Safeguarding Vital Data and Staying Out of the Headlines
# Table of Contents

Common Sources of Insider Risks .................................................. 3  
What You Can Do to Spot and Minimize Insider Risks ......................... 4  
Intel Security’s Solutions for Insider Risk Management .......................... 5  
Conclusion .................................................................................. 6
As data breaches continue to rise in number and severity, organizations are coaching employees on safe “data behavior,” while also using updated monitoring techniques to reduce exfiltration, ensure compliance, and improve visibility and control. No organization wants to be the subject of a high-profile data breach headline, but avoiding that fate can be more difficult than ever without new approaches and philosophies toward data loss prevention.

Ensuring that your organization doesn't become tomorrow's cautionary tale is essential—for many reasons. First, the costs to remediate data breaches are substantial and rising: New data from the Ponemon Institute indicates that the average cost of a data breach is now US$4 million, up 29% since 2013.¹ That includes a wide range of issues, from rebuilding data stores and shoring up security defenses to paying fines due to regulatory noncompliance.

Second, the loss of brand equity due to the negative publicity of a breach, while difficult to calculate precisely, is undeniable. Just ask a senior executive or board member at any of the countless name-brand organizations that saw their corporate secrets exposed in the media or on social networks. There is even a critical fiduciary element to protecting vital information: 68% of all breaches are required to be publicly announced.²

Third, more and more organizational data is now considered mission-critical. And that data resides in new, diverse places—consumer-class devices, applications downloaded from web stores, cloud services and Internet of Things (IoT) devices, sensors, and systems. Just identifying the location of data, let alone categorizing its criticality, is more difficult than ever.

Finally, the damage caused by loss of customer and partner confidence can be the biggest problem of all, simply because of the considerable amount of time it takes to rebuild loyalty and trust once private, confidential data has been exposed.

Putting in place a comprehensive, holistic data loss prevention (DLP) solution requires a combination of careful planning, development, and coaching of security best practices for employees and contractors; implementation of sophisticated data loss prevention (DLP) tools; and automated, yet flexible, policy management that doesn't put undue burden on overworked IT and security staffs.

This effort focuses on three major components, all of which must be addressed—individually and collectively—in order to fully protect the organization against the loss of vital data. These three pillars are:

- **Prevent data breaches and exfiltration**: A coordinated approach to DLP is central to protecting vital data; no longer will disparate solutions do the job.
- **Achieve compliance**: Regulatory mandates are a moving target, and most organizations have to contend with multiple compliance requirements across industries, geographies and use cases.
- **Regain visibility and control**: It’s not enough to monitor endpoints for malware and other threats. Organizations need total, real-time visibility and the ability to control infiltration and exfiltration—and respond efficiently and reliably.
Prevent Data Breaches and Exfiltration

If you knew there was a 26% chance that your organization would suffer a material data breach involving at least 10,000 lost or stolen records, you’d probably be terrified—and then you would want to quickly modernize your approach to DLP. That scenario is a reality. According to Ponemon’s latest data, the average cost of a lost or stolen record is now US$158—an all-time record, according to their research.3

Securing data, whether in the data center or at the endpoint, has always been tricky, and the introduction of numerous bad actors and innovative, insidious, malware into the equation has raised the stakes considerably. Add in the fact that data now resides in many unconventional locations, including unmanaged consumer devices, point-of-sale systems and kiosks, public cloud services, removable media such as USB drives, virtual infrastructure and IoT systems, and the problem is magnified further.

As a result, there are now more entry points for malware, and more risks—such as zero-day threats, advanced persistent attacks, social engineering, phishing and sophisticated exploit kits—waiting to be unleashed by a click on an innocent-looking email or a familiar web address.

Defending the “new perimeter” now requires a host of inbound protection solutions, such as intrusion prevention systems, identity/access management, threat intelligence services, managed security service, event management tools, and mobile device management, among many others.

The use of inbound security tools alone has proven insufficient when it comes to stopping sensitive data from leaking out of the organizations. To battle both malicious and accidental data leakage and exfiltration, organizations need a comprehensive DLP framework that secures vital data in motion, in use, and at rest. It also requires coaching and guidance on fundamental user behavior in order to spot potential problems before they turn into breaches, as well as modernized tools to make that coaching educational rather than punitive.

Without acknowledging the increasing likelihood of data breaches and exfiltration of vital data, organizations are going to be caught napping and end up in the headlines. And without the right tools and updated practices, that risk will continue to rise. So too will its negative impact.

Achieve Compliance

Compliance has become increasingly important as a security issue in direct correlation to the growing volume, variety, and velocity of regulatory demands. Compliance mandates span different industries, geographies, and use cases, and it is increasingly likely that an organization will need to deal with multiple, overlapping compliance mandates at any point in time. For instance, imagine a publicly traded medical products retailer selling into a range of countries around the world; that organization has to deal with a plethora of mandates touching a huge swath of its vital data.

Securing information for compliance purposes has become far more sophisticated in recent years because being compliant is more than simply passing an annual audit. Compliance is a day-in, day-out state, and organizations must know at all times the status of regulated data, particularly data in motion throughout the enterprise, including to and from the cloud.

