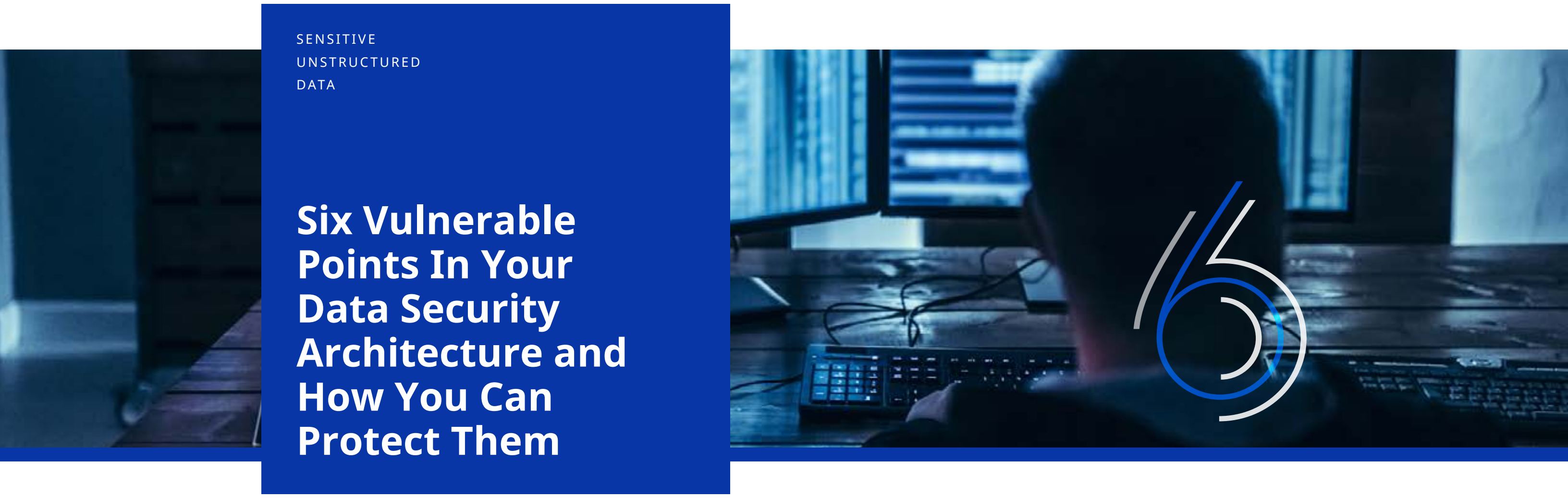
FASOO

WWW.FASOO.COM



SENSITIVE
UNSTRUCTURED
DATA

Six Vulnerable Points In Your Data Security Architecture and How You Can Protect Them

> Do you know where you are most vulnerable? Now is the the time to check these key trends:

1. Hybrid and Multi-Cloud
2. Privacy
3. Insider Threat
4. Security Gaps
5. Remote Workforce
6. Third-Party Collaboration

1. Hybrid and Multi-Cloud Environment

According to Flexera’s “State of the Cloud, 2020 Report”, organizations use an average of 2.2 public and private cloud providers. This exposes your data to the following risks:

Identity and Access Management (IAM): You may have heard the phrase, “identity is the new perimeter”. This “new perimeter” is the intersection of users, devices, and cloud services. Due to the COVID-19 pandemic and increasing regulations, many companies across the globe have had to reconsider how much access their employees have to their systems, applications, and data.

Security: Educate your Governance, Risk and Compliance (GRC), IT security, and Human Resources (HR) teams on the latest risks and make sure they have the data-centric tools they need to combat them. Ultimately, a breach will significantly impact your organization’s reputation and finances.

Data Residency: Data Residency: Cloud environments are boundless and can be located anywhere in the world. Legal and regulatory requirements are imposed on data in the country or region it resides. Review where your sensitive unstructured data is stored (on or off-premise) and make updates accordingly.

SOLUTION CONSIDERATION:

A data-centric approach identifies files and secures them in a centralized management system to provide consistency across all channels. Using discovery tools helps locate your data and classifies it with specific tags to control their cloud location.

2. Privacy

Today’s privacy regulations demand greater visibility and control over an individual’s data. Regulation types include:

- **Responding to the Rights of Individuals:** Regulations such as General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) give individuals greater rights to their personal data. Data subject and consent rights must be associated with all information collected on an individual.
- **Access and Revoke:** Every file access (system and user) must be traced for data collected. Individuals can elect how and when their data is used. The “right to be forgotten” requires total removal of all data and most transactions. Your organization’s staffing department must respond promptly to any individual privacy and audit requests. Breach notifications timelines are tightened (GDPR and CCPA is 72 hours).

