

# KEY METRICS THAT SHOULD BE PART OF YOUR CYBERSECURITY DASHBOARD

- Identify critical security metrics across diverse facets of IT

# Table of contents

■ Introduction	3
■ Endpoint security	4
■ Network security	8
■ Privileged access management	10
■ Identity and access management	13
■ Consolidated security dashboard	16
■ About	18

# Introduction

**S**ecurity has consistently held significance within IT and its importance has steadily increased over time. The traditional method of relying on a specialized security team to identify vulnerabilities and offer recommendations to production teams has evolved. Every area of IT has a security aspect to it, covering the entire lifecycle of your hardware, software, people and network.

Implementing an extensive array of metrics to oversee security isn't a practical or scalable approach, especially considering the diverse facets of IT, such as endpoint security, privileged access management, network access, and identity management. A more efficient strategy involves selecting key metrics from each of these areas to create your ideal IT security dashboard. The selected metrics should encompass the fundamental aspects that demand constant attention throughout the entirety of the IT landscape, leaving no room for compromise under any circumstances. Minor deviations in these key metrics can serve as indicators of potentially significant issues.

In this e-book we will discuss key metrics from the following aspects of IT and build a consolidated view of IT security with some tips on how you can combat security threats.

## 01 Endpoint security

## 02 Privileged access management

## 03 Network and application security

## 04 Identity and access management

ManageEngine Analytics Plus, an IT analytics software, has several fundamental aspects at its core that facilitates a consolidated view of IT. These functionalities are invaluable to IT security teams:

- Gather data from all relevant IT sources.
- Display complex statistics in an easy-to-digest format.
- Highlight hidden and less-tangible signs of infiltration, vulnerabilities, and security gaps.

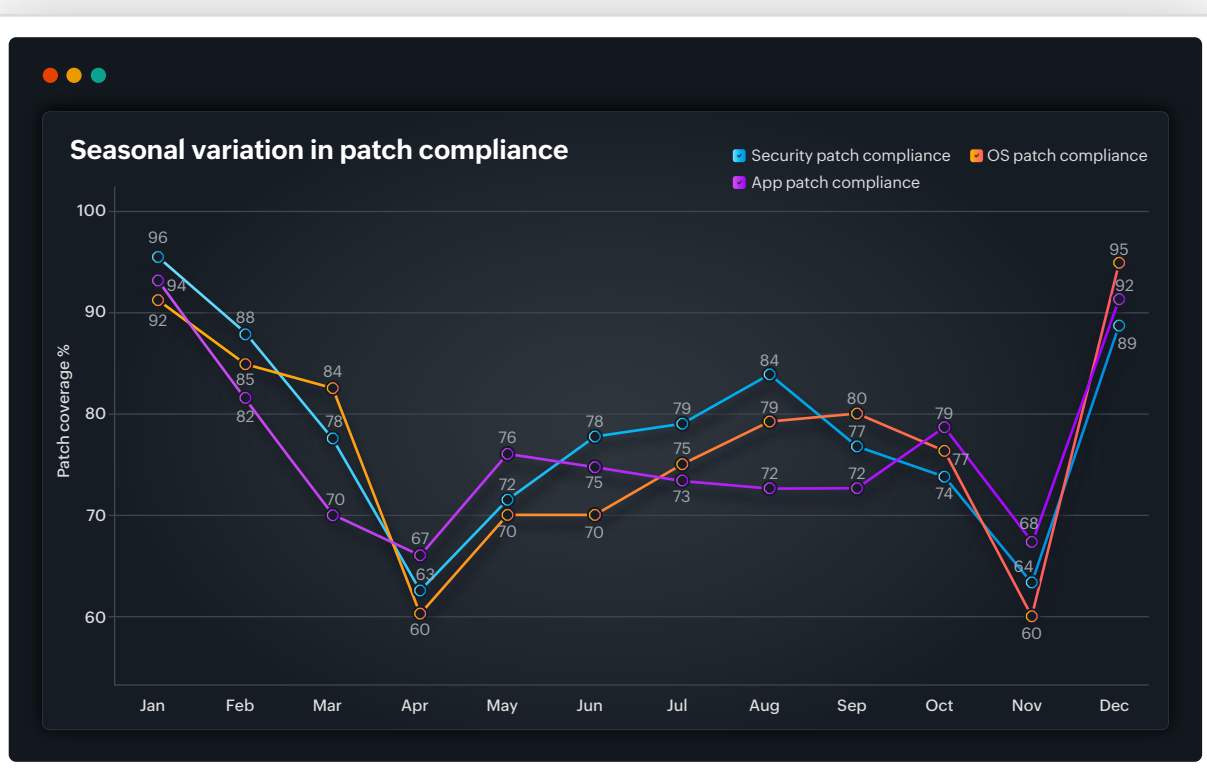
These qualities make ManageEngine's IT analytics software the ideal candidate to build your SOC or SecOps dashboards.

