observe IT
a division of Proofpoint

SOLUTION BRIEF

Insider Threat Management and User Entity Behavior Analytics Comparison

Insider Threat Management (ITM) and User Entity Behavior Analytics (UEBA) solutions are alternative technology solutions to enable insider threat programs. ITM solutions detect threats by building contextual data on user activity and data interaction by insiders, while UEBA technologies rely on artificial intelligence to identify anomalies from second-hand data collected from logs of IT and security solutions.

Summary

Insider Threat Management (ITM) solutions protect against data loss, malicious acts, and brand damage involving insiders acting maliciously, negligently, or unknowingly. These solutions collect first-party data on users and files providing granular visibility into insider threats. ITM solutions have the detection and response capabilities to directly address insider threat security challenges. In comparison, UEBA solutions monitor and alert on user behavior anomalies based on ingesting and analyzing data second-hand from IT and security technologies. These anomalies are deviations from past behavior ("baseline" or "normal"), not necessarily insider threat scenarios. By focusing on the broader Security Information Event Management (SIEM) market and relying on varying quality of data sources in each case, they provide generic visibility and detection. The customer is often burdened with tuning their models for insider threat use cases.

Product Architecture

ITM solutions leverage lightweight, endpoint sensors (i.e. agents) that collect first-party information on user activity, data movement and application use that is driven by the user on their keyboard or through the mouse. Context-based detection and response capability enables security teams to identify potential risks and rapidly investigate whether action needs to be taken. In comparison, UEBA solutions aggregate and analyze logs from other security and IT solutions. Using machine learning and other statistical techniques, these platforms alert based on suspected anomalies in user behavior. Analysts must review alerts and pursue investigations using other tools.

ITM vs UEBA Capability Comparison

	INSIDER THREAT MANAGEMENT (ITM)	USER ENTITY BEHAVIOR ANALYTICS (UEBA)
Visibility: User actions context	✓	✓
Visibility: File movement context	✓	Limited
Visibility: Time to value	Immediate	Months (to baseline)
Detect: Insider threat alerts	✓	Limited
Investigate: Irrefutable & easy to understand evidence	✓	x
Respond: Real-time user education	✓	x
Respond: Soft blocking (e.g.: closing applications & logging off users)	✓	x

Technical Details

VISIBILITY

User actions context

ITM solutions collect first-party, trustworthy information on application titles and URLs, printer spool, keylogging, command line activity, mouse movement and cut/copy/paste and other mouse/keyboard shortcuts through lightweight endpoint sensors. By visualizing and correlating this data in easy to understand timelines of activity, ITM solutions provide trustworthy context on user actions.

File movement context

ITM solutions track the history of files across applications, endpoints and users, from origin through renaming and movement to destination outside corporate endpoints using their lightweight endpoint sensors. This provides context to the eventual data exfiltration by negligent or malicious users. On top of this, 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.

Time to value

ITM solutions provide immediate insights into user activity and data movement. It starts with silent installations and easy enterprise deployments without requiring complex integrations with many other tools. On top of that, ITM solutions correlate user activity and data movement immediately without needing weeks to months of training data to baseline “normal” behavior.

DETECT

Insider threat alerts

ITM detection capabilities span across insider threats from unauthorized activity and access to risky accidental actions and unwanted data movement ahead of costly security incidents. These alerts are easy to refine and understand in enterprise environments, even for non-technical teams. They do not require the expertise of data scientists or deep cybersecurity experience.

INVESTIGATE

Irrefutable & 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 of endpoint activity instead of hard-to-decipher logs, Legal, HR, business units and cybersecurity teams collaborate more effectively and quickly during high-stress and urgent investigations.

RESPOND

Real-time user education

ITM solutions provide real-time user notifications when users trip one of the insider threat alerts so that they can be reminded of the corporate acceptable use policy and other security policies. Such notifications also provide the user the ability to inform security teams of the legitimate circumstances for the activity that tripped the alarms.

Soft blocking (e.g.: closing applications & logging off users)

ITM solutions can close applications and log users out of their endpoint session when users trip high severity alerts that indicate clear malicious intent.

Summary

UEBAs have been successful with detecting sophisticated and advanced technical threats such as account compromise and privilege escalation and identifying significantly anomalous behavior. Insider Threat Management solutions are successful in their focus on protecting against potential insider driven damage based on the context of the situation rather than whether it is anomalous or seems normal. Real-time, easy to manage and understand detection requires alerts, notifications and context tuned to the frequency of insider threats. Immediate, cost effective and accurate response requires strong and easy to share evidence when collaborating with teams outside security. ITM solutions deliver return on investment (ROI) for insider threat teams in by reducing mean time to detect (MTTD), reducing mean time to respond (MTTR) and letting teams operate more resource efficiently.

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.

observe IT
a division of Proofpoint