

DISCOVER THE MISSING PIECES IN YOUR CYBERSECURITY STRATEGY

- A comprehensive guide to eradicate evolving cyberthreats with AI-driven analytics

Table of contents

■	Introduction	3
■	Harnessing real-time automated anomaly detection for proactive network security	4
■	Comprehensive detection of privileged access vulnerabilities with AI-powered user behavior analysis	9
■	Bolstering hybrid infrastructure resilience with nuanced threat intelligence	14
■	Accelerating incident resolution with cross-correlation	17
■	Conclusion	22
■	About ManageEngine Analytics Plus	23

Introduction

The global cybersecurity landscape is rapidly evolving. As cybersecurity budgets and spending continue to soar, the threat landscape is also becoming increasingly complex. This trend is highlighted by the fact that the **global cybersecurity market** ^[1] is predicted to grow from \$262.4 billion in 2021 to a staggering \$450 billion by 2025. Yet, the **Global Cybersecurity Outlook 2024** ^[2] report from the World Economic Forum found that 81% of cybersecurity leaders feel more exposed to cybercrime in 2024 compared to the previous year.

One key reason for this contrariness is cyberthreats becoming more sophisticated, unique, and capable of bypassing traditional security measures. This is evidenced by Fortinet's 2023 **Global Threat Landscape report** ^[3], which found a 68% increase in unique exploit detections over the past five years. In such highly dynamic threat environments, conventional security strategies often fall short, leaving organizations vulnerable to devastating breaches.

As a result, cyber resilience has become a major concern for business and IT leaders. According to **Accenture** ^[4], 74% of CEOs are worried about their organization's ability to mitigate the damage from a cyberattack. To tackle this challenge effectively, organizations must transform their cybersecurity approach to keep up with the evolving threat landscape.

This e-book introduces four emerging strategies that can transform the cybersecurity approach, enabling organizations to stay ahead of threats and safeguard their IT landscape. By leveraging the cutting-edge, analytics-powered strategies discussed in this e-book, organizations can build a foolproof security perimeter that adapts to the ever-changing threat landscape.

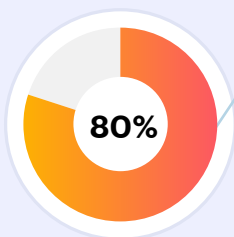
01 | **Harnessing real-time automated anomaly detection for proactive network security**

Ensuring flawless network security is a critical priority for organizations worldwide. In today's connected IT landscape, most IT assets or components link to some form of network. Therefore, any breach in network security can disrupt the entire organization and lead to insurmountable losses. This makes proactive threat detection and prevention paramount.

One of the earliest and tell-tale indicators of network compromise is unusual traffic flow. Such an anomalous phenomenon could stem from common attacks like distributed denial-of-service, advanced persistent threats, botnet activity, and more, all targeting an organization's network for data exfiltration, ransomware injection, and other malicious ends. These threats must be triaged and addressed promptly.

The traditional security approach often relies on setting baseline values based on expected normal traffic behavior and creating static, manual thresholds to trigger alerts for potential network breaches. However, these preset thresholds and baseline values, established through historical data analysis and understanding of normal behavior, fail to account for the dynamic, user-specific, seasonal, and strategic business scenarios present in a diverse, constantly evolving IT environment. This leads to a high number of false positive alerts that disrupt critical day-to-day business operations, eventually resulting in alert fatigue and impacting cyber response.

A recent independent survey^[5] by Intrusion revealed

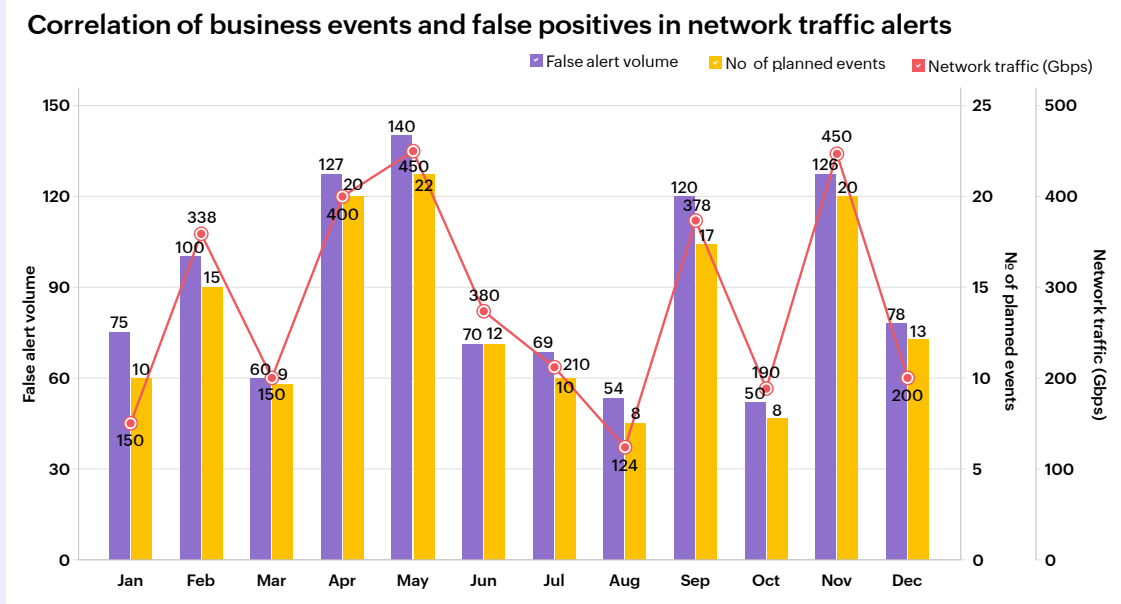


- Cybersecurity analysts spend a significant portion of their time trying to resolve these false positive alerts.

Therefore, it is imperative for IT teams and security analysts to effectively deal with false positive alarms generated by static traffic thresholds.

The below analysis illustrates several key issues with using static thresholds to detect anomalous network traffic, such as:

- During months with strategic business events, there is a legitimate spike in network traffic that gets incorrectly flagged as a false alarm by the static thresholds. This traffic is expected and part of the norm for those scenarios.
- The configured static thresholds fail to differentiate between event-related, normal traffic increases and truly anomalous traffic patterns. This leads to a high number of false positives.
- The increasing volume of false positives can result in alert fatigue, negatively impacting the productivity of security engineers and IT teams alike.



