CloudLock

Whitepaper

Building the Human Firewall

Rethinking information security for the cloud

At a Glance

Intended audience:

• C-level security, compliance, and trust professionals at companies using or considering public cloud platforms such as Google Apps, Salesforce, Dropbox, or Box

• Compliance and privacy officers at organizations responsible for ensuring adherence to established regulations such as PCI-DSS, SOX, and HIPAA

Takeaway:

• Readers will learn why security is not achieved via a gateway solution, but instead, how a cohesive discovery, classification, and governance framework which reflects risk as it actually plays out is the most effective way to approach the design of an information security and compliance strategy

Introduction

One of the truths about the security industry is that it is inherently reactive; as threat and risk evolve and change, the concepts that drive organizational and regulatory policy adjust to reflect those risks. If one looks back to the end of the twentieth century, for example, the primary threat to an organization came in the form of external threat: an outsider who hacked or socially engineering their way into a network, a physical breach where an attacked planted a rogue device somewhere within the building, or a criminal who physically accessed and compromised hardware and software from within the company server room.

Accordingly, much of what was available from the security market was focused on these threats: firewalls and devices that monitored packets, biometric devices designed to secure access to sensitive equipment, and anti-virus tools that were capable of finding compromised software and reporting it back to the IT team before significant data loss could occur.

From Device-Centric to Data-Centric

As we enter the second decade of the twenty-first century, however, the nature of risk has changed. Organizations are increasingly moving their data into the cloud, and away from on-premise systems; the rise of services such as Google Apps and Salesforce has been astronomical -- the latter being on track to reach over $7 billion (USD) in revenue by the end of 2014.

The incredible speed of this change has left the security and response industry reeling. Major vendors are struggling to realign their product and service offerings to meet the needs of a paradigm that is no longer focused on on-premise data management. As multiple industries are drawing down their IT teams and getting away from hosted server management, new risks are arising and being left unanswered.

What this has resulted in is a net increase in data exposure. Ironically, the problems that the industry faced a decade or more ago are largely being resolved. Where once data loss was primarily a factor of unpatched servers, insecure facilities, and computer viruses, the cloud providers who manage the enormous data centers have consolidated their infrastructure and implemented management systems that ensure that these types of vulnerabilities are rare if not impossible to find and exploit.

However, this has led to a degree of complacence around risk in general, as the underlying lessons learned during the early years of network security are seemingly forgotten in lieu of single-source solutions that allow for technical compliance with externally owned regulations, rather than effective and practical security that addresses the ways in which data are exfiltrated from the modern cloud-based network. Two models exist for responding this risk: API-driven solutions integrated at the cloud platform provider, and gateway solutions that attempt to interdict data prior to it reaching the cloud.

The Rise of New Risks

In examining how data breach risk has changed, consider the significant incidents that were made public in 2013:

January	Security firm Mandiant reports on the APT1 group, detailing the size and impact of an unprecedented cyber-attack on US companies and government facilities
February	A major breach of the United States Federal Reserve is publicized and attributed to the Anonymous hacktivist group, resulting in the loss of sensitive credentials, personally identifiable information (PII), and bank information
March	Evernote, the popular note taking application, reports that a coordinated attempt to access secure areas of its service occurred, with nearly 50 million usernames, email addresses, and supposedly encrypted passwords being potentially accessed
April	Popular consumer service Living Social announces that more than 50 million accounts were potentially compromised
May	Content management system Drupal reveals that its users credentials, countries, email addresses, and passwords were lost in a data breach, via a malicious third-party application
October	Adobe announces that its services were breached, and more than 38 million customer accounts had their data compromised, along with the source code for Photoshop
December	Retail giant Target announces that an attack on their point-of-sale credit card swipe machines resulted in the loss of more than 40 million credit and debit card records, and more than 70 million customer records containing personally identifiable information were lost
December	Neiman Marcus reveals that thousands of its customer's payment card records were compromised between July and August of 2013

What is evident is that there is a cross-industry issue with security; breaches targeting sensitive payment card information (PCI), personally identifiable information (PII), and intellectual property (IP) are increasing, and the measures taken even by large and thoughtful organizations are failing to keep pace with the reality "on the ground".

