Insider Threat Management and Endpoint Data Loss Prevention Comparison

Insider Threat Management (ITM) and endpoint Data Loss Prevention (DLP) solutions are often compared to each other. ITM solutions are context aware to the user and sensitive data, while traditional endpoint DLP solutions focus only on data movement.

Summary

In the past, organizations were most concerned about protecting regulated and easily identifiable information (such as PII,PHI, and PCI-related data). That was possible as only a small minority had access to sensitive data. Now, we are all working with sensitive data, whether we are developing, marketing, selling or manufacturing products and services. Think of sales conversations in which roadmaps and case studies are commonly shared. With that, security teams' are now focused on the context in which the user interacts with your sensitive data.

Traditional endpoint DLP solutions detect and prevent endpoint-based data loss based on data discovery, classification and content inspection at the user's endpoint. ITM solutions provide a context-aware approach that protects against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly. Such solutions focus on detection and response by providing user context and evidence, instead of prevention-only approach from traditional endpoint DLP vendors. With the importance of intellectual property, development plans, customer information and other sensitive data to organizations, context on user interactions with your sensitive data is critical for modern data protection & governance.

Product Architecture

ITM solutions provide a lightweight, endpoint sensor with context-aware detection and response. You should expect very low endpoint impact and little to no maintenance with every technology change and product upgrades. ITM solutions collect user activity and data movement that is driven by the user on their keyboard or through the mouse. In comparison, traditional endpoint DLP solutions live within the kernel on the endpoint. They only monitor file events, most of which are not user driven. Such solutions have struggled with endpoint performance degradation.

ITM vs Endpoint DLP Capability Comparison

	ITM	TRADITIONAL ENDPOINT DLP
Detect: User risk context	✓	x
Detect: File movement context	✓	✓
Detect: Insider threat alerts	✓	x
Investigation: User context aware	✓	x
Investigation: Irrefutable and easy to understand evidence	✓	x
Investigation: Context aware to other security alerts	✓	x
Response Actions: Real-time user education	✓	x
Visibility: Discover and classify regulated and structured data	Yes, through lists	✓
Visibility: Identify Intellectual Property (IP), business documents and unstructured data	Yes, through partnerships	✓

Technical Details

DETECT

User risk context

ITM solutions can detect risky user activity on endpoints through granular visibility into application titles and URLs, printer spool, keylogging, command line activity, mouse movement and cut/copy/paste and other mouse/keyboard shortcuts.

File movement context

E.g.: Before leaving the organization, sales John downloaded customer & pricing lists from the corporate CRM application, renamed both to photo.jpg and photo1.jpg and exfiltrated via a USB stick. Traditional endpoint DLP solutions may provide disparate alerts around the download and exfiltration, if configured properly. The security team is left to manually correlate the user, alerts and file in question. In comparison, ITM solutions provide the granular visibility in an easy to understand, real-time story. That can be the difference between resolving incidents in minutes, not days of investigation.

ITM solutions have visibility into user interaction with files and data such as renaming, copying and moving unstructured data.

Insider threat alerts

While the number of vectors for data exfiltration have increased, traditional technologies such as USB devices and email are still as commonly used as are cloud storage applications. Users are savvy enough to find the blindspots in traditional endpoint DLP solutions. Modern security teams look to ITM solutions to provide detection across exfiltration vectors.

ITM solutions span across insider threats from unauthorized activity and access to risky accidental actions and unwanted data movement ahead of costly security incidents.

INVESTIGATION

User context aware

ITM solutions focus on the “who” behind risky activity so that security teams uncover the user and their intent behind the chain of actions related to an alert or an investigation.

Irrefutable and easy to understand evidence

ITM solutions provide easy to understand evidence in PDF reports and through screen capture. Given the evidence is based on timelines of events and screenshots, instead of hard-to-decipher logs. All business units from Legal, HR and Cybersecurity can collaborate more effectively during investigations.

Context to other security alerts

ITM solutions provide before, during and after user context to point-in-time alerts from other security solutions to quickly determine false positives from alerts requiring further investigation.

RESPONSE ACTIONS

Real-time user education

ITM solutions provide response actions rather than hard prevention features. The most common are real-time notifications such that when users trip a security alert, this can be tied to their organization's security policies and act both as a deterrent and training to educate users, if they make an out-of-policy mistake.

VISIBILITY

Contextualize regulated and structured data

Regulated and structed data refers to Personally Identifiable Information (PII), Protected Health Information (PHI), sensitive payment card data by PCI standards and other easily identifiable information often stored in SQL databases. ITM solutions provide lightweight classification based on file location, file destination and file type. For example, ObserveIT ITM can also track sensitive files based on imported lists of sensitive file names from a data classification provider.

Contextualize Intellectual Property (IP), business documents and unstructured data

Sensitive information in such files is often actively being modified and hence cannot be easily identified using endpoint DLP classifiers. Most ITM solutions either have lightweight alternatives to detecting and classifying sensitive IP or integrations with classification providers. For example, ObserveIT ITM has lightweight classification based on file location, file destination and file type and is building integrations with Proofpoint CASB for content inspection and Microsoft Azure Information Protection for data classification.

Summary

Traditional endpoint DLPs have proven to be successful with preventing easily identifiable data loss and helping organizations meet strict data security regulations. With a context-aware approach, Insider Threat Management solutions are successful in enabling organizations to detect and respond more effectively when tackling potential damage by employees, third party vendors and contractors, either by accident, with malice or under compromise. Such risky activity may cross data loss boundaries and lead to privilege abuse, unauthorized system changes and brand damage.

For more information, visit https://www.observeit.com/solutions/protect-from-data-loss/

LEARN MORE

For more information, visit **observeit.com**.

ABOUT OBSERVEIT

ObserveIT, a division of Proofpoint, is the leading Insider Threat Management (ITM) solution with more than 1200 customers globally. ObserveIT helps organizations protect against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly.

The ObserveIT platform correlates activity and data movement, empowering security teams to identify user risk, detect to insider-led data breaches, and accelerate security incident response. Leveraging a powerful contextual intelligence engine and a library of over 400 threat templates drawn from customers and leading cybersecurity frameworks, ObserveIT delivers rapid time to value and proven capability to streamline insider threat programs.

observeIT
a division of Proofpoint