To address these problems, organizations often move towards a more dynamic approach that accounts for expected variations in network traffic.

Dynamic thresholds, which reassess and adjust threshold values dynamically in response to variation in common parameters like planned traffic spikes and daily activities, are generally considered the better alternative to static thresholds. However, even dynamic thresholds struggle to fully capture the complexity of real-world network traffic. Moreover, it is impossible to configure dynamic thresholds that cover every possible planned and unplanned scenario, including:

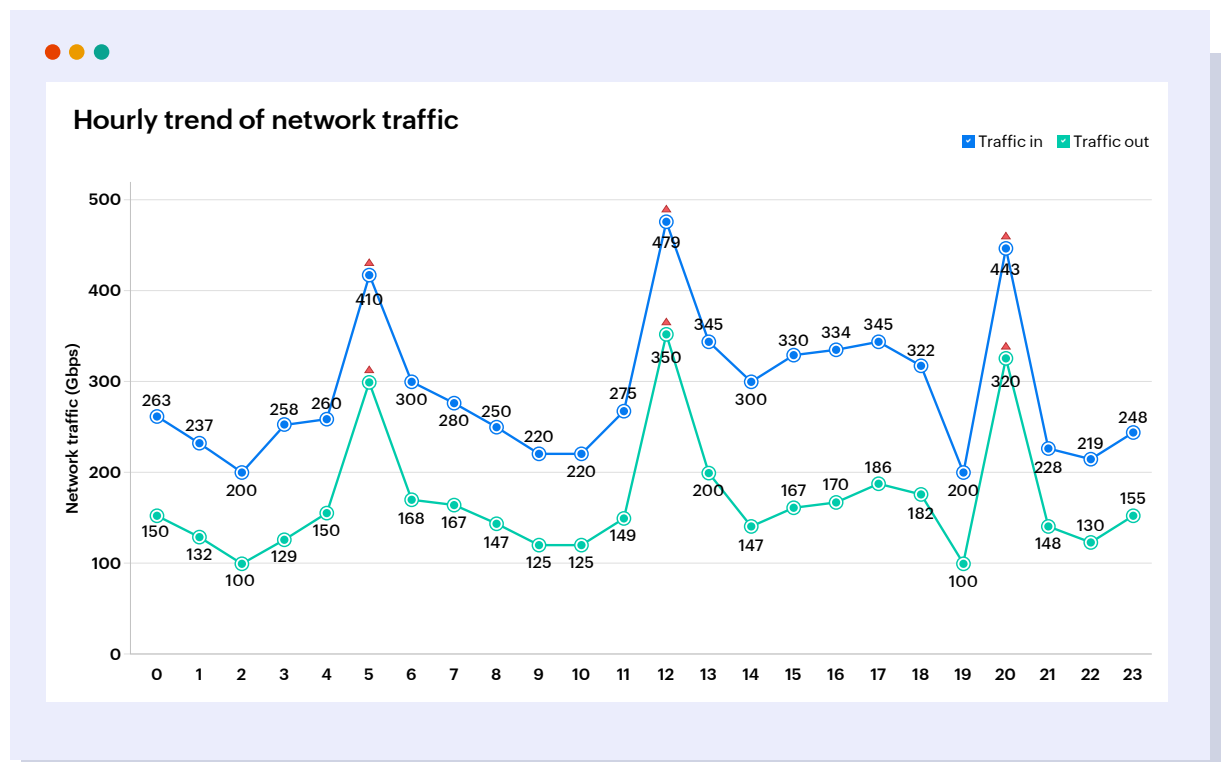
- Natural increases in traffic during events that signal business growth, like sales, holidays, or product launches.
- Low-level yet significant deviations in traffic patterns, such as intermittent bursts of unauthorized data exfiltration, that may not breach set thresholds.

Automated anomaly detection and alerting is the future of threat prevention

By moving away from manual or dynamic thresholds and towards real-time, automated anomaly detection, security teams can enhance their network security posture. With advanced AI and ML algorithms, automated anomaly detection allows for continuous monitoring of traffic patterns without relying on preset thresholds.

By leveraging the smart anomaly-based alerting capabilities in Analytics Plus, ManageEngine's flagship IT analytics platform, security teams can automatically flag outliers or anomalies that exhibit a significant deviation from the standard traffic flow pattern, helping them precisely identify suspicious trends in real-time traffic flow.

This approach adapts to the natural ebbs and flows of network traffic, ensuring that only truly anomalous activity triggers alerts. Anomaly-based alerts also help in detecting subtle yet potentially harmful deviations that may go unnoticed when using preset threshold-based alerts, effectively distinguishing between regular traffic fluctuations and genuine threats.

