www.ibs.com.cy

SAFEGUARD YOUR DATA: GAIN VISIBILITY AND FLEXIBILITY WITH A SINGLE ENDPOINT AGENT.

The increase in remote work, easy access to data and tools, and high employee turnover has heightened the risk of data loss and insider threats. According to CISOs, nearly two-thirds (63%) of businesses experienced sensitive data loss in the past year, while insider threats have surged by 44% in recent years.

These challenges require security teams to identify and prevent risky behavior to minimize damage. It is essential to recognize that data doesn't lose itself; people are responsible for its loss. Therefore, modern information protection strategies must prioritize individuals.

However, information protection directly impacts end users, making it crucial for security teams to implement controls and monitoring without compromising user experience or performance. Let's explore how this can be achieved:

1. Not all users are the same:

    - Insiders are individuals who have authorized access to a company's systems, networks, and data, implying trust from the business.
    - Not all insiders pose a threat; only those who are careless or abuse their trusted position are considered insider threats.
    - Monitoring efforts should focus on gaining insights into the riskiest users all the time and low-risk users some of the time, rather than collecting endpoint telemetry for all users continuously.

2. Everyday users (90% of the population):

    - Most users fall into the low-risk category.
    - Monitoring data movement associated with these users (e.g., access, usage, copying files, printing sensitive documents, cloud sync) is sufficient.
    - Violations of corporate policy can be captured for security team review.

3. Risky users (10% of the population):
    - Risky users include departing employees, privileged users, third-party contractors, and Very Attacked People™ (VAPs).
    - Monitoring must extend beyond data activity to include user behavior.
    - Capturing screenshots of risky behavior provides context and forensic evidence for cross-functional investigations involving HR and legal departments.

To effectively monitor both everyday and risky users while preserving user experience and productivity, Proofpoint offers a combined data loss and insider threat solution. This solution utilizes a single lightweight endpoint agent with the following advantages:

- User Experience and Productivity:
    - The agent runs in user mode, minimizing conflicts with other agents.
    - Users remain unaware of its presence, and system performance remains unaffected.
- Seamless Policy Switching:
    - Security teams can switch a user's monitoring policy from everyday to risky and vice versa as circumstances change.

The monitoring capabilities differ based on user types:

- Everyday Users:
    - Capture data activity (e.g., file copying, document printing, cloud syncing).
- Risky Users:
    - Monitor data activity and user behavior (e.g., application use, web browsing, security controls tampering, unauthorized software).
    - Capture metadata and screenshots as forensic evidence for investigations.

A real-life example of the value of such monitoring arises with departing employees. Once an employee gives notice, they may start preparing for their next opportunity, potentially intending to take sensitive data with them. In this scenario, the departing employee transitions from being an everyday user to a risky user, leading to increased monitoring, including the capture of screenshots.

A global hospitality company faced a similar use case and turned to Proofpoint's converged Endpoint DLP and Insider Threat Management (ITM) solution. By implementing this solution, the company achieved increased visibility into the activities of both everyday and risky users, ultimately saving costs. The company had previously used Proofpoint ITM on a small number of risky users but desired to expand monitoring capabilities due to growing employee turnover and increased remote work. Budget constraints were a challenge, but the converged solution provided the needed visibility and flexibility without the requirement for two separate agents. Presently, the company monitors 18,000 users with Proofpoint Endpoint DLP and a small subset with ITM, dynamically applying the risky user policy as necessary.

To further enhance visibility and efficiency, Proofpoint Endpoint DLP and ITM are integrated into Proofpoint Sigma, an information protection platform. This platform assists companies in preventing data loss, investigating insider threats, and blocking cloud-related risks. With the unified console provided by Proofpoint Sigma, security teams can view and investigate alerts generated from endpoint, email, cloud, or web activities, eliminating the need to pivot between multiple tools.

By leveraging a single endpoint agent, businesses can protect their data with enhanced visibility and flexibility. Monitoring every day and risky users ensures a comprehensive approach to information protection without compromising user experience or system performance.

Source