# 01

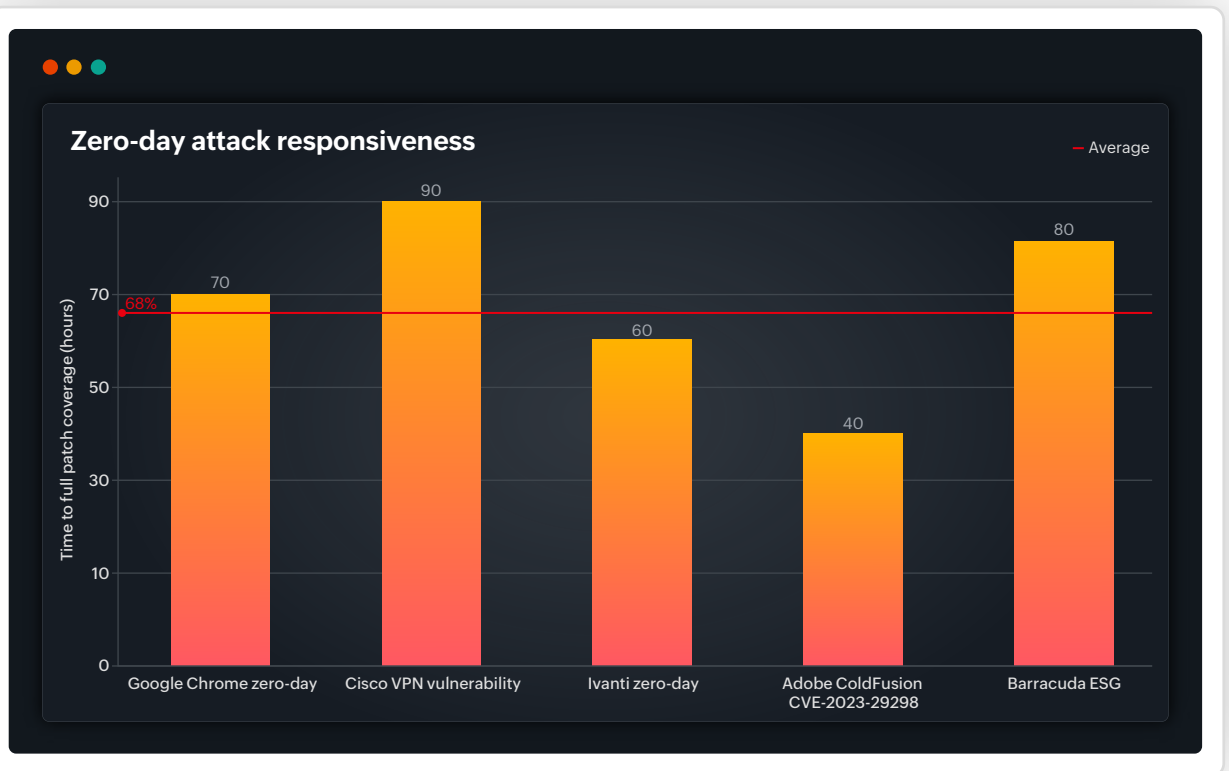
## Endpoint security

Ensuring endpoint security is one of the most fundamental and straightforward things organizations can do, but ironically, most successful security breaches occur due to vulnerabilities at an endpoint level. Patch compliance is a key component in ensuring the security of an organization. However, most organizations look at the overall patch compliance percentage at a given point of time, and fail to track it as a trend over time.