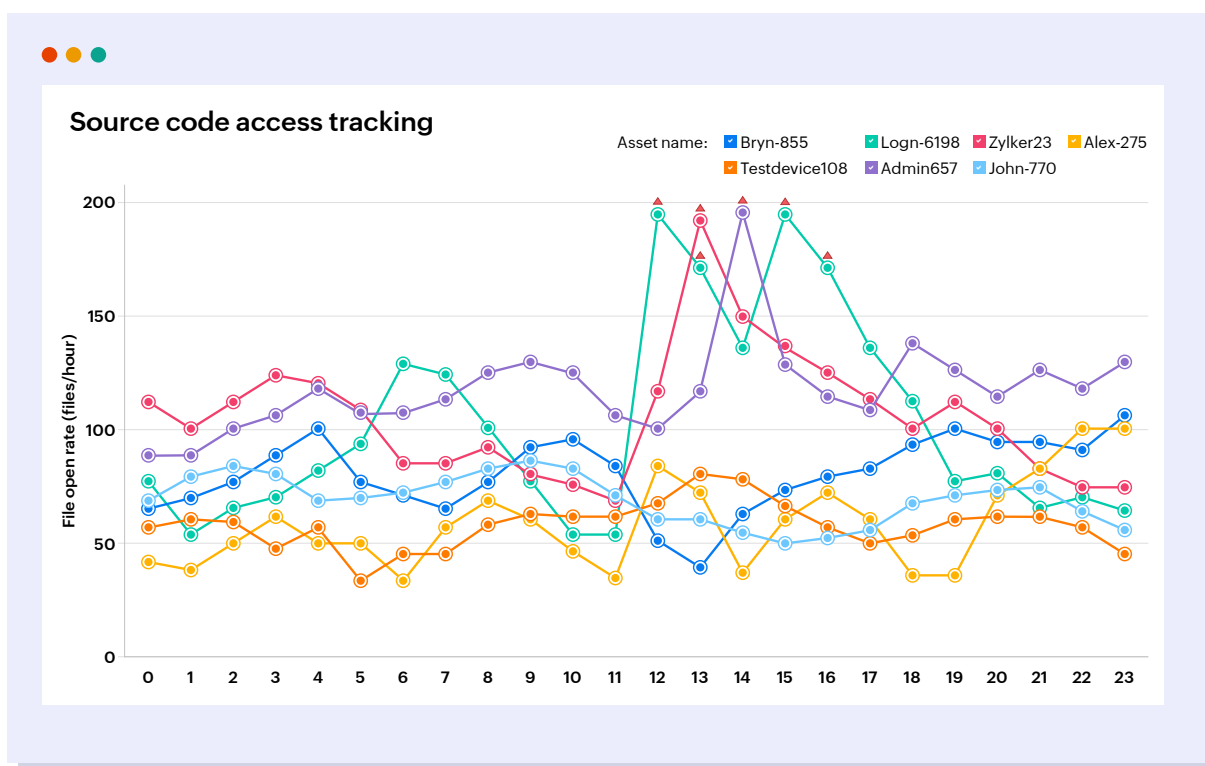


By adopting this approach, CISOs can significantly enhance their network security posture, reducing false positives and ensuring that true threats are caught and addressed promptly.

Beyond network traffic monitoring, automated anomaly detection capabilities also aid in detecting signs of compromise in endpoints, weeding out shadow IT, blocking data exfiltration, and reducing the impact of zero-day threats.

Let's take a look at how automated anomaly detection can play a crucial role in proactively identifying signs of compromise on endpoints—the first line of defense in an organization's network. With endpoints being the most common initial access point for malicious actors, this strategy enables organizations to quickly detect and block potential threats before they can gain a foothold and lead to costly vulnerabilities.

Organizations can reduce such vulnerabilities by effectively monitoring endpoints for unexpected behavior or operational anomalies.



The above analysis tracks the hourly frequency of access to a highly sensitive source code file for the company's flagship software product by various endpoints within an organization's engineering department. You can clearly observe from the analysis that there is an anomalous increase in the number of times devices Admin657, Logn-6198, and Zylker23 accessed the file between hour 12 and hour 18. Through automated anomaly detection, IT teams can recognize and flag these anomalous deviations as potential signs of an endpoint being compromised and initiate an alert for immediate investigation.

02 **Comprehensive detection of privileged access vulnerabilities with AI-powered user behavior analysis**

As seen above, proactive strategies like automated anomaly detection are the most effective defense any organization can deploy to prevent cyberthreats before they occur. However, the vast and diverse threat landscape makes it impossible to catch every threat before it reaches its target. The next supplemental strategy for security analysts is to accelerate threat detection and minimize access to privileged data to avoid critical impact on the organization.

In today's complex and distributed IT environments, privileged access management (PAM) has become indispensable. PAM focuses on monitoring and regulating access to an organization's most sensitive assets and data, limiting it to a few high-priority individuals or accounts. In recent times, privileged accounts have become prime targets for cyberattacks, especially ransomware and malware attacks, making effective monitoring of privileged accounts and data essential for mitigating the risks involving these high-value accounts.

Privileged accounts face numerous attack vectors, including insider threats, credential leaks, brute-force attacks, and social engineering. Organizations have relied on tracking user activity, maintaining logs of users with access to privileged accounts, and monitoring password reset requests as their primary strategies for detecting and mitigating PAM threats. However, these methods are often reactive.

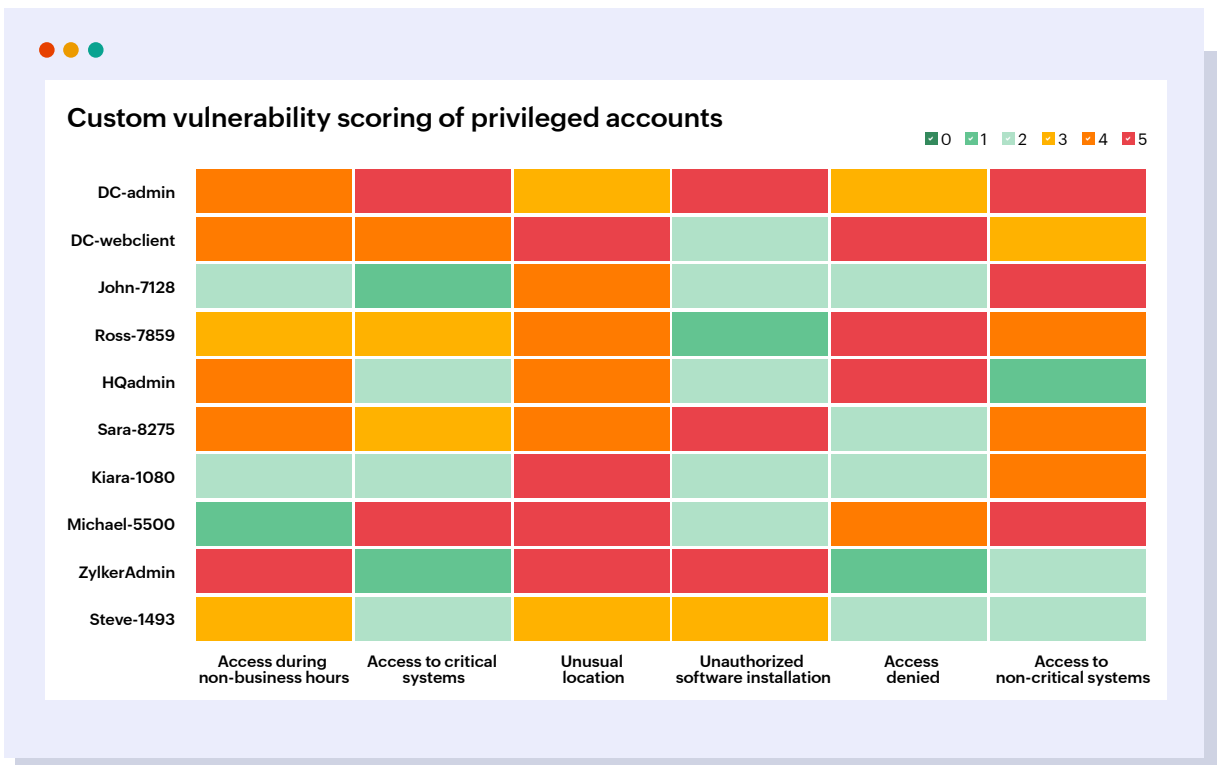
For instance, monitoring frequent password changes may help identify suspicious activity, but by the time it's flagged, damage may have already occurred and even compounded. Similarly, logging access records uncovers who accessed what and when, but it doesn't prevent unauthorized access from happening in the first place.