Problematic Strategies

The gap between the investments being made by organizations and the security they actually need is largely driven predicated on weak access to accurate data. In a 2013 survey sent to more than 500 organizations, CloudLock found that 66% of respondents' employees admitted to installing unsanctioned and unmonitored third party applications from within their environments. Nearly half said they were sharing files, including those containing potentially regulated or sensitive data, between their personal and professional cloud accounts. Nearly a quarter said they went so far as to share their login credentials with other employees for the sake of convenience.

What this points to is that the practical gaps in security for these organizations cannot be managed through offline or gateway technology alone; negligence around data stewardship happens in the cloud itself, where end-users make decisions around data access and use in realtime, and where security needs to sit in parallel to those behaviors. As the lines between professional and personal computing blur, the well-intentioned insider becomes increasingly more of a vector for data loss than any hacker or criminal, at least on the independent actor level. The easiest way to compromise the integrity of an organization's information security perimeter is by way of the people who already have access to the data and who hold credentials that can be used to modify or share it.

In a 2013 study, the Ponemon Institute notes that of those organizations storing data in the cloud, more than half of the respondents indicated some mechanism of data encryption was in use for the information that they were transferring to the cloud. An increasingly wider market for cloud encryption vendors has arisen in response, with various promises of regulatory compliance and security as a result of employing encryption technologies as the primary mechanism for enforcing security within a cloud platform.

While the case for encryption is strong, it is largely based on an outsider threat model; the statistics around where risk comes from suggest that while part of a coherent cloud security strategy, encryption on its own is now sufficient.

Solve for What Matters

What the CloudLock study also shows is that employees are exfiltrating data and compromising security after data was passed through point-of-access solutions, including cloud encryption.

Consequently, there are two responses open to the security-conscious IT team: a draconian crackdown, where new restrictions on what and how company information can be accessed will be implemented, or a holistic approach that seeks to engage users and treat them as partners in the security discussion.

Real World Implications

In tracking the efficacy of these different security models, CloudLock considered an organization that was utilizing Salesforce for customer and company data in the cloud. They had acquired the platform to both reduce IT cost and to increase their sales and account management teams' efficiency, and had implemented encryption within the Salesforce instance, designed to ensure that no external actor could gain access to the sensitive and regulated data which formed a core aspect of their business.

With a legacy of highly secure on-premise servers, this particular company believed that its universal use of AES-256 on all data that was considered sensitive would ensure the safety of their data.

What they had not realized, however, was that the business objectives around the use of Salesforce and the security team's goal in applying universal encryption were at odds, and the former would take precedence. An audit revealed that departmental-level managers, seeking to increase operational efficiency through the use of various third party platform plugins and applications, were creating and sharing supposedly secure sandbox environments with outside vendors as part of their regular RFP processes. In doing so, they were cloning production data into *unencrypted* shadow copies of the normally protected on-premise data. These sandboxes, while short-lived, contained potentially significant amounts of protected information.

Absent an information security program that hinged upon the discovery, automatic classification, and governance of this type of regulated data, this organization was blind to the risk. The fault was not in their willingness to take security seriously, but rather, in the misapplication of a point solution (strong encryption) as a catch-all for cloud security.

The People Centric Security Alternative

The cloud's importance and the reasons for its prevalence do not exist in isolation from broader trends in technology. There is a convergence of principles that have made it possible; the primary factors at play for most organizations which either have or are considering adopting a cloud strategy are (1) the increase of interest in mobile computing, (2) the promise of streamlined IT, both from a budgetary as well as a technical perspective, and (3) the increased satisfaction and effectiveness of their end-users, who are likely familiar with the technologies and conveniences of similar platforms in their personal lives.

It is this final point that must be the basis for an appropriate, modern, and cloud-based security strategy.

