EGNYTE

Selecting the Right Cloud & Data Security Solution

A Guide For Mid-Market CIOs

www.egnyte.com | © 2020 by Egnyte Inc. All rights reserved.

The digital transformation of businesses has pushed more applications and services to the Cloud. Coupled with the rapid shift to a work from home (WFH) environment, the need to share content is growing dramatically. In turn, security and compliance personnel are challenged to understand and address new threats to information security.

More web applications mean more web traffic. While this can be forced through an internal VPN when workers are on premises, remote workers may elect to bypass a corporate VPN and use poorly-secured WiFi networks and personal devices to access cloud-based business applications. As a result, organizations are likely to have "data sprawl," with sensitive data on personal devices, in mailboxes, in consumer-oriented file sharing applications, and in unsanctioned applications.

More cloud applications and more data in the cloud, accessed from more (unsecured) locations and devices presents an enormous attack surface to defend. How can security teams bring this under control?

Key Findings from the 2020 Egnyte Data Governance Trends Report

76 Percent of IT executives are concerned about unstructured data sprawl

97 Percent of the CIOs believe the security and controls for their existing content management systems are inadequate

29 Percent believe their employees follow information security policies well.

Compliance and Security Are Not Just for Large Enterprises

The 2020 Egnyte Data Governance Trends Report showed widespread concern over data sprawl and internal security. CIOs' concerns are well-founded. The growth of cloud applications like Office 365, Box, Slack, Salesforce.com, Dropbox, and others means more sensitive information is stored off-premises, where IT, security, and compliance teams have little visibility or control.

Most organizations believe some form of WFH will continue in the future. A recent survey found that 83 percent of organizations are planning for long-term remote working, and that 74 percent believed their response to security threats was less effective due to remote working.

Security events, of course, can lead to compliance issues. Whether by accidental loss or a data breach, organizations of all sizes must comply with regulatory standards to protect credit card data, Personally Identifiable Information (PII) and Personal Health Information (PHI). HIPAA and PIPEDA, the PCI Data Security Standard, and the California Consumer Privacy Act (and similar state-level laws) cover organizations that conduct business in North America. Compliance with the General Data Protection Regulation (GDPR) is required of organizations that do business with residents of the European Union.

The threat to mid-sized organizations is real. Large enterprises have the resources to maintain dedicated security and compliance teams to manage network defenses and build application security programs, making a hacker's job more difficult. The hacker's solution, of course, is to attack smaller organizations in the supply chain that have trusted access to the mid-sized and larger organizations' systems. From the attacker's viewpoint, finding the "weak link" in a trusted third-party is just as effective – and simpler – than attacking the larger organization directly. It matters little to the attacker that they destroy the reputation of these suppliers and partners in the process.

The problem is not theoretical. The 2013 Target Stores breach resulted from an employee of an HVAC vendor logging into Target's network using a device previously infected through a phishing attack. The attack then moved to Target's systems, reported back to a command-and-control server, and eventually exfiltrated millions of customer records. Leading cyber insurance provider The Hartford cites a study claiming, "63 percent of all data breaches can be linked either directly or indirectly to third-party access." Likewise, a survey by Spiceworks found that 44 percent of the firms responding reported a breach in the previous 12 months caused by a vendor.

Visibility is Paramount to Protecting Data

Most data must be shared to have value. In addition to employees, third parties often require access to sensitive information. Project plans must be shared with suppliers and subcontractors, design documents often require approval from local legislative groups, and employee information is provided to payroll and insurance providers.

The problem for most organizations can be condensed to three questions:

What data do we have? Organizations produce lots of data. Some is critical, some is regulated, and some is benign. Research and trade secrets must be kept from competitors and PHI and PII must be protected from leakage. Identifying and classifying data by sensitivity is the first step in any information security program.

Where is our data kept? Often the biggest challenge to organizations is simply identifying where all of their information is maintained. Digital transformation spreads data out to cloud applications, employees have data on company-owned and personal devices, and long forgotten "shadow IT" projects where links to proprietary information may exist.

Who is using our data? Legitimate use of sensitive data occurs daily. To identify malicious use of sensitive data requires organizations to understand baseline activities. The key to a successful information security program is to identify and block malicious activity without hampering data access by authorized users.

Mid-market CIOs Face A Dizzying Array of Options

There is no shortage of vendors offering a variety of solutions for managing and sharing data. These range from free-to-use consumer solutions to expensive and complex enterprise offerings. Mid-sized organizations can struggle with either. The former often lack centralized controls and adequate reporting and the latter can overwhelm overcommitted IT organizations and understaffed security and risk teams.

