IDC VENDOR SPOTLIGHT

Securing Cloud and Mobile While Keeping Employees Happy

January 2014

Adapted from *Worldwide Security 2013 Top 10 Predictions* by Christian A. Christiansen, John Grady, Phil Hochmuth, et al., IDC #239424 and *2013 U.S. Cloud Security Survey* by Phil Hochmuth, Christina Richmond, Sally Hudson, et al., IDC #242836

Sponsored by Bitglass

Cloud computing challenges traditional notions of IT and information security. Sensitive IT assets — applications, databases, and data storage — traditionally operate behind corporate firewalls or within secure, dedicated hosting environments. However, the economics of cloud computing is pushing more organizations to deploy sensitive IT assets into external, untrusted IT environments or even partially trusted environments. While the cost savings and efficiencies of cloud are great, moving sensitive workloads outside the firewall can raise confusing regulatory and compliance situations and potentially leave sensitive information and assets exposed to misuse or theft.

This Vendor Spotlight explores the balance organizations must strike between maintaining information security and ensuring employee privacy, and it discusses the role that Bitglass plays in the growing market for new security solutions.

Introduction

Today, IT professionals want to be viewed as enablers. This means meeting the demands of employees and the business, without sacrificing data security.

Software as a service (SaaS) and bring your own device (BYOD) represent two major transformations in enterprise IT:

- SaaS: Advantages over on-premise software include flexibility and cost savings.
- BYOD: Advantages include productivity, where employees can get work done from anywhere, anytime.

SaaS applications store sensitive enterprise data outside the enterprise, adding security and compliance risks when compared with on-premise software deployments. With BYOD, enterprises potentially lose control of corporate data that is stored on personal mobile devices. Both SaaS and BYOD offer significant benefits but introduce information security challenges to the enterprise. With employees using cloud applications and their own mobile devices, corporate data has the potential to move outside the corporate environment, and IT loses visibility and control over that data.

Existing technologies don't meet these needs because users and their devices, as well as any associated applications and data, are outside the protection of most enterprise IT infrastructures. Because the monitoring capabilities of IT are limited in these environments, audits can become more difficult. The potential for loss of corporate data (and the potential for a public breach notification) increases as well. Weak access control can increase the vulnerability of the devices and the corporate applications that are connected via those devices.

Given the shift of power and influence in recent years in favor of employees and line-of-business managers, the fix for these issues must balance the needs of the employee with the needs of IT. In situations when IT is slow to respond or provides antiquated technologies for employee productivity, employees often respond by sourcing their own technology, which makes data security even more challenging.

IT Needs

Visibility and control. IT needs to know who is doing what inside of corporate SaaS applications in the form of actionable reporting and audit capabilities. Contextual access controls should allow the enterprise to decide who accesses what and under what conditions. IT needs to know what happens with sensitive corporate data after it has left the cloud and has been downloaded to employee devices. What data left, how sensitive is it, and who downloaded it are among the questions IT must answer. Visibility is also a strong deterrent to unauthorized dissemination of sensitive corporate data.

Security and compliance. Employees don't want to give up control of their personal device to the organization. IT needs to secure the data on BYOD devices without installing software agents on each and every device. In the cloud, security and compliance of data at rest are the two primary drivers for cloud encryption. In terms of security, the risk of breach and data theft or loss is top of mind for organizations in all industries. As for compliance, certain verticals require data to be encrypted on the public Internet. A cloud encryption solution must use an internationally approved and thoroughly vetted encryption algorithm, such as AES-256, with bulk encryption. In a SaaS environment, an encryption solution must support virtualized storage with key management controlled by the customer and/or the SaaS provider. In certain countries, careful attention must be paid to the physical location of files relative to local privacy regulations.