Attempting to combat advanced access management threats using reactive methods is akin to bringing a knife to a gunfight. Modern access management challenges require modern solutions. In today's age of AI, leveraging AI and ML algorithms offers a more impactful approach to detecting and thwarting security incidents targeting privileged accounts. Organizations can harness the power of AI to enhance traditional user behavior monitoring for privileged accounts. This allows for real-time analysis of factors like login times, access patterns, and the frequency of privileged actions to quickly identify and mitigate potential threats.

● **Custom privileged risk scoring model: Tailoring user behavior analysis to organizational needs**

The key benefit of AI-based user behavior analysis is the ability to create custom user behavior analysis models tailored to an organization's specific needs and operating conditions. By leveraging the AI-driven features of Analytics Plus, security analysts can develop custom models for vulnerability assessment. This allows organizations to define their own risk factors based on access management policies and security-related usage patterns. The custom models then automatically analyze user- or account-level usage, assign vulnerability scores, and identify the privileged accounts that require attention.

This custom vulnerability scoring model offers more flexibility and control as it's common practice for PAM solutions to have tight control over their proprietary scoring models. The analysis allows organizations to add their own criteria and parameters based on the organization's needs as well as apply custom weightage to each factor. Furthermore, they can leverage AI-powered scenario analysis to dynamically adjust the weightage based on changing conditions, ensuring the vulnerability scores align with the situation at hand.



The heat map above visualizes the risk scores of 10 privileged accounts using a custom risk scoring model. Each account is automatically assigned a score ranging from one to five, with 5 indicating the most vulnerable accounts and 1 the least vulnerable. This scoring is based on the account's behavior against the six specified scenarios.

An overall vulnerability score for each user can then be calculated by combining the weighted scores for each scenario as shown in the below analysis. This allows organizations to prioritize high-risk accounts for immediate attention, ensuring that response efforts are both strategic and effective.



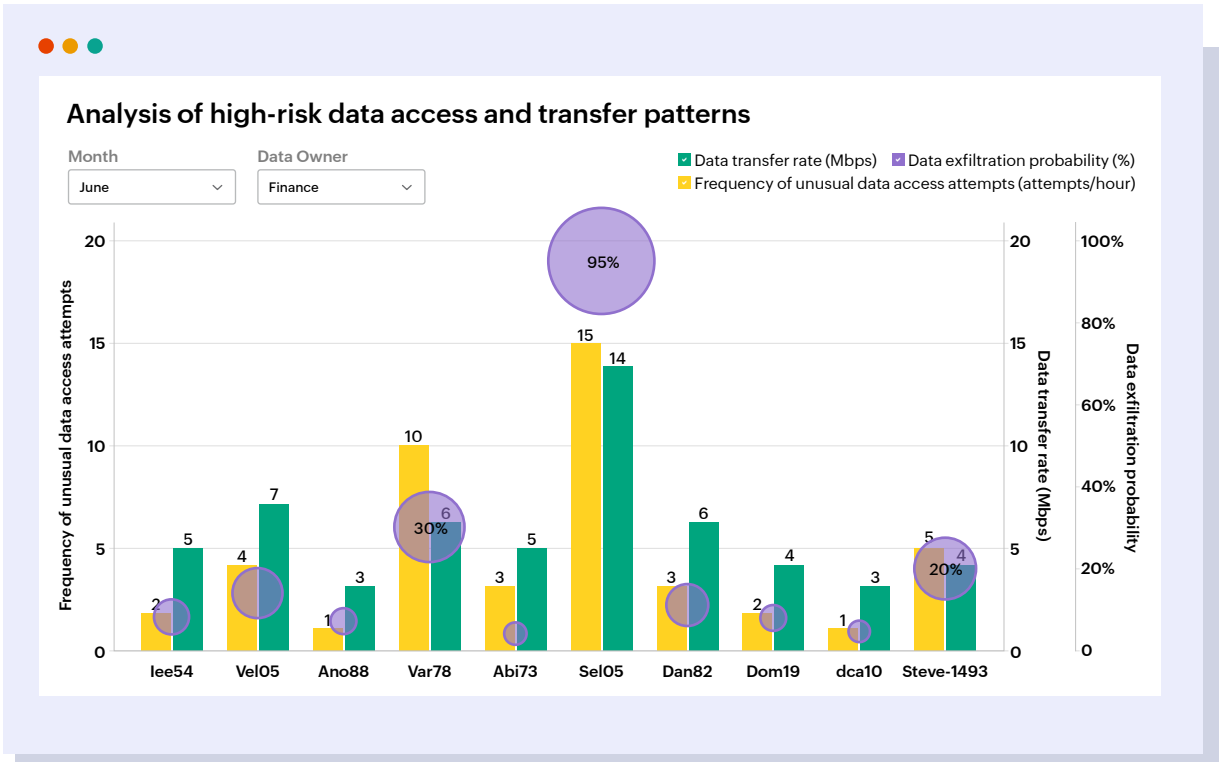
AI-powered user behavior analysis offers a proactive approach to detecting and mitigating vulnerabilities, especially for privileged accounts. By implementing custom risk scoring models tailored to an organization's specific needs, businesses can significantly enhance their ability to detect and respond to potential threats, ensuring the security of their critical assets and data.