Consumer-Grade Solutions, Minimal Assembly Required

Local File Shares, Office 365, and Google Docs

Every business utilizes file systems and an office suite of some kind. Combined with a spreadsheet to track permissions, the result is a homemade content management system. For no additional cost, users can share files and collaborate on documents in the cloud.

> 63 percent of all data breaches can be linked either directly or indirectly to third-party access
>
> **- The Hartford Staff**

This model works when limited to very small teams and a small number of files, or when the content is not privileged in nature. Marketing can work with an outside vendor on branding and content, or finance can share information with an accounting firm. However, it quickly becomes unmanageable when the content is sensitive or as the number of participants and files increases.

- Managing user permissions for each individual file is cumbersome, and authorizations can be lost if the owner of the file is unavailable or leaves the organization.
- Auditing is extremely limited, adding risk to organizations with regulatory obligations.
- There is high risk of data loss when each individual user has download privileges (or simply the ability to copy/paste).

While these systems will always be an important collaboration tool for organizations, they cannot meet the compliance and security requirements of the mid-market or organizations that are viewed as critical in the security supply chain.

Enterprise Solutions, Assembly Required

File Hosting Services

Cloud-based file hosting services provide users with desktop and mobile applications for storing and sharing files. While most were originally built for consumers, business users have adopted the services as well.

The advantages of the services are clear; they provide an inexpensive and simple-to-deploy model for small teams to store, distribute, and share documents. As teams or projects grow "elastic" licenses can be adjusted to support an organization's needs.

However, the simplicity of the model leads to poor governance and security controls. In a cloud file sharing model, each user is assigned and manages personal folders and decides who can access files that are stored in each folder. This introduces several security and compliance issues:

- Limited visibility to sensitive data. There is no automated method to identify and classify sensitive data.
- No centralized control. All permissions are controlled by individual users, including providing rights to external users.
- User authorization is manual. Removing permissions for individuals who no longer require access to a folder must be done individually for each folder.
- Data loss can occur due to inappropriate permissions. Users can download and move files and/or share files indiscriminately.
- Because the model lacks IT oversight, compliance audits are challenging. Each user controls his/her own file deletion and logging is inadequate; IT cannot provide evidence of deleted files.

Consumer-First FSS Solutions

Collage of individual accounts that create islands of content

Data Loss Prevention

Data Loss Prevention (DLP) solutions are designed to protect sensitive information from "insider threats" and accidental data loss. Most work by "tagging" sensitive data and enforcing appropriate use policies to prevent legitimate users from taking risky actions (e.g., downloading files to a removeable drive), protecting data when shared (e.g., forced encryption when emailing a sensitive file), or identifying anomalous behavior that could indicate a malicious action (e.g., collecting and encrypting large amounts of data or logging in from unusual IP addresses). DLP is typically deployed at the network level as well as on endpoints, specifically on laptops and servers.

DLP solutions offer far greater control to IT, risk management, and security teams. File scanning routines can examine files to discover and classify sensitive information using regular expression rules such as text strings that resemble social security or credit card numbers. Granular policies can manage privileges by role or individual user, and many include "blocking" capabilities, forcing users to escalate requests for approval when an action violates standard policies or otherwise appears to put data at risk.

While DLP offerings protect data and provide better governance controls than unsecured file sharing solutions, they can present challenges as well.

- False positives are common as the systems "learn" or mistake legitimate behavior as malicious. This inhibits adoption and results in user resistance, limiting a tool's enforcement capabilities.
- Most endpoint DLP solutions are agent-based, requiring kernel-level control to monitor tagged data and enforce controls. These "hook and inject" solutions can introduce performance problems and may be incompatible with some systems. If sharing information with partners, those devices must also include an agent.
- Policies can become complex and difficult to manage. Pairing users and roles with allowed actions can require significant oversight and hamper solution rollouts for organizations that lack large IT departments.
- User pushback is common when policies impede existing workflow. This can result in users actively working to bypass controls or putting DLP solutions into "monitor-only mode". The former can put data at risk and violate compliance requirements, while the latter alerts on rather than blocking attacks.

Cloud Access Security Brokers

Cloud Access Security Brokers (CASB) are a new category of products that combine multiple security and compliance offerings into a single solution. As the name implies, CASBs sit between cloud providers and cloud consumers to enforce an organization's security policies.

CASBs can include:

Application and Data Discovery – CASBs examine web proxy and firewall logs to identify all cloud services and "shadow IT" projects, as well as unsanctioned applications like file sharing and peer-to-peer utilities. CASBs also automatically risk classify all structured and unstructured data.