Tracking compliance as a trend is important because endpoint patching is an ongoing and continuous process, rather than a one-time activity. Organizations need to be wary when their compliance takes a dip and also establish patterns in its upward or downward movement. Recognizing these patterns helps in establishing reasons behind the lapse and can aid in realigning specific processes that cause the patch compliance to deteriorate.

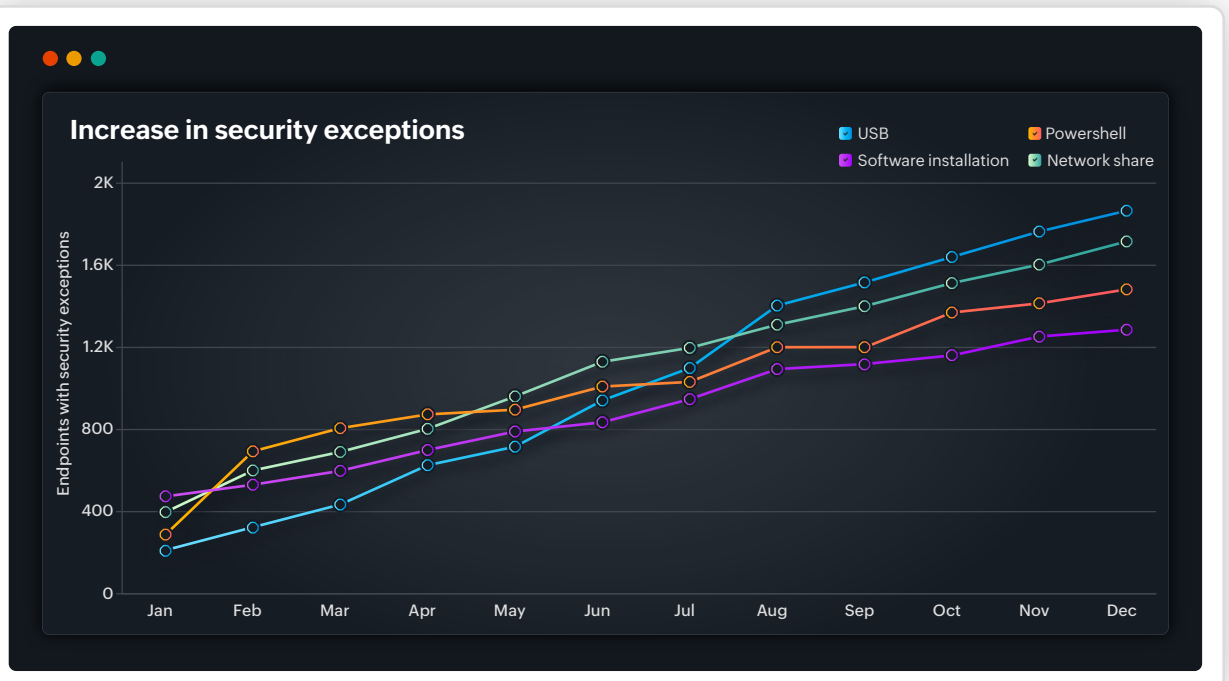


Zero day attacks throw a wrench in an organization's patch schedules, as they require organizations to put other priorities aside and ensure security patches are pushed as soon as possible in order to mitigate exposure to an ongoing attack. It is essential for organizations to measure how long they need to complete 100% coverage while deploying critical and time-sensitive patches. Security teams should track and aim to constantly improve their response time in mitigating exposure to zero day attacks, as every passing minute counts.