Ease of deployment. IT needs a solution that operates in the network rather than at the endpoints and does not require a team of network administrators to roll out. Solutions that operate in the network are easier to deploy and manage than solutions that are installed on devices. For example, a forward proxy solution that requires settings on every firewall and mobile device to forward the traffic is expensive to deploy and manage. In comparison, a reverse proxy solution can accelerate the response to information requests without requiring an endpoint client. Reverse proxies do not require multiple points of integration and are supported from any device the moment it is turned on.

Furthermore, IT needs a solution that interoperates with existing infrastructure such as firewalls, directories, and single sign-on systems.

Employee/User Needs

Mobility. Users want to be able to access corporate data from any device, anywhere. In BYOD environments where the user owns the device, device-level security access solutions such as VPNs and/or custom network settings can increase IT administration. Users may not be familiar with how to install a VPN, create a key, and operate the VPN, which can generate costly help desk calls. Corporate and personal traffic is backhauled through corporate networks. This means that large amounts of personal traffic (e.g., video, music, email, social networks) can burden corporate networks.

Productivity. Logging on to a VPN can delay access to corporate resources or slow down access to performance-sensitive SaaS applications, thereby inhibiting employee productivity. Some public networks block VPN traffic. This can generate help desk calls as well. Other business functions and applications may also be complicated by client-side security controls.

Privacy. When users own the device, they do not want the inconvenience of turning corporate security on or off depending on personal use. Moreover, they do not want the corporate logging of personal information. In some countries, this inadvertent corporate logging may also violate local privacy laws.

Transparency. Users need to have the same native experience with each application. For example, users want to use the native email applications on their mobile phone, while a mobile device management (MDM) solution might require a separate corporate email client. Security solutions that slow down or alter the user experience are invasive and lower productivity.

In addition, users want privacy in their personal communications. Employees are suspicious of security solutions that transport, handle, or inspect their private, personal activity. An example would be a forward proxy solution that routes and monitors all traffic bound for google.com because the corporation uses Google Apps. In doing so, the forward proxy would also inspect employees' personal communications on Gmail or searches on Google. Employees have the right to privacy.

Shoehorning Existing Technologies to Fit the Cloud/Mobile Need

Current solutions are often draconian and mitigate mobile's focus on innovation and increased productivity. For example, cloud applications use proxy-based security application to enforce the policy. This reduces the utility of mobile devices by slowing down application access and requiring potentially cumbersome access procedures (VPNs) that may not work with certain Web-based applications. Likewise, MDM and MAM (mobile applications management) may require customized applications because MDM/MAM may not work with standard SaaS and other Web applications. MAM and MDM may require both client-side and server-side adjustments. This adds significant complexity to IT management and further inconveniences users.

Sometimes, business units and certain departments will circumvent IT's restrictions by creating their own mobile solutions in conjunction with SaaS implementations that are outside IT's purview. These "rogue SaaS implementations" can cause severe problems with data protection, customer privacy, regulatory compliance, and audit failures.

IDC talked to one customer that did an audit of its in-house SaaS applications. The customer expected to find roughly 30 instances, but it was very startled to discover over 300 SaaS applications in use, including unauthorized customer relationship management (CRM), collaborative software (e.g., Evernote), and shared cloud storage (e.g., Dropbox). Interestingly enough, IT talked to the "rogue" business unit and realized that these applications were often critical to corporate innovation and productivity. Rather than prohibit the rogue SaaS implementations, IT recognized its role as a service organization and embraced the enemy. IT worked with the business unit to bring many of the applications into corporate compliance without substantially affecting the user experience or the value of the applications.

Benefits of New Technologies

Because MDM/MAM solutions may require custom browsers and rewritten applications, bringing rogue SaaS applications into compliance can be difficult. With improved visibility and auditability, organizations can reduce the risks associated with data loss and strengthen access control. In addition, new technologies enable organizations to adopt cloud apps previously prohibited because of security concerns and allow IT to better meet the needs of the business.