The applications of AI-powered user behavior analysis should extend beyond privileged accounts. For instance, it is a powerful tool for detecting data exfiltration, a significant concern for organizations as data becomes increasingly valuable, and one that frequently originates from insider attacks.

Insider threats—whether malicious or accidental—pose significant challenges, leading to data breaches and data loss that can cause severe financial and reputational damage.

A malicious insider with access to sensitive data might target small volumes of sensitive data to avoid detection by systems that monitor data transfer rates. Such threats could go unnoticed unless the organization employs AI-powered user behavior analysis to continuously monitor and analyze user behavior, detecting patterns that are indicative of an insider threat.

For instance, say an employee with access to highly sensitive financial data but who rarely accesses it except at the end of the fiscal year suddenly starts accessing and downloading that data during non-working hours in June. In this case, an AI-based user behavior analytics model, as shown in the below analysis, would flag this activity as a potential data exfiltration attempt.

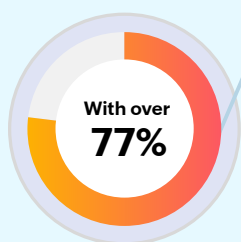


The analysis visualizes a custom KPI—data exfiltration probability. This percentage indicates the likelihood of a specific user being the source of insider threats. This metric can be automatically computed based on a user's frequency of unusual data access attempts and data transfer rates, as determined by the custom user behavior analysis model.

Security and IT teams can leverage these insights to immediately investigate and mitigate the risk before any significant damage occurs. This proactive approach revolutionizes insider threat detection and helps prevent data exfiltration, keeping organizations secure in an increasingly complex threat landscape. By taking a more proactive, AI-driven approach to threat detection and mitigation, organizations can stay ahead of evolving security challenges and better protect against costly breaches.

03 Bolstering hybrid infrastructure resilience with nuanced threat intelligence

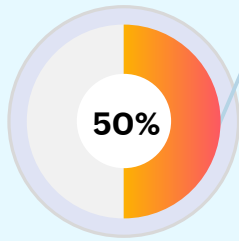
As organizations continue to embrace the cloud, there is a never-before-seen increase in the adoption of hybrid infrastructure that blends on-premises and cloud environments. While hybrid infrastructure offers flexibility and scalability, it also brings forth new security vulnerabilities and challenges.



organizations^[6] using multi-cloud applications or hybrid deployments, achieving a resilient and stable hybrid infrastructure security posture has become the need of the hour.

In the rat race to embrace hybrid infrastructure benefits, ensuring robust security often takes a back seat, leaving IT teams exposed to cyberthreats such as malware, ransomware, and data breaches.

According to the 2024 Cloud Security Study^[7] by Thales Group

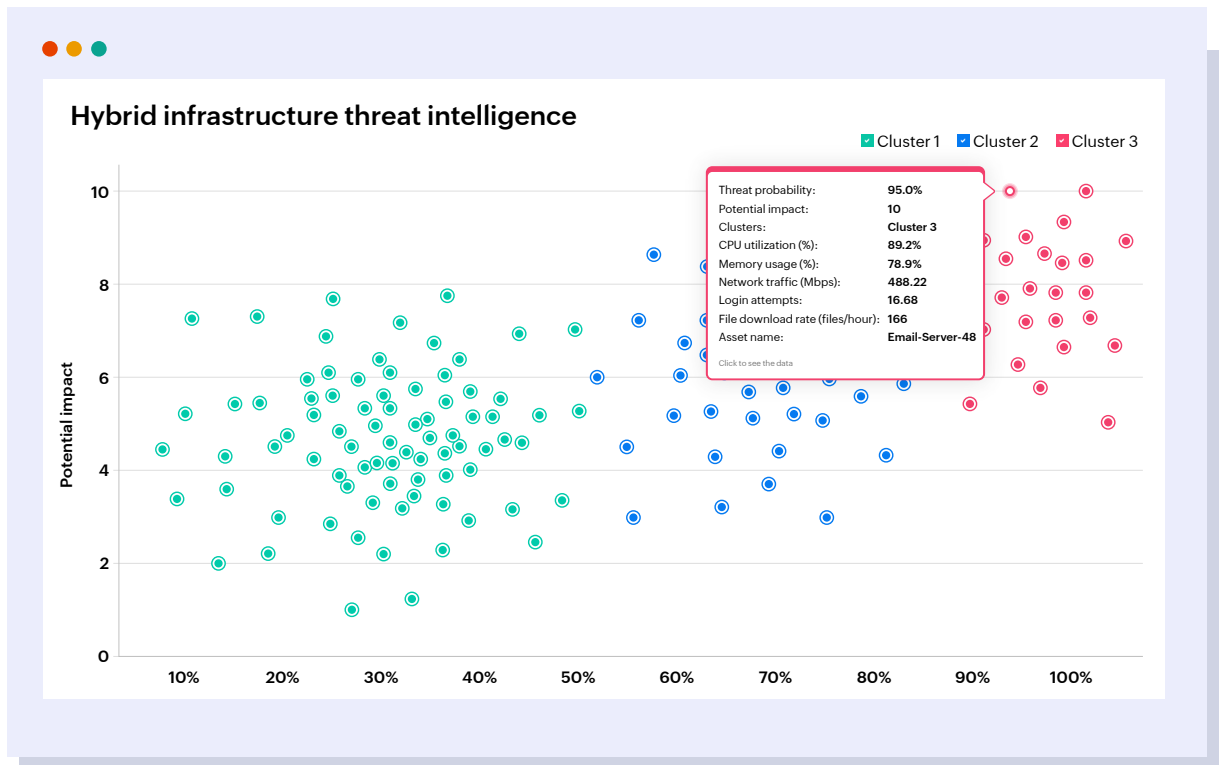


organizations globally struggle with compliance and privacy management in the cloud compared to on-premises setups.

Cloud-related security incidents have also surged exponentially, with 44% of organizations reporting cloud data breaches and 14% experiencing breaches within the past year—and this trend is expected to rise, particularly in vulnerable hybrid environments.

While many organizations employ threat intelligence strategies like signature-based analysis, heuristic analysis, and rule-based alerts to detect and prevent threats within traditional IT infrastructures, they often lack comprehensive strategies for detecting and mitigating complex threats in hybrid landscapes efficiently.

