FROST & SULLIVAN

Comprehensive and Unified Data Protection for Distributed Work Environments

Zscaler's Solution to Data Loss Prevention and Protection

FROST & SULLIVAN EXECUTIVE BRIEF

Organizations handle a lot of sensitive data every day, but they struggle to keep that data protected while facing further potential penalties if they do not stay compliant with regulatory requirements. A part of this challenge is that organizations are grappling with highly distributed data resulting from the rapid adoption of SaaS and cloud applications.

Over time, organizations have partnered with multiple vendors to try to identify and secure sensitive data across their enterprise environments.

The **adoption of multiple point products** often fails to work cohesively when securing information, leading to fragmentation that creates vulnerabilities in data protection strategies.

The adoption of generative AI has only exacerbated the challenge, with users chasing productivity gains introducing new avenues for data loss.

The Threats Against Valuable and Sensitive Data

The Lifeblood of Organizations

Protecting It Against Both Inside and Outside Threats

Maintaining and Demonstrating Compliance

DATA The Lifeblood of Organizations

Digital systems are the lifeblood of modern enterprises, with the prevailing use of technologies like cloud, mobility and now AI today. This is driven by the growth in data, the use of data to solve customer problems and to provide value to users. This data must be protected, to protect competitive advantage, meet customer expectations as well as meet data privacy regulations and compliance requirements.

But the data estate is expanding, with data now residing:

- On-premises
- In the cloud
- In various SaaS applications everywhere

As such, managing this data and protecting enterprise competitiveness is growing increasingly difficult and complex.

Enterprises recognize this importance, but often partner with multiple vendors, deploying different point products to form a patchwork that fails to provide CIO teams with a comprehensive and integrated way of better protecting precious data.

DATA Protecting It Against Both Inside and Outside Threats

Organizations are also facing the threat of bad actors due to data's value. While many companies focus on ransomware strategies, they often neglect comprehensive data protection. This oversight is particularly concerning given that most ransomware attacks now employ double extortion tactics, encrypting and threatening to publish or sell data, necessitating a robust data protection plan as an integral part of any effective ransomware defense.

Bad actors aren't the only worry—those *inside the organization* can be a risk. **The Insider Threat Report 2023 from Cybersecurity Insiders revealed that 74% of organizations consider themselves at least moderately vulnerable to such threats**. This is not always malicious data theft; these leaks often stem from negligence or accidental loss.

Regardless, the damage is the same. These interconnected issues underscore the complex and evolving nature of cybersecurity challenges facing businesses today. Frost & Sullivan research found that data security is the top priority area for enterprises, but achieving protection can be complicated.

DATA Maintaining and Demonstrating Compliance

Organizations must juggle achieving protection against data loss with maintaining compliance. These related goals can be at odds. Fulfilling compliance with regulations such as GDPR and HIPAA is a constant and complex battle for organizations as the sheer scope and intricacy of these regulations make it challenging to ensure continuous compliance.

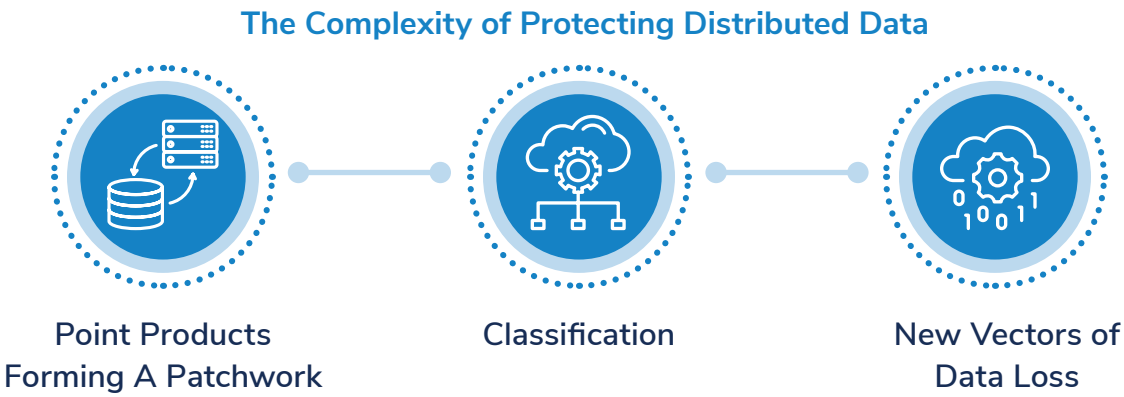
Organizations must continuously monitor and update their policies and procedures to align with the latest regulatory requirements, which can be time and resource consuming. The need for visibility into the state of compliance at any given time is crucial, but achieving this can be daunting given the dynamic nature of data processing and the continually evolving data protection and threat landscape.

> **Data security is the top priority area for enterprise, according to Frost & Sullivan research."**

This struggle to maintain compliance and effective protection highlights the need for a unified and proactive approach to data protection and privacy, achieved through a DLP platform that ensures organizations can effectively navigate the complexities of robust protection of distributed data while maintaining regulatory compliance.