SOLUTION CONSIDERATION:

Deep visibility tools accumulate access information during the entire lifecycle of the sensitive unstructured data. You should avoid traditional tools that provide limited visibility and require forensic action to search log files.

3. Insider Threat

While external threats from hackers and cybercriminals make the headlines, trusted insiders can pose a greater threat to your sensitive unstructured data. A traditional security infrastructure focuses on external threats using firewalls, anti-malware, intrusion detection, and other security solutions. These solutions may not prevent an employee, contractor or third party vendor with access from sharing it with unauthorized users.

There are three types of insider threats that require your attention:

1. Accidental: An employee or contractor may accidentally share a document with the wrong person exposing sensitive data. Once out of the person’s control, the information could go anywhere, violating privacy regulations and compromising your competitive position.
2. Negligence: An IT or security administrator forgets to apply a security patch or update to a firewall rule, exposing your sensitive unstructured data to theft. This is most likely an oversight, since many IT and security groups are overworked and understaffed. Another example would be for a user to deliberately circumvent security policies.
3. Malicious: Employees, contractors or partners who want to harm your organization or make money selling valuable information to competitors. This type of insider threat is difficult to stop because many have a legitimate need to access sensitive unstructured data.

SOLUTION CONSIDERATION:

Deep visibility tools accumulate access information during the entire lifecycle of the sensitive unstructured data. You should avoid traditional tools that provide limited visibility and require forensic action to search log files.

4. Security Gaps

Despite significant investments in security infrastructure and the deployment of data loss prevention capabilities, breaches are at all-time highs. Threat actors have greater success exfiltrating information on endpoints and servers where sensitive unstructured data is common.

What you need to acknowledge and have teams address:

- **Beyond prevention:** Data Loss Prevention (DLP) blocks and prevents sensitive data activities but doesn’t protect the data itself. Data breaches continue. Organizations and regulators are recommending the increased use of encryption to address the challenge.

- **Not a breach:** Many regulations take into account if encrypted data was considered a breach or not. Fines can be significantly reduced depending on the status.
- **Ransomware:** While companies may still be subject to disruption, often the most significant risk is sensitive data being exposed to the public or provided to others for financial gain. Data protected with encryption eliminates this risk. Encryption is mandated in modern-day regulations such as GDPR, CCPA, and New York State Department of Financial Services (23 NYCRR 500).

SOLUTION CONSIDERATION:

Enhance existing DLP investments by encrypting files with sensitive data. Use centralized encryption key management to maintain protection and control wherever the file travels.

5. Remote Workforce

This is a significant trend that's been recently accelerated by COVID-19. Security and privacy implemented in corporate offices can't be replicated at each home. Review your current policies to see if they address:

Home office/Virtual Workspaces: Work is more likely to happen on unmanaged and shared devices, over insecure networks, and in unauthorized or non-compliant apps.

Increased downloads: Slow network traffic, the convenience of working and sharing files - all result in increased volumes of sensitive unstructured data on endpoints.

Insider threat: Insider threat: Unintentional errors disclosing sensitive content increases without safety precautions. Malicious intent from at risk employees with access to home-based, non-sanctioned portable drives and printers is particularly concerning.

SOLUTION CONSIDERATION:

Use strong data-in-use tools like rights management capabilities that restrict printing and storing content on removable media.

6. Secure Third-Party Collaboration

Customer information shared with others remains your responsibility, regardless of who leaks the data. The challenges here are:

Privacy Regulations: Information that personally identifies an individual and associates that individual with financial, healthcare, and other data.

Screen sharing: Zoom, Skype, WebEx, Google Chat and Google Meet, Microsoft Teams, Free Conference Call, and similar applications expose sensitive information to screen capture by others.

End of project: Sensitive information often remains with third parties long after the project or relationship ends, often unprotected.

SOLUTION CONSIDERATION:

Deploy agentless browser collaboration with file tracking and protection. Screen blocking of sensitive information during collaboration sessions prevents losing sensitive data. Revoke access of sensitive files if shared with third parties once no longer needed.

KEY TAKEAWAYS

Proactive organizations stay ahead of these vulnerabilities by acting early to evaluate the impact of safeguarding their sensitive unstructured data.

Recommended best practices include:

1. Update GRC policies to reflect new guidance
2. Perform security gap analysis of current infrastructure
3. Implement employee awareness training as new risk and threat vectors emerge

Educate and empower your organization to stay one step ahead of hackers, cybercriminals, threat actors, and those with malicious intent.

Sales & Partnership: (732) 955-2333 | inquiry@fasoo.com

FASOO