Incorporating cluster analysis, a proven IT intelligence technique, can play a pivotal role in bolstering cybersecurity measures, especially in incident detection and intelligence within hybrid environments. By aggregating closely related security indicators from both cloud and on-premises platforms, such as data transfer, resource utilization, usage patterns, and network traffic flows, clustering can effectively identify patterns and anomalies, offering valuable insights into infrastructure and cloud security threats.



This analysis showcases how organizations can use clustering to group hybrid IT resources based on their risk of being targeted by attackers and the possible severity or consequence of a cybersecurity incident.

Cluster analysis groups all individual resources into three clusters based on four key factors from activity logs—resource consumption (CPU and memory usage), data exfiltration (data transfer rate), usage patterns (login attempts and file download rate), and network traffic flows. This provides a comprehensive view of the threat landscape in the hybrid IT infrastructure by visualizing the threat probability and potential impact of any cybersecurity incident (values ranging from 1 to 10, where 1 represents the lowest impact and 10 represents the highest impact).

The resources in Cluster 3 exhibit unusually high levels of data transfer, CPU and memory usage, login attempts, file downloads, and network traffic—likely indicating the presence of malicious, high-impact threats that require immediate attention. Cluster 2 shows moderately elevated values for these factors, suggesting potential malicious activity that warrants further investigation. In contrast, Cluster 1 represents a normal pattern of hybrid resource usage with minimal threat probability and impact.

By applying clustering to user activity and resource usage data, organizations can effectively and quickly identify and investigate suspicious patterns that might otherwise go unnoticed amidst the sea of information generated in evolving IT landscapes. This AI-driven approach enhances threat intelligence in hybrid and cloud environments, enabling faster response to potential breaches and strengthening overall cybersecurity defenses in IT environments.

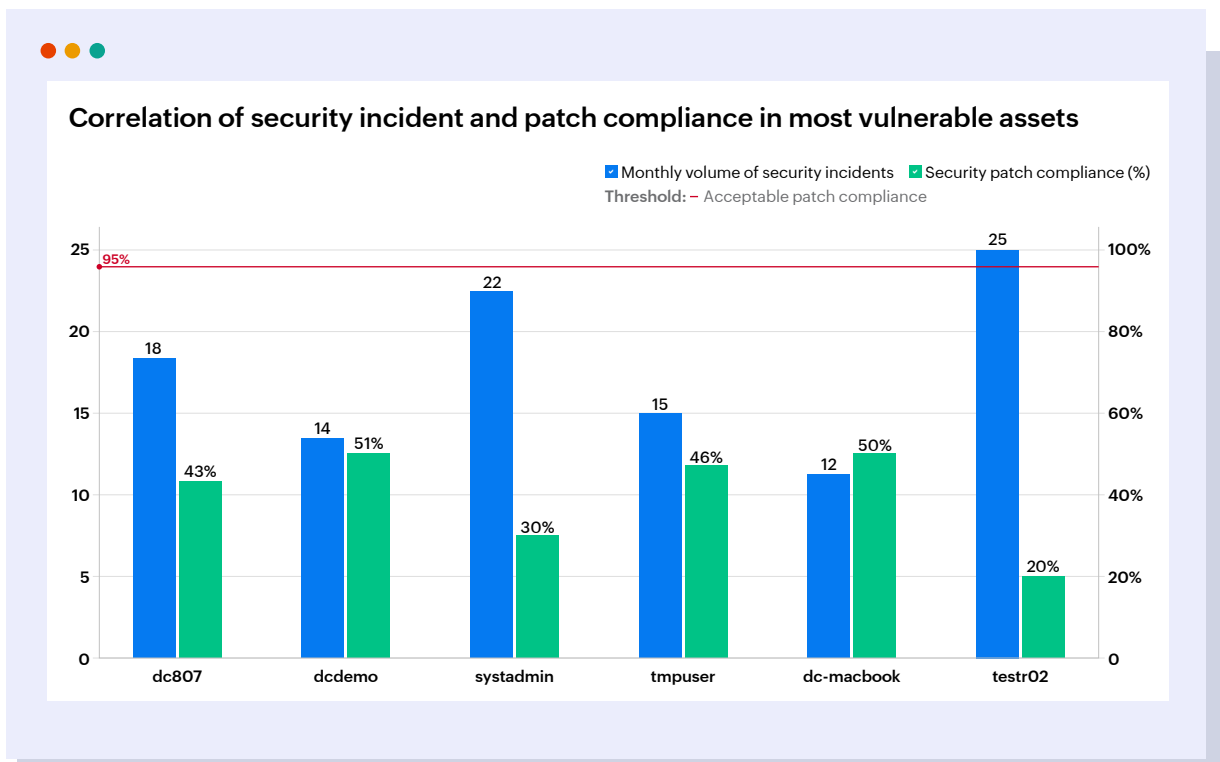
04

Accelerating incident resolution with cross-correlation

When an organization detects a security incident within its IT landscape, resolving it quickly becomes the top priority. However, the urgency to act when critical systems are compromised and sensitive data is at risk often leads to hasty, surface-level analyses that address only symptoms rather than the underlying cause. This approach can result in recurring incidents or even allow the issue to spread stealthily to other areas, eventually leading to newer, more severe problems.

The key to permanently and effectively eliminating a threat lies in conducting a thorough root cause analysis. Unfortunately, many organizations shy away from this approach due to the time-consuming nature of traditional methods. A comprehensive root cause investigation involves a detailed, step-by-step examination of each module in the IT infrastructure, which can take hours or sometimes days. While this process is critical for identifying the true cause, it may not always seem feasible when operations are at a standstill and the clock is ticking.

For example, consider an organization's most vulnerable assets, frequently subjected to security incidents. A quick analysis might reveal low patch compliance as the primary issue.



This visualization illustrates the initial analysis wherein high incident rates are attributed to low patch compliance, leading to a focus on immediate deployment of missing patches and implementation of more rigorous and regular auditing to ensure ongoing patch compliance for these devices.

While this approach might appear to resolve the incident for the time-being, it often fails to address the underlying problem in the long run. Even after implementing such ad-hoc patch compliance remedies, the incidents may persist, spreading in terms of coverage, frequency, and impact. This indicates that the initial analysis did not uncover the root cause of the problem.