Data Security – While most DLP solutions focus on preventing sensitive data from moving to the cloud, CASBs recognize that SaaS, IaaS, and PaaS services are a requirement for today's organizations and extend traditional DLP to native cloud applications.

Access Control – CASBs act as a proxy, funneling all traffic through the CASB for inspection. In addition to enabling granular application permissions (identification and authorization) adaptive access control helps to identify sensitive data exfiltration.

User and Entity Behavior Analytics (UEBA) – UEBA is a DLP alternative that baselines all user activity then uses machine learning to identify anomalous and malicious actions.

Malware Detection – By acting as a proxy between cloud users and providers, CASBs can also inspect all inbound traffic and perform static and dynamic malware analysis and threat intelligence to identify and block malicious code.

While CASB systems provide very good visibility to sensitive data and shadow IT, they do not always help solve all of the issues that they highlight.

- Like DLP solutions, CASBs often lack knowledge and context about how individual applications and cloud services handle permissions. Poorly configured and managed systems or attempts at granular policy enforcement can result in false positives and frustrated users. Further, proxy-based CASBs may cause an outage for end-users if a SaaS application alters its user interface.
- System latency can be experienced, due to real-time content inspection when a user uploads or downloads a file.
- Systems outside of the cloud environment require separate controls. For example, a CASB lacks visibility to off-the-network FTP transfers and mobile devices.
- Most importantly for the mid-market, CASBs require significant management oversight. They can actually diminish the overall efficacy of the security team, since there is a need to acquire, deploy, monitor, and maintain every security solution separately.

Primary Reasons Don't Use Full Capabilities of DLP/CASB Solutions

77 Percent Capabilities are too difficult to implement, maintain, and administer

57 Percent Our business systems have adequate data protection capabilities built in

55 Percent We lack personnel with proper security skills to manage DLP/CASB solutions

Source: Forrester Consulting

Purpose-Built Solutions for the Mid-Market Enterprise

Mid-sized companies have the same collaboration, security, and compliance requirements as their larger counterparts, but often lack the staff and resources needed to acquire, configure, and manage multiple enterprise solutions. At the same time, relying on homegrown or consumer-oriented solutions will not satisfy regulatory obligations, partner scrutiny, or Board expectations.

The middle ground between consumer-centric and large enterprise offerings requires a solution that provides enterprise-grade capabilities without the need for extensive configurations and management oversight. It should provide at a minimum:

Information Governance –The most critical function of a content collaboration system is the ability to automatically locate, classify, and risk rank all of the information in the enterprise and apply compliance and security policies to ensure proper use and protection.

Data Visibility – Organizations require visibility to sensitive information no matter where it exists, including cloud applications, local data stores, employee devices, and shadow IT.

Data Classification – User (manual) classification cannot scale to thousands or millions of files. The system must be able to identify sensitive information like names and postal addresses, dates of birth, financial information such as invoices, bids, credit card or bank account numbers, and individuals' health-related data automatically.

Minimize Data Footprint – Content sprawl occurs as organizations add users, devices, and information to their systems. Cloud storage, BYOD devices, email, and messaging applications all maintain copies of the same data. A professional collaboration system should identify redundant and orphaned/unused data that can dramatically increase the risk of data exposure.

Secure Collaboration –Email is widely used for sharing information, documents, and files, but when teams iterate through documents using file attachments it enlarges an organization's data footprint (and email storage requirements). Email attachments can often be replaced by web links to collaboration utilities or shared folders that maintain automatic versioning and file locking for the documents. Unlike consumer-oriented file sharing, an enterprise quality secure collaboration solution will allow discrete permissions for sub-folders (versus automatic permission inheritance) and allow unlimited file sizes.

Data Security – Visibility to sensitive files is the most critical component of data security. Close behind is the ability to identify which data is at risk from insecure locations, and can result in public exposure, overly permissive access, or exposure to malicious internal or external actors. This requires an understanding of the following:

Which folders contain the most sensitive information? – In many organizations a small percentage of folders contain the majority of sensitive information. A strong solution will allow administrators to find these locations quickly.

What data is publicly exposed? – A recent study estimated that 6 percent of Google Cloud buckets are misconfigured to allow public access. Errors like that have resulted in:

- The exposure of more than 100 GB of data from the US National Security Agency (NSA)
- More than 5.5 million files from a project management firm with information on cybersecurity firms, universities, and others
- Public access to information on more than 93 million Mexican citizens.

Who has access to sensitive data? - The Principle of Least Privilege states that users should be given only those privileges needed to complete their required tasks. In many organizations, "privilege creep" occurs when users change roles but maintain access rights that are no longer needed. For example, a user in Finance involved with payroll would need access to HR files on salaries. If that employee moved to an Accounts Receivable role, his or her access to HR files should be terminated. Similarly, as engineers switch projects, their access to product management and design documents should change.