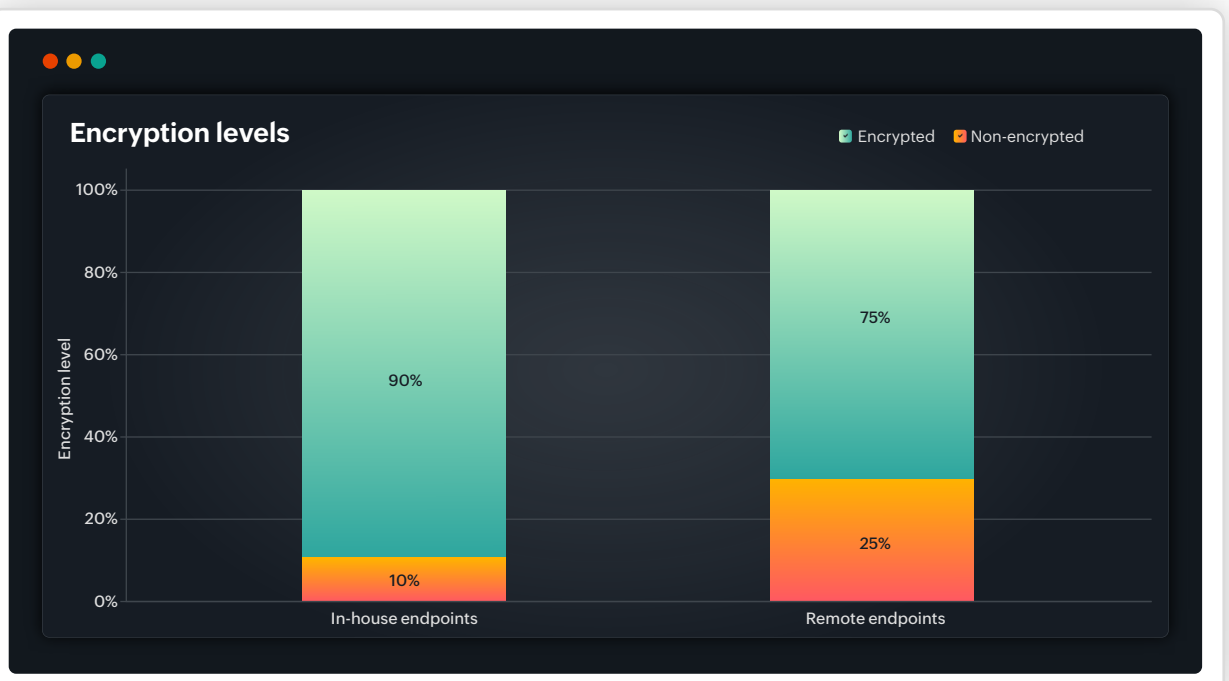


**Tip:** ManageEngine Analytics Plus allows security teams to embed live security feeds from the internet that allow IT admins to get instantly notified of zero day attacks. These feeds can be embedded in existing security dashboards or security teams can set up dedicated dashboards to watch live feeds.

Once we have the bases covered with ensuring a consistent patch compliance percentage, the next order of business is plugging other aspects of an endpoint that serve as usual entry points for malicious software. There is an array of various restrictions that organizations set up on an endpoint, including disabling software installations, restricting USB access, and restricting Powershell access, in an effort to close the common entry points used by hackers. However, due to business requirements, there is always a portion of the endpoint inventory that do not have these restrictions. Organizations should ensure that the percentage of endpoints that are exceptions doesn't exponentially increase over time. That provides a larger surface area for infiltration.



If security measures fail and a breach is established, an encrypted hard disk ensures confidential data isn't exploited. In a post-breach scenario, an encrypted hard disk ensures organizations from losing customer trust, as the customer's data is protected and cannot be used by hackers for financial gain. Ensuring a healthy encryption status is necessary, especially on devices that are not always connected to the primary network, which has all the essential restrictions in place.





**Tip:** Analytics Plus allows teams to set up dynamic thresholds based on KPIs such as percentage of endpoints without encryption or restrictions. This allows security teams to be notified when the volume of such endpoints reaches unintended levels.