At the same time, compliance has taken on a meaning outside the scope of regulatory requirements. Compliance also incorporates corporate governance that establishes guidelines on how vital data is managed, from collection and storage to backup, archiving, and, eventually, elimination. Additionally, DLP for compliance requirements must take into account civil and even criminal legal issues such as e-discovery.
This puts intense pressure on organizations to construct a DLP strategy that automatically treats vital data in a manner aligned with policies, and that those policies are managed automatically and can be adapted, as needed, to ever-changing business requirements.

Again, a meticulously crafted mix of DLP and encryption tools, along with innovative coaching methods to help users police themselves when it comes to handling vital data appropriately, is essential for ensuring compliance. For instance, imagine the scenario in which a financial analyst downloads an unreleased version of the upcoming earnings report onto a USB drive in order to study the report on a personal device at home. Rather than blocking the download, a pop-up window might appear, reminding the user that the data in question is deemed proprietary and asking him or her for an approval code to complete the task.

**Regain Visibility and Control**

As unstructured data—much of it considered mission-critical—continues to expand at eye-popping rates, organizations are struggling to fully understand just what data they have and where it resides. This lack of visibility, and the resultant lack of control of the data, has alarming consequences for organizations on all levels—operational, legal, regulatory, and financial.

With traditional corporate boundaries being reshaped, rewritten, and even erased entirely, securing data sources, applications, and devices requires increased visibility into the location, behavior, and status of vital data. This is exacerbated by such powerful forces as bring your own device, public cloud services, virtual machine sprawl, virtual workforces, and shadow IT, all of which tend to put added stress on traditional security defenses.

Regaining visibility into and control of, sensitive data is both more important and more challenging. This means that DLP’s mandate must be expanded to include all infrastructure types: physical and virtual, on premises and cloud, data center, and remote.

Cloud computing, in particular, presents unique DLP challenges when it comes to visibility and control. With so much data being sent from on-premises environments into the cloud, from one cloud to another or from the cloud back to on-premises infrastructure, simply knowing the location of critical data can be extremely difficult. Additionally, once data leaves traditional on-premises security defenses, there may be no guarantee that private data is sufficiently safeguarded unless encryption becomes a central DLP element.

In these increasingly prevalent scenarios, a new approach to security management is required. A comprehensive, single-pane-of-glass approach that automatically unifies all security policies regardless of data type, device location, user privileges, risk factor, or compliance mandate is essential to allowing important information to appropriately pass from point to point safely and reliably.

**The Intel Security Data Protection Framework**

Safeguarding vital data is far more challenging than ever, due to the many factors, ranging from new threat vectors and an expanding number of new devices to the expanding impact of data breaches on the organization. That means that creating and deploying the proper DLP framework requires doing away with narrowly focused security solutions and instead utilizing a strategically planned, comprehensive, multilayer defense that covers data on premises or in the cloud, in the physical or virtual infrastructure.

Security decision makers should seek out technology partners that understand how to deploy a comprehensive, integrated set of solutions that span and link DLP, encryption, and device control and have the capability to manage common policies, incidents, and workflow all under a unified management framework.
Intel Security offers a broad set of tools designed to safeguard vital data in a manner that promotes alignment across tools in order to create actionable insights that block data exfiltration and other unauthorized data movement.

McAfee Data Protection is an enterprise-wide framework for safeguarding vital data residing at any point—on the network, in the cloud, on endpoints or personal devices, or on virtual machines. The integrated and comprehensive solutions include:

- **McAfee Total Protection for Data Loss Prevention**: Incorporates endpoint DLP, network DLP, and device control to protect sensitive data wherever it lives—on premises, in the cloud or at the endpoints.
- **McAfee Complete Data Protection suites**: Block unauthorized access to sensitive information and preventing exfiltration using policy-based security, native encryption, drive encryption, and removable media encryption.
- **McAfee® ePolicy Orchestrator® (McAfee ePO™) software**: A centralized management console that links security management functionality across systems, applications, networks, data, and compliance solutions. Security professionals can use McAfee ePO software to continuously detect and respond to emerging, advanced security threats across all possible points of infiltration, while spotting and blocking potential exfiltration attempts.

Finally, in the event of an actual data breach, Intel Security's Professional Services organization acts as an incident response resource to immediately and fully remediate data exfiltration. This team of security professionals helps to identify security gaps, particularly weak spots in security defenses that have yet to be penetrated.

**Conclusion**

A big part of the new reality of IT security is understanding, acknowledging, and planning for the inevitability of the steadily increasing complexity, risk, and financial impact of security breaches. Addressing this dilemma requires more than just technology, even though sophisticated new tools have helped to make this process more effective. Instead, organizations need to look at risk and potential data breaches as business problems that require a combination of tools, practices, processes, coaching, and services that make successful DLP a reality.

Since staying out of the headlines for an expensive and embarrassing data breach is a goal for all organizations, new solutions and approaches are mandated in order to deal with a rapidly expanding set of threat vectors. Intel Security offers organizations the ability to protect, detect, and correct issues before they permeate the organization and do untold damage. Additionally, Intel Security’s centralized management framework gives organizations the ability to prevent data breaches and exfiltration, ensure compliance and regain visibility and control.

For more information, please visit:
www.intelsecurity.com

---

3. Ponemon, ibid