For organizations that are working to secure their data in the cloud, that strategy needs to begin with an understanding of where the risks are. Not all data that is stored in a system like Salesforce is sensitive; in the example above, blocking the ability to create and share sandbox environments would likely result in credential misuse or even a decline in core platform adoption, as the business needs of the department heads and line of business owners came into conflict with the security requirements being placed on them.

Instead, a cloud-focused security program should be predicated on the idea that specific controls should be applied to data only when it is both (a) sensitive, and (b) exposed or in violation of regulatory requirements.

Secondly, it is critical to understand that the perimeter is no longer the boundary of the LAN or VPN. Relying entirely on a single solution or technology (e.g., the encryption module in use in the case study) will often result in a reduction in effective security -- the impression that "everything is covered" results in a lowered sense of awareness on the behalf of the end users and data owners.

The alternative here is to work with those staff on a direct, personal, and role-appropriate basis, leveraging discovery capabilities to approach policy violations in real time, before any damage is done, and making them salient to the staff who have stewardship over the exposed data.

Finally, the cloud-focused security or IT team must seek opportunities to make technology transformative business drivers, rather than blockers. If staff are seeking opportunities to access their content from home, while on the road, or via mobile devices, then the investment should be made in tools to monitor for suspicious login activity or potential abuse of those platforms, rather than seeking to implement complex network-level solutions that raise the barrier to use and introduce additional risk and single points of failure.

Principles of People Centric Security

Step 1: Trust
The hardest thing for most organizations to do is to accept that the role of IT has changed; cloud technology has provisioned access to end-users in a way that has never been seen before, with the very lines of the network blurring as a result of BYOD policies, work-from-anywhere access to sensitive and protected data, and increased demand to do more with less.

In general, people behave according to the expectations placed upon them; treating users as trusted partners makes it possible to encourage smart decisions around data security.

Step 2: Teach
With proper discovery technology in place, make it easy for users to recognize honest mistakes and quickly remediate them. It is through constant and timely engagement -- "teachable moments" -- that lessons about data access and compliance can be enforced, *before* there is a breach.

Step 3: Lead
Consider implementing automated data classification systems to complement outreach; the goal of PCS is to increase security by reducing rules, fixing mistakes without driving users into shadow IT solutions, and ultimately to make security a transformative enabler.

Conclusion

The rate of data loss and data breaches is accelerating, and that trend will continue for the foreseeable future. The cloud and the factors that have and will continue define its role are dramatically affecting how IT, business, and technology as a whole will be used. Simultaneously, there are multiple competing ideas, vendors, and solutions available to attempt to provide a measure of security in this tumultuous landscape.

As with any dynamic market, consider whether a particular strategy is aligned well with the fundamental factors that underlie the specific problems you are attempting to solve. In terms of cloud security, the decision is often between those solutions that are conceptually comfortable but limited in scope, and those which require that the solution reflect the same changes that the organization itself is undergoing.

Finally, seek out ways to enforce security within the cloud, rather than outside of it. Cloud-to-cloud security addresses where the daily decisions about how, when, and where to work with potentially sensitive information are most closely connected to the risk and possible prevention of data loss. Technological complexity is often met with resistance, and given the myriad options available for self-selected devices, services, and even cloud providers, resistance often leads to abandonment and secretive risk.

In other words, work with users, not against them. Find ways to make them more effective, and seek out opportunities to do so that works in a hybrid or even pure cloud way, rather than by attempting to force outdated and heavy-handed controls onto a mobile and sophisticated user base.

About CloudLock

Headquartered in Waltham, Massachusetts, CloudLock is the world's leading cloud data security company. Our solutions give organizations control over their data in the cloud, without requiring invasive in-band technology, complicated overhead, or unanswered regulatory risk.

Many of the world's largest companies and institutions trust CloudLock's approach of directly integrating with cloud application platforms, which makes robust security controls immediately available at a fraction of the cost and complexity of other alternatives. For more information, visit www.cloudlock.com.

CloudLock • 203 Crescent St., Ste 105 • Waltham, MA 02453 • 781-996-4332