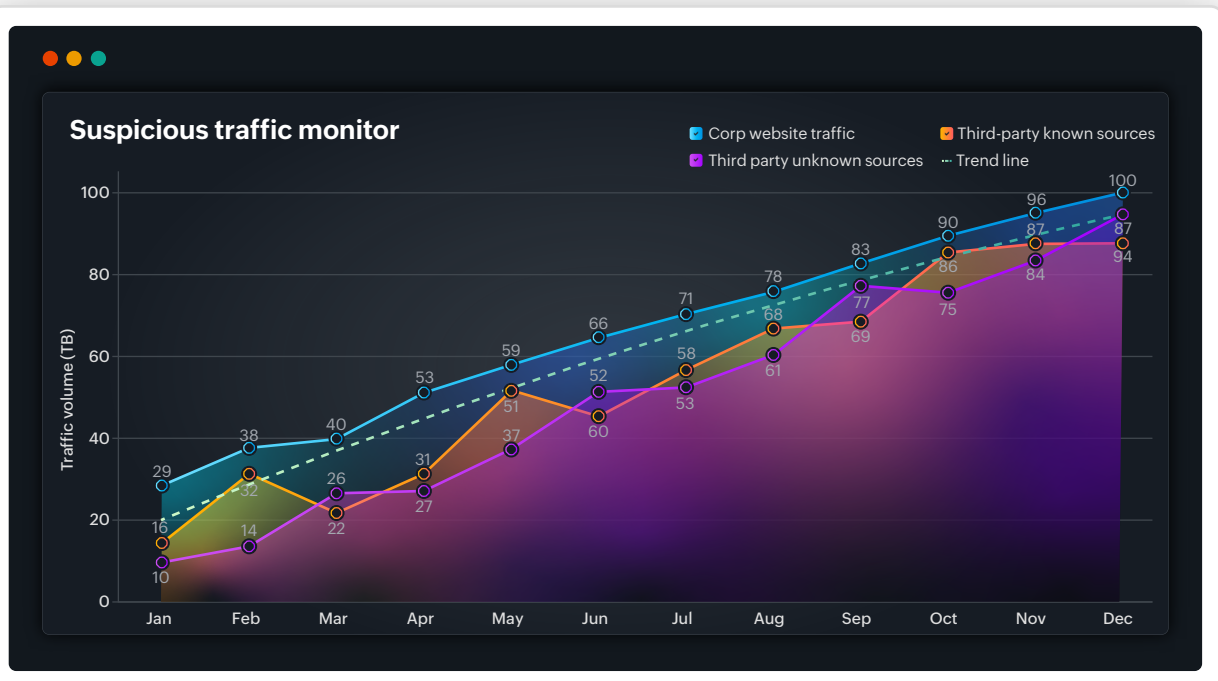
## 02

# Network security

Outside of insider attacks, nearly every other form of security breach can be traced to the network or internet. It's imperative that security teams keep close control over what makes it through the network. While most companies regulate what users can access on the internet, it is impossible to create a database of every malicious website and block access to them. Also, security teams can set up anomaly detectors to catch unusual traffic flowing through the network. These can serve as the first sign of unintended activity in the network.

Security teams should also account for a natural increase in web traffic when the business expands and shouldn't treat every increase in network traffic as an outlier. A good practice is to look at traffic metrics in conjunction with events that point to infrastructure expansion. An example of an infrastructure expansion is the addition of new endpoints due to an increase in head count.





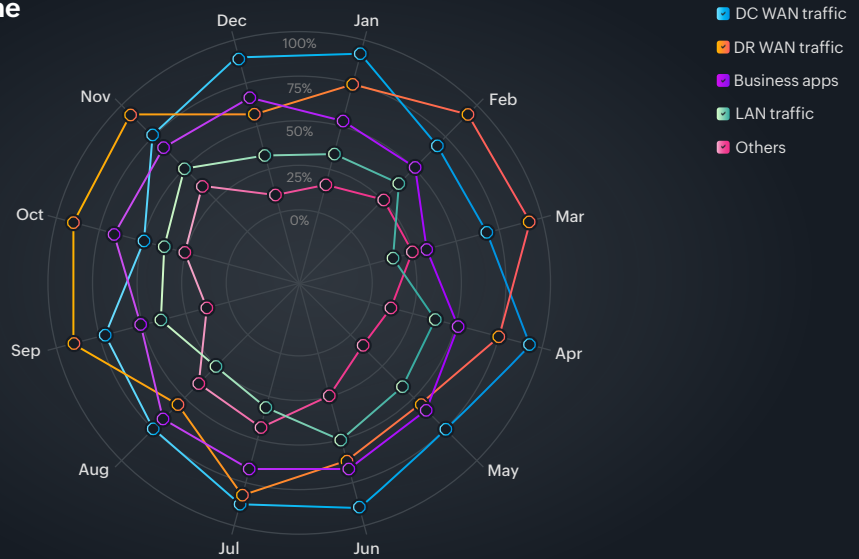
**Tip:** Security teams can use machine learning to set up a baseline for traffic flow and anomaly detection. While setting this up, ensure high traffic nodes are treated as exceptions so they don't show up as false-positive spikes in traffic.