The Complexity of Protecting Distributed Data

Organizations' security teams face a complex landscape of data risks, including highly distributed data, sophisticated bad actors, and insider risks, all while struggling against the limitations of fragmented point solutions.



Point products form a patchwork that is unable to support teams while holistically managing and protecting sensitive data

Point solutions are adopted over time to meet an organization's evolving needs. However, the bolt-on approach and independence of these solutions often complicates data protection efforts by creating a more complex environment to manage. This is because they:

- **Are resource intensive:** Implementing multiple solutions requires increased staff training, a broader team skill set, and more time dedicated to system maintenance.
- **Give fragmented Alerts:** Alerting becomes disjointed across point products, hindering a comprehensive understanding of data loss incidents and delaying timely responses.
- **Leave blind spots:** Siloed solutions lead to a lack of correlation and no unified view of data protection, with separate DLP engines working in isolation.

The overall result is a highly complex system that is challenging to manage effectively, reduces threat detection and response efficiency, and potentially leaves gaps in data protection coverage.

> **Most organizations are blind to their data's location due to its distributed nature and disjointed siloed point products."**

Classification Leading to Further Data Confusion

Efficient classification is a challenge for organizations. Classification is prone to error due to both a lack of good tools, ineffective home grown tools and because the data to be classified is not always human-created or straightforward (e.g., software code), which complicates the process. With data everywhere and always moving, these challenges are further amplified.

Despite these challenges, accurate classification is necessary to effectively protect sensitive data across various locations like SaaS, IaaS, inline, and devices. This is especially troubling for critical or sensitive data. Proper classification is required to secure organizations data, whether it is intellectual property or information protected by laws like PCI or GDPR, to maintain compliance as well as security.

GenAI Is a New for Vector of Data Loss As Users Experiment With New Tools

Organizations must contend with an evolving landscape of data protection challenges, including generative AI tools that have emerged as a double-edged sword. While these tools have become invaluable assets for many employees, enhancing productivity and creativity, they also present risks to data security. According to a survey by 3Gem,

> **31% of employees acknowledged entering sensitive data like customer information— including personally identifiable information—as well as sales and financial data into these tools."**

Companies need to adapt their data protection strategies to address the unique risks. Blocking these applications to protect data can hinder productivity, but allowing their use can expose organizations to significant risk.

Organizations face significant challenges in securing their data, especially within the context of distributed and dynamic environments. Point products often struggle to effectively secure data spread across various devices and cloud destinations, leading to fragmentation and vulnerabilities in data protection strategies.

Further, the constant creation and movement of data pose a daily challenge in accurately classifying it, making it a relentless task to keep up with the pace of data generation. The proliferation of generative AI tools further complicates this landscape, as they introduce risks that are difficult to mitigate. Finding a balance between allowing the use of these AI-driven applications to maintain productivity while preventing data loss is a critical issue.

[This is the summary recommendation: an adaptive and integrated approach is required]

An adaptive, integrated approach is required to protect sensitive data anywhere, automate discovery and classification, and adapt to new vectors as enterprises evolve.

A comprehensive and adaptive approach, one that detects anomalous behavior and dynamically identifies the most critical risks to data security, is essential to navigate these complexities and ensure robust protection without compromising operational efficiency. The ideal protection must be holistic. By addressing these issues with a more integrated platform approach, organizations can streamline their data protection efforts and improve their overall security posture.

What Does a Modern Data Protection Platform Look Like?

The ideal DLP solution offers a comprehensive approach to protecting sensitive information across an organization's digital ecosystem supporting people, process and technology goals.

TECHNOLOGY

Integrated and Unified Technology to Support the CIO Team

A unified DLP policy that ensures consistent alerting across all channels eliminates discrepancies and provides a single assessment for data protection.

The ideal solution should offer comprehensive protection across multiple channels, including endpoints, email, cloud applications, networks, and removable storage devices, to prevent data exfiltration through various potential exit points.

The solution should enforce policies that are unified across all channels. This ensures that alerting remains consistent as it moves across the organization.

Such a data protection platform approach enables improved outcomes by combining proactive prevention with real-time monitoring and response capabilities.

This allow organizations to quickly identify and mitigate potential data loss incidents while maintaining regulatory compliance and protecting sensitive and valuable intellectual property.

PROCESS AI-Powered and Automated Processes to Streamline Operations

AI-powered automation in data discovery and classification is essential for accelerating the labor-intensive and daunting task of daily manual data classification.

Streamlining daily operations through the automation of common workflows is vital. By automating routine tasks, organizations can enhance productivity, reduce errors, and free up resources for more strategic activities.

It is crucial to have a deep understanding of new regulations, and an accurate measurement of existing compliance. This ensures that the organization remains aligned with evolving regulatory requirements, maintaining a high level of compliance and mitigating the risk of non-compliance.

Effective system processes are essential to maximize the capabilities of data loss prevention tools, ensuring the organization's data is secured to the highest standard.