Corporations can ease deployment of security policies on rogue SaaS implementations with cloud-based:

- Tunnel termination
- Inspection/pattern matching
- File buffering/caching
- Watermarking of sensitive files and information

As a result, management overhead is reduced because of the elimination of client-side components.

Market Trends

In terms of mobility, everyone likes to use their own tools. They already know how the tools work, and they can easily switch from one task to another. Therefore, it is not surprising that employees are starting to use the same devices and applications in both their personal lives and their professional lives. The ability for employees to bring the latest mobile technology into the workplace is a huge productivity boost. Moreover, there are other benefits. Corporate capex is reduced because capital budget spending on mobile devices is reduced. Opex is reduced because users self-support in many cases. Given all these factors, it is not surprising that IDC research shows that more than 62% of organizations are BYOD environments.

However, there are drawbacks. Employees might inadvertently (or intentionally) share sensitive data outside the corporate environment. The corporate network security perimeter that was carefully designed and fortified over the years is now rendered porous by BYOD mobile devices.

Cloud is also an important trend affecting IT. Enterprises are increasingly migrating to cloud-based SaaS applications to achieve cost and management savings. SaaS applications are better suited to a mobile workforce because they can be accessed from anywhere without the need for a VPN.

But, SaaS applications pose significant security challenges:

- SaaS data sits on servers outside the corporate network, creating security vulnerability for many corporations.
- IT has little visibility into how users access SaaS.

"Rogue cloud" is rampant. According to IDC, 72% of organizations saw at least one incident of unauthorized use of cloud computing services over the past 12 months; among these firms, more than half said they created a workaround with the individual or group to allow continued use of the technology. As mentioned previously, IT organizations succeed when they embrace BYOD and SaaS and help secure rogue implementations so that businesses can adapt to changing external market conditions rather than being forced to adapt to unprofitable internal IT practices.

Considering Bitglass

Bitglass was founded in 2013 by a team of industry veterans with a proven track record of innovation and execution. Bitglass has attracted investment from tier 1 venture capital firms Norwest Venture Partners and NEA via a $10 million Series A investment in February 2013. Bitglass is based in Campbell, California.

The Bitglass product includes the following capabilities:

- SaaS reverse proxy for data and control traffic that secures cloud and mobile, without capturing employee personal data.

Cloud Data Protection

- Clientless selective wipe and restore of mobile data (no software agent), allowing an organization to manage its data, not the user's device
- Persistent data tracking for documents on the Internet
- Mobile DLP — automatically remove sensitive data before download

Unified Identity and Contextual Access Control

- Role-based provisioning and access
- Native single sign-on or via integration with cloud identity products
- Automatic user provisioning
- Mobile auto-enrollment
- Contextual access control by device, geography, time of day

Analytics and Visibility

- Deep visibility into application usage and alerts on suspicious activities across all networks
- Detailed transaction logging
- Fine-grained location tracking
- Search by keyword, user, application, and more
- Rapid deployment — even large organizations can deploy in minutes

For cloud data protection, Bitglass transparently secures corporate data anywhere in the cloud and on mobile devices. In addition, Bitglass provides identity and access control via contextual access control and enterprise identity integration. Seamless deployment is supported via auto-redirect, auto-enrollment, and auto-discovery that enable users to access business applications directly, yet traffic is diverted through the system.

Challenges

When devices are lost or stolen, many IT organizations will still need a unified solution across heterogeneous devices that can remotely lock or wipe a mobile device. For data protection on the device, tracking functions are valuable, but internal or external policies may require encryption of all data on the device. Of course, if IT encrypts all data on the device and holds the cryptographic keys, users stand to lose all their personal data and applications when the device is lost or stolen or when they leave the company.

Conclusion

Increasingly, users (especially senior executives that originally drove BYOD) don't want to give IT the right to wipe all apps and data off their personal devices at any time for any reason. IDC predicts that CISOs will arrive at a BYOD security policy that strikes a balance between user freedom and protection of corporate assets.