Security teams should monitor unusual spikes in network traffic and ensure most of the traffic flowing through the network is encrypted. Encrypted traffic is a good fail-safe in a post-hack scenario where a hacker has established successful packet sniffing, but cannot make sense of any of the data due to the encryption. Though its practically impossible to encrypt every piece of traffic flowing in-and-out of the network, security teams should aim at enforcing HTTPs protocol on all business critical applications.



**Tip:** Flow analyzers (Netflow, Jflow, Sflow, etc.) are a good source of information to get details on the volume of traffic that is encrypted. Analytics Plus can pull aggregated data from flow analyzers and bifurcate encrypted and non-encrypted traffic to show a true sense of the volume of encryption. Security teams can use this information to take necessary action to increase the percentage of traffic that is encrypted.

Encryption volume

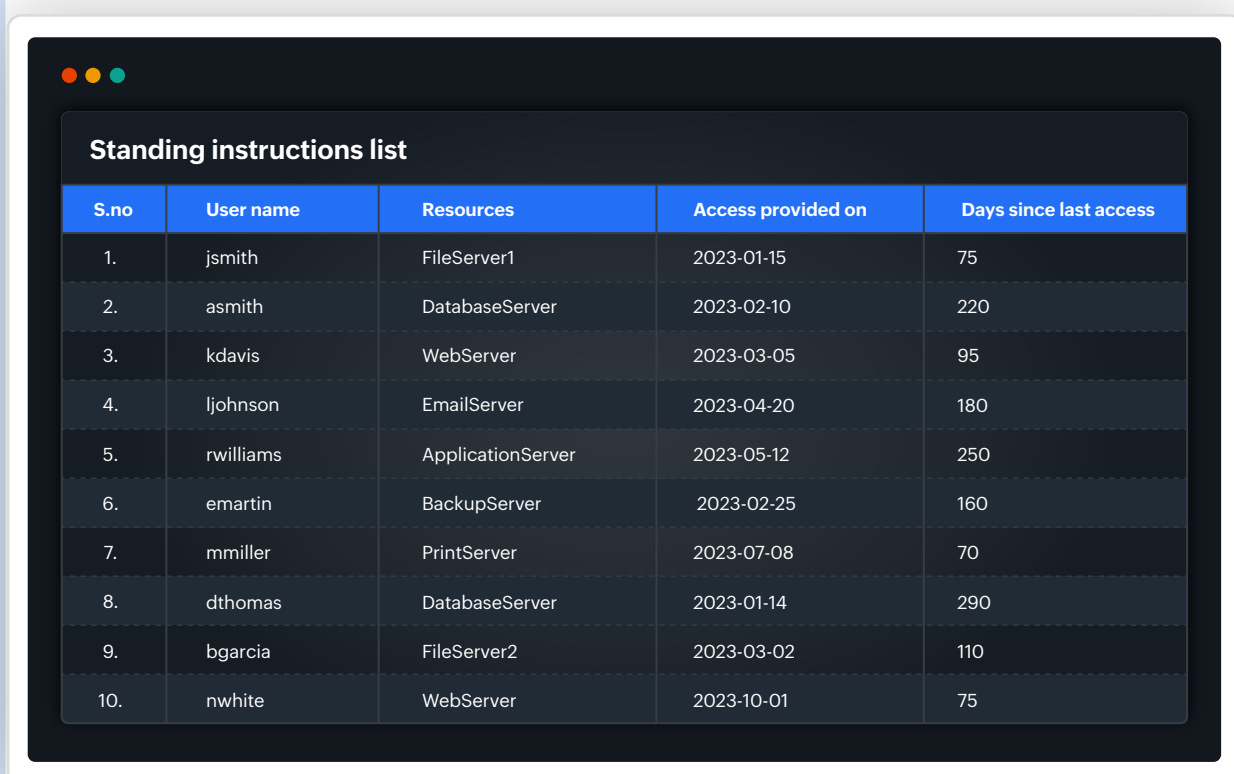


## 03

# Privileged access management

Privileged accounts need special attention due to their sensitivity and the compounding consequences in the event of a security breach. It's usually not the lack of processes or security measures that leads to a privileged account breach. Instead, it's the failure in adhering to the rules put-forth. This essentially implies that even with a meticulously designed protocol, the organization's vulnerability increases significantly if these guidelines are not strictly adhered to.