PEOPLE Enabling Users and Customers to Incorporate Data Best Practices

The solution should integrate with existing communication channels to enable coaching of both good and bad behaviors. This approach ensures that the program is widely supported and understood across the organization, fostering a culture of compliance and best practices.

While dedicated IT resources are necessary, a well-designed and properly built program based on the above automation tenets can achieve more with fewer resources. This efficient use of IT resources allows for greater scalability and effectiveness in managing the system.

Acknowledging the importance of people in the data security approach facilitates a seamless operation, where automation is effectively utilized to support and enhance the efforts of the individuals at the core of the organization.

How Zscaler Helps Deliver Better Data Protection

Zscaler's DLP platform, integrated within the Zero Trust Exchange, provides a unified solution that effectively addresses data protection intricacies in complex, distributed environments.

Protect all data channels

By filling security gaps and simplifying operations, it offers seamless protection across all channels, including the internet, email, endpoints, SaaS, IaaS, private apps, and generative AI apps.

Auto Data Discovery

The platform leverages AI-powered algorithms to enable automatic data discovery and classification, enhancing the accuracy and efficiency of identifying sensitive information without extensive manual configuration. Zscaler's solution identifies the data, data usage, and provides organizations with a dashboard with actionable insights for data leaving the organization, data at rest in SaaS applications, cloud services, and endpoints.

Secure GenAI Use

Zscaler's Data Protection solution provides visibility for GenAI applications, Shadow Gen AI applications, combined with user activity. This allows organizations to apply granular DLP policies at the user prompt level. Zscaler's solution protects against data loss while allowing productive use of generative AI tools, ensuring that employees can safely leverage productivity-enhancing technologies.

Zero Trust with Inline Proxy Inspection

It inspects all internet and encrypted traffic at scale. The Zero Trust Exchange creates secure, direct connections between users and applications to reduce the attack surface and minimize data risks.

This comprehensive approach strengthens data protection strategies, enhances the user experience, and improves the operational efficiency of organizations.

Unified Protection Across All Channels

A platform-based approach with centralized DLP enables seamless protection across key data loss channels, including inline inspection for data in motion, API-based controls for cloud data at rest, and device-level security. This unified approach ensures end-to-end visibility and control over sensitive data, while allowing flexible scalability to add new channels as needed. By eliminating fragmented point products, it reduces complexity, lowers costs, and strengthens compliance for distributed environments.

Streamline processes with Workflow Automation

The solution simplifies processes through streamlined and automated workflows, freeing up resources and increasing efficiency, enabling organizations to achieve more with fewer resources, and respond to incidents quicker.

Ensure compliance with Posture Management

Posture Management ensures that regulatory compliance is achieved even in a world of constant regulatory evolution, continuously protecting organizations from the risk of non-compliance.

Adopting a Data Protection Platform Is Vital Because the Data Ecosystem Is Changing Rapidly

As outlined, organizations face a complex landscape of risks, including:

- Highly distributed data,
- Sophisticated bad actors, and
- Insider threats

...all while struggling against the limitations of fragmented point solutions.

The ideal approach to addressing these challenges lies in adopting a comprehensive, integrated platform solution that offers unified DLP policies, consistent alerting across all channels, and comprehensive protection. By combining proactive prevention with real-time monitoring and response capabilities, organizations can more effectively safeguard their sensitive information and intellectual property.

By implementing an integrated DLP platform, organizations are able to achieve improved efficiency through AI powered data discovery and classification. The ideal solution ensures regulatory compliance now and in the future as regulations evolve. It is also critical that the platform supports the people, integrating with existing communication channels to coach both good and bad behaviors, fostering a culture of compliance and best practices.

> **Zscaler's solution leverages AI-powered data discovery and classification for enhanced accuracy and efficiency, offering seamless protection across all channels and allowing for the productive use of innovative technologies like generative AI tools."**

Process streamlining and automation through a robust and comprehensive platform is a critical aspect in improving data protection strategies. Zscaler's solution enables organizations to strengthen their data protection strategies while maintaining operational efficiency.

It is crucial for organizations to adopt holistic, adaptive data protection strategies that can keep up with emerging threats and technologies. Integrated solutions that offer comprehensive protection, user coaching, and streamlined operations, like Zscaler's platform can better secure an organization's valuable data assets and help maintain a robust security posture.

Putting It All Together: Data Protection With SSE

Delivering a meaningful data protection strategy begins with a solid understanding of architectural fundamentals. Data protection delivered from a Security Service Edge can offer significant advantages by reducing complexity and point products while enhancing data risk reduction.

With Zscaler's Data Protection Platform, organizations can adopt a unified, comprehensive approach to data loss protection. This allows for easy scaling of protection across all key data loss channels and accelerates visibility and control around Gen AI Applications, SaaS Platforms, and Devices.

Ultimately, this approach enables companies to confidently embrace digital transformation initiatives, harness the power of new technologies, and drive innovation while safeguarding their most valuable asset—their data. In the current, rapidly evolving digital landscape, a robust and adaptable data protection strategy is not just an option but a critical necessity for long-term success and resilience.

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➜

FROST & SULLIVAN