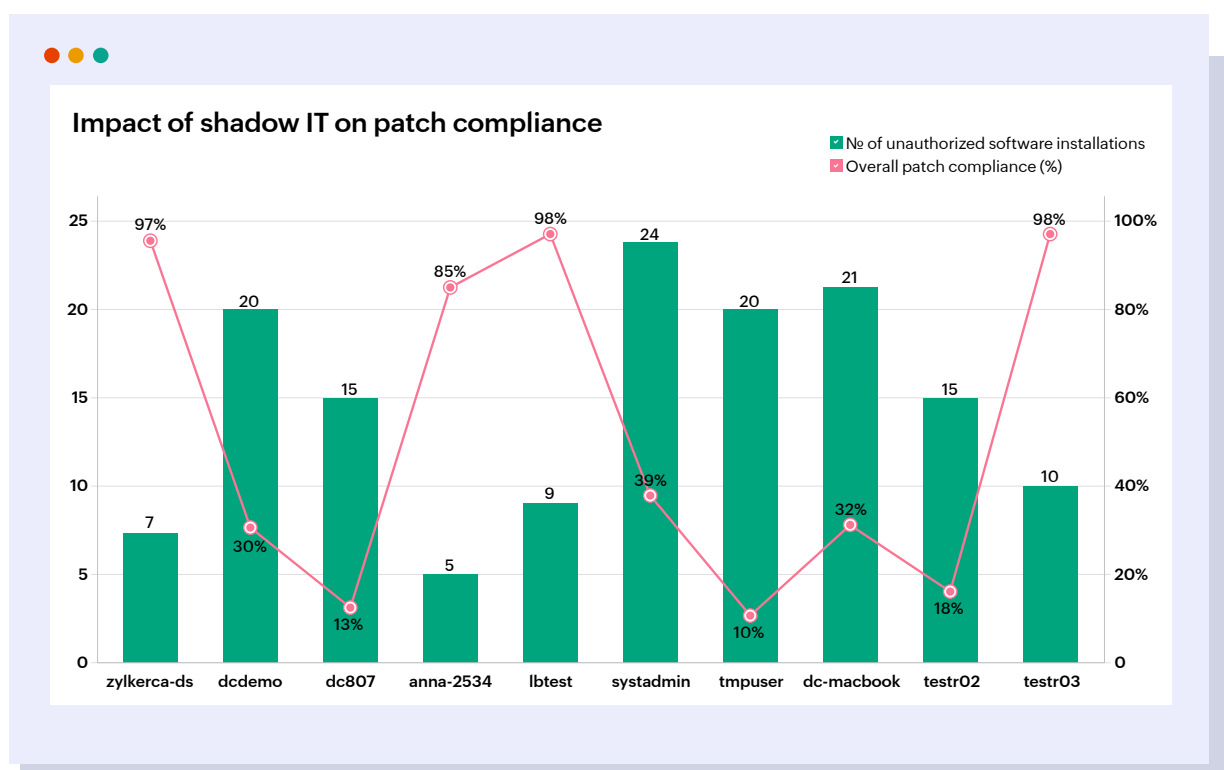
Without digging deeper into the root cause, IT teams might never uncover the true resolution for the issues affecting these assets.

The power of cross-correlation in incident root cause analysis

Cross-correlation of data across multiple IT systems and tools enables a more thorough root cause analysis, leading to a faster and more reliable resolution for security incidents. By examining data across various tools and applications running in the IT environment, such as the service desk, endpoint manager, operation manager, application manager, and security applications, in a single, comprehensive window, organizations can identify hidden relationships and uncover deeper security issues that a surface-level analysis might miss.

Circling back to the case of the most vulnerable endpoint assets, it is evident from our previous analysis that low patch compliance was seemingly the primary cause of the high incident rate. However, to understand the issue fully, security teams need to dig further and apply the highly effective *five whys* framework for a deeper, more rigorous root cause analysis.

It is recommended to investigate why patch compliance is low for just these assets, when most other assets meet the expected compliance levels. By correlating data from the service desk and endpoint management tools, the investigation reveals the underlying issue—shadow IT.



This visualization demonstrates how cross-correlation reveals deeper connections between the endpoint security incident rate and shadow IT practices that were not apparent in the initial analysis.

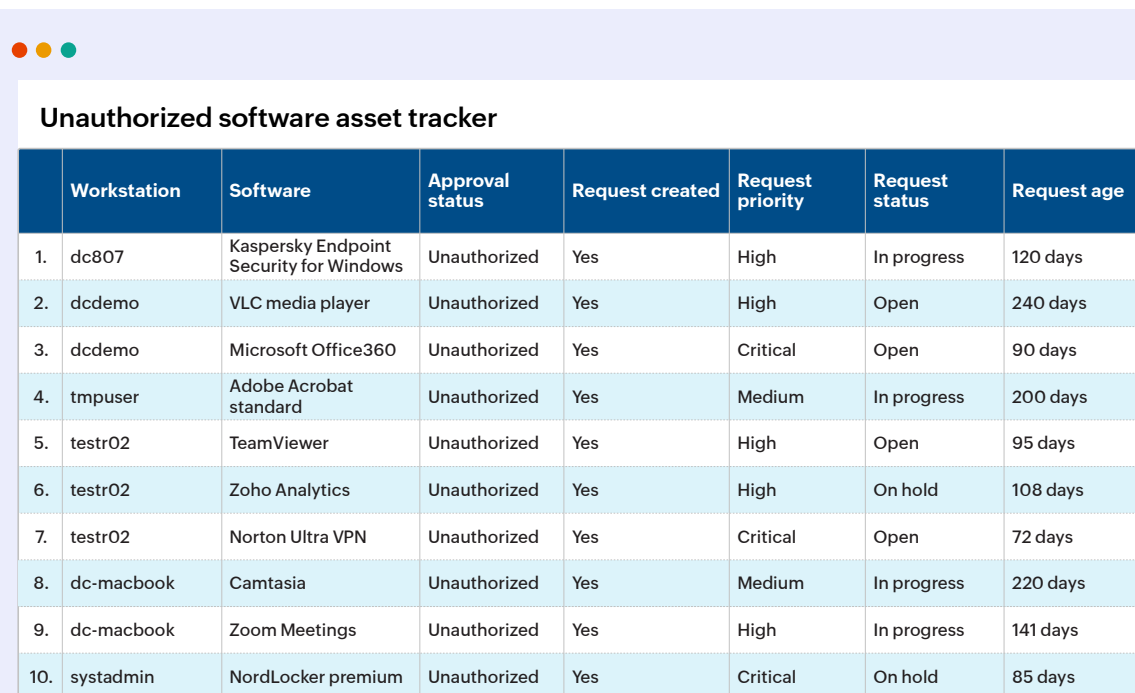
From this analysis, you can observe that for certain assets, the patch compliance percentage was low because there was a higher number of unauthorized software installations not covered in the patch deployment policy. Though the patches for authorized software were up to date in these assets, the existence of unauthorized software kept patch compliance low.

