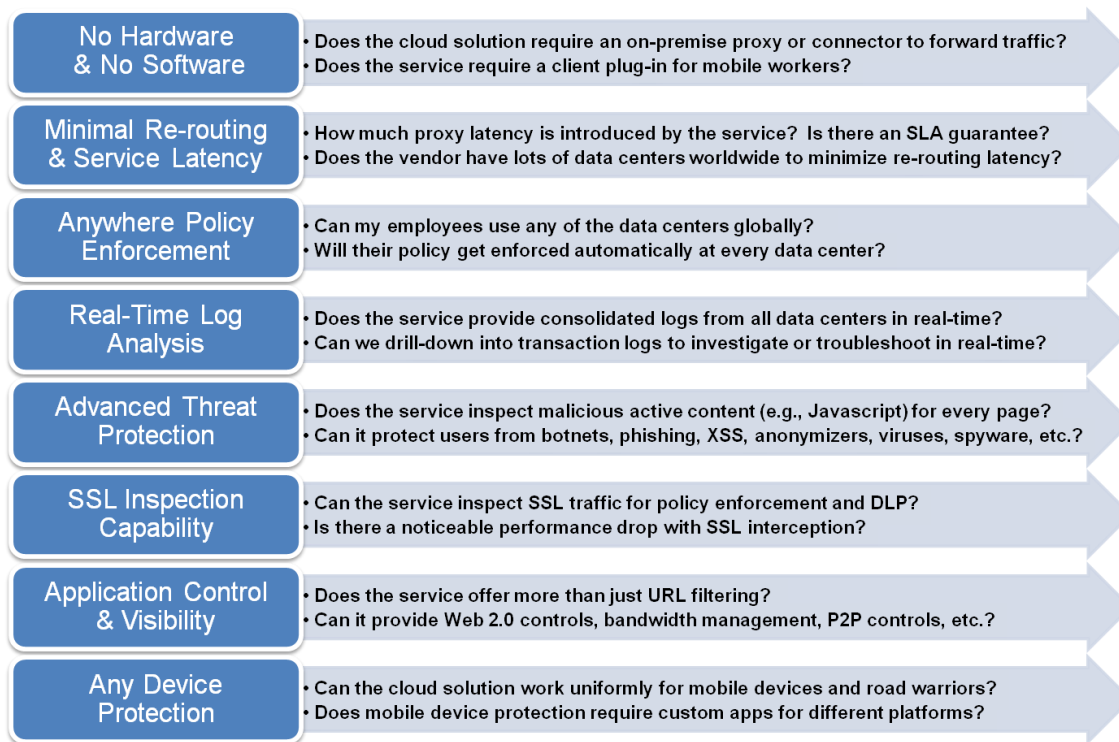


Figure 3: Salient criteria for selecting the right web and email cloud based security service



## Conclusions

Cloud computing has already transformed the enterprise application and infrastructure paradigm by delivering them as a subscription based service. On-premise equipment, major capital expenditure and large IT maintenance costs are giving way to nimbly deployed services that can be enabled and scaled on demand. This transition is allowing businesses to focus on their customers and solutions and not on managing IT appliances or software. Cloud computing benefits are now rapidly being realized for enterprise IT security as well. Integrated web and email security, delivered as a service through a cloud based offering, is quickly replacing on-premise proxy servers, URL filters, web malware appliances, anti-spam appliances, data loss prevention appliances, etc. The pervasive nature of the cloud is perfect for distributed enterprises and the mobile workforce – they need not be tethered to “boxes” while getting gap free protection and full policy compliance. Cloud based security is facilitating fast and agile deployments with little or no follow-on maintenance for enterprise IT. The cloud is inherently resilient with no single point of failure. The elasticity of the cloud allows enterprises to future-proof their security requirements without having to invest upfront in over-provisioned appliances. By eliminating the need for any hardware or additional software, upfront capital expenditure is negligible for cloud based security. Cloud based solutions can provide enterprises with superior web and email protection at a 60% lower overall cost and simultaneously eliminate all the hassles of managing their own equipment.