Which Activity is Legitimate, and Which is Malicious? – Sensitive information is a target for hackers and competitors. Increasingly, ransomware attacks are used effectively to encrypt data rather than to steal it. The trend of WFH complicates Security's job. A solution that manages data effectively will include analytics to identify anomalous behavior that could indicate a malicious attack. This could include users logging in from unusual IP addresses or at unusual times, high levels of moving, copying, or downloading files, or a high velocity of file access and file changes (e.g., encryption) that could indicate a ransomware attack.

Compliance – Virtually every organization faces multiple regulatory standards. These standards can be very granular with specific guidance (such as PCI-DSS) or quite vague, requiring "reasonable security" standards. Understanding which of the overlapping standards applies to your data is just the first step. The most critical task is translating individual requirements into data security controls; ensuring that only the right people have access to files and are acting within policy.

Compliance requires granular visibility to in-scope data such as names, addresses, and account numbers. It also requires audit-quality evidence that simplifies audits and reporting to senior management and regulatory bodies. This can include proving what information was exposed in the event of a breach or accidental data loss as well as ensuring that all information is identified and securely deleted for Subject Access Requests.

Mid-market companies often lack dedicated compliance teams. Look for solutions that provide the ability to translate regulatory standards into workable policies, and back that up with out-of-the-box reports for standards such as GDPR, CCPA, HIPAA, PCI-DSS, FISMA, GLBA, GxP, and others.

> The same type of error is often found when organizations provide unprotected links to sensitive data. Be sure to look for solutions that allow private or password-protected links.

Next Steps

The "best" solution will vary based on your organization's needs, budget, and technical capabilities. Start-ups and organizations with few outside partners may choose to continue with office suites and consumer-based file shares. Those with large IT and security teams and mature processes and controls may opt for a combination of best-of-breed CASB, DLP, and network security solutions.

For those organizations in the middle: with hundreds or thousands of employees, large partner networks, and more modest IT and security capabilities, a comprehensive collaboration and data governance solution can provide better coordination, more flexible controls, and more robust security. A managed solution has the added benefits of a low cost of ownership, deployment simplicity with faster "time to value", management simplicity that doesn't burden scarce internal resources, and simplicity of use; boosting productivity without changing how employees collaborate.

	Pros	Cons
Local Files Shares & Online Office Suites	• Affordable • Simple for small groups • Limited user training requirements	• Departmental solution – Cumbersome for mid-sized and larger organizations • Poor Governance – No centralized controls • No visibility to sensitive data • All authorizations are manual – Difficult to prevent data loss • Poor audit and compliance capabilities for regulated data
File Hosting Services	• Affordable • Simple for small groups • Limited user training requirements	• Departmental solution – Cumbersome for mid-sized and larger organizations • Poor Governance – No centralized controls • No visibility to sensitive data • All authorizations are manual – Difficult to prevent data loss • Poor audit and compliance capabilities for regulated data
Data Loss Prevention	• Granular control over sensitive data that has been properly classified • Centralized policy management • Role-based privileges • Automated controls • Good audit capabilities	• Require security and operational resources to deploy and manage • May be expensive to license and maintain • Agent-based solutions can be prone to technical issues • Identifying sensitive data is often manual, slowing roll-outs • Granular policies may hamper scaling the solution and lengthen time-to-value • False positives inhibit adoption and cause pushback, limiting enforcement capabilities
Cloud Access Security Brokers	• Strong data discovery • Good data loss prevention for Cloud-based data • UEBA can detect anomalous behavior • Able to inspect traffic for malware	• Require security and operational resources to deploy and manage • May be expensive to license and maintain • Weak security for internal data • Proxy-based solutions can cause latency • Granular policies may hamper solution scaling and lengthen time-to-value • No visibility to off-network activity

Want to Learn More?

For additional information about how Egnyte helps organizations meet the challenges of secure collaboration and simple configuration and management, visit www.egnyte.com to schedule your complimentary Data Governance Assessment now.

EGNYTE

Egnyte provides the only unified cloud content governance solution for collaboration, data security, compliance, and threat prevention for multicloud businesses. More than 17,000 organizations trust Egnyte to reduce risks and IT complexity, prevent ransomware and IP theft, and boost employee productivity on any app, any cloud, anywhere. Investors include GV (formerly Google Ventures), Kleiner Perkins, Caufield & Byers and Goldman Sachs. For more information, visit **www.egnyte.com.**

Contact Us

+1-650-968-4018

1350 W. Middlefield Rd.
Mountain View, CA 94043, USA

www.egnyte.com