Further investigation is needed to understand the reason behind the extensive usage of unapproved software, especially on these vulnerable assets. These devices not only lack proper patch compliance but also show high levels of shadow IT installation and usage.

Understanding the relationship between shadow IT and asset management

The issue of shadow IT often stems from inefficient asset management practices. When employees feel that existing IT systems and tools are too inadequate or slow to meet their needs, they may turn to unauthorized alternatives to get their work done. This can be indicated by a mounting volume of service requests, extended time to fulfill these requests, and a decline in overall productivity.

By carefully analyzing the data from asset management systems and endpoint applications, IT teams can discover that the fulfillment process for new, high-priority software requests has been extremely delayed. This in turn leads to a high number of unfulfilled requests, mounting ticket volumes, and a subsequent increase in security incidents due to decreasing patch compliance.

A screenshot of a web application window titled "Unauthorized software asset tracker". The window has a light blue header and a white table area. The table has 8 columns: an index column, Workstation, Software, Approval status, Request created, Request priority, Request status, and Request age. It contains 10 rows of data, all showing unauthorized software with varying request ages and statuses.

	Workstation	Software	Approval status	Request created	Request priority	Request status	Request age
1.	dc807	Kaspersky Endpoint Security for Windows	Unauthorized	Yes	High	In progress	120 days
2.	dcdemo	VLC media player	Unauthorized	Yes	High	Open	240 days
3.	dcdemo	Microsoft Office360	Unauthorized	Yes	Critical	Open	90 days
4.	tmpuser	Adobe Acrobat standard	Unauthorized	Yes	Medium	In progress	200 days
5.	testr02	TeamViewer	Unauthorized	Yes	High	Open	95 days
6.	testr02	Zoho Analytics	Unauthorized	Yes	High	On hold	108 days
7.	testr02	Norton Ultra VPN	Unauthorized	Yes	Critical	Open	72 days
8.	dc-macbook	Camtasia	Unauthorized	Yes	Medium	In progress	220 days
9.	dc-macbook	Zoom Meetings	Unauthorized	Yes	High	In progress	141 days
10.	systadmin	NordLocker premium	Unauthorized	Yes	Critical	On hold	85 days

This line of analysis can help organizations identify gaps in their asset management practices, whether in procurement, licensing, approval, or deployment. Armed with this knowledge, they can take necessary steps to ensure timely asset availability and reduce the risk of shadow IT, and in turn, mitigate security incidents effectively.

As seen in the above analyses, cross-correlation of data from multiple IT tools enables an accelerated and thorough approach to identifying the root cause of security incidents. This comprehensive analysis helps organizations uncover hidden issues and implement more effective solutions. In addition to allowing security teams to resolve incidents quickly, this approach prevents recurring incidents and limits the spread of incidents across the organization's interconnected IT environment—a critical capability for maintaining a strong IT security posture.

Conclusion

Cyberthreats and threat actors are rapidly evolving, becoming increasingly sophisticated with each passing day. Traditional security measures and strategies are no longer sufficient to address this modern, ever-changing threat landscape.

By incorporating advanced analytical techniques such as real-time automated anomaly detection, AI-powered user behavior analysis, clustering, and cross-correlation, organizations can fortify their cybersecurity strategies against advanced threats. These emerging techniques can enhance threat detection, enable more effective threat response, and provide a proactive approach to future-proofing and safeguarding an organization's IT infrastructure, ultimately improving overall cyber resilience.

About

ManageEngine Analytics Plus is an IT analytics and decision intelligence solution designed to provide organizations with a unified view of their IT operations, correlate interdependencies and derive meaningful insights. It breaks down data silos by consolidating both on-premises and cloud infrastructure KPIs. Analytics Plus measures the efficiency of network operations, tracks the responsiveness and availability of business applications, evaluates technician performance, assesses the progress of processes, and flags security anomalies. This comprehensive analysis is achieved by connecting to all IT software that forms the backbone of an IT infrastructure. These consolidated insights enable organizations to make data-driven decisions that enhance operational efficiency and drive business success.

Kick-start your IT analytics journey with a free trial of Analytics Plus.

Want to learn more about the product before giving it a try?

Sign up for a free, virtual tour with one of our solution experts.



Reference

1. <https://cybersecurityventures.com/cybersecurity-spending-2021-2025/>
2. https://www.weforum.org/publications/global-cybersecurity-outlook-2024/?utm_source=google&utm_medium=ppc&utm_campaign=cybersecurity&gad_source=1&gclid=CjwKCAjw8fu1BhBsEiwAwDr5jB0sjfAPt-rX9p_lzRlnDLy_yLbcBdCrG0HWGgkCRW8DMDlig0S9kxoCPwsQAvD_BwE
3. <https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-1h-2023.pdf>
4. <https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-The-Cyber-Resilient-CEO-Final.pdf#zoom=40>
5. <https://financialpost.com/globe-newswire/intrusion-research-shows-confidence-in-teams-and-technologies-to-thwart-cyberattacks-yet-cyber-breaches-still-commonplace-suggesting-false-sense-of-security>
6. <https://www.manageengine.com/log-management/ebooks/cloud-security-outlook-2023.html?types-of-logs?success=yes>
7. https://www.thalesgroup.com/en/worldwide/defence-and-security/press_release/cloud-resources-have-become-biggest-targets



© ManageEngine, a division of Zoho Corporation