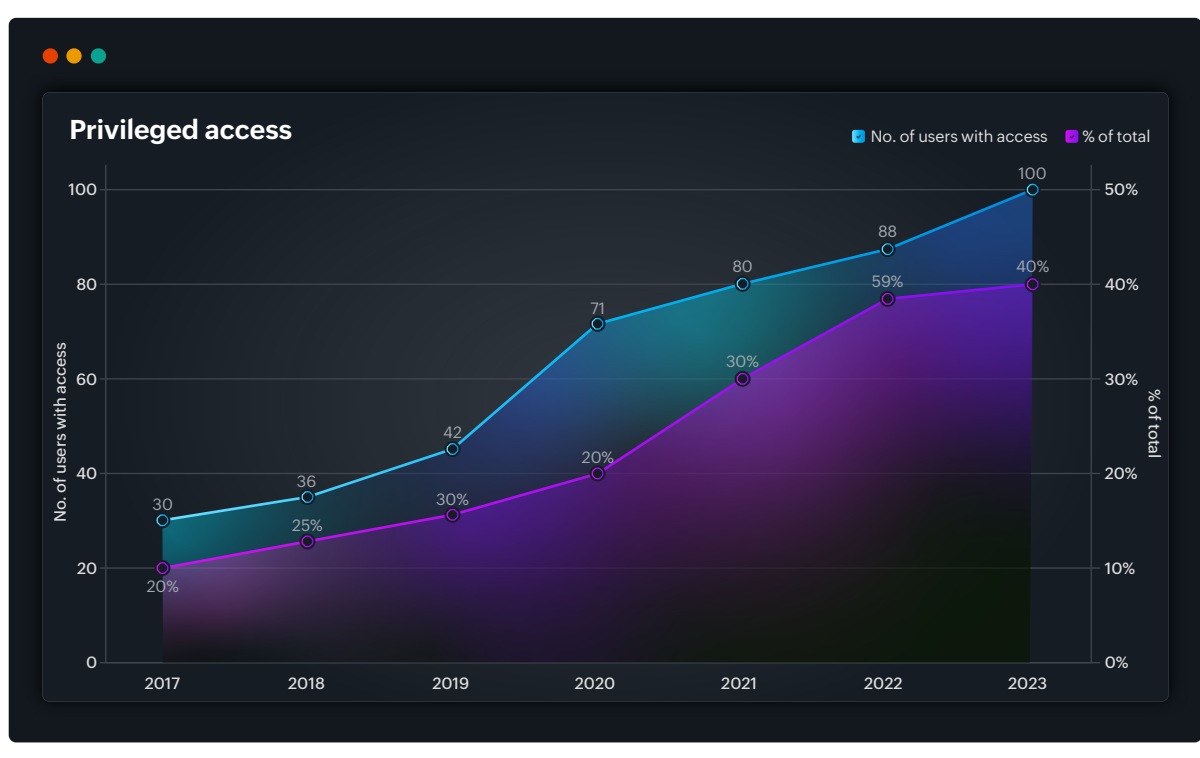
The recommended approach to handling privileged access is monitoring and verifying privileged access usage patterns, starting with ensuring access is available only to users who require it and are actively using it. While privileged access management (PAM) applications offer the option of providing time-based access to users, admins tend to provide access to sensitive accounts without those restrictions. The following analysis shows the list of users who've gone months without using their access to privileged accounts. Security teams should conduct periodic reviews of this list to ascertain the necessity of such access for these users.



The screenshot shows a window titled 'Standing instructions list' with a table containing 10 rows of user access data. The table has five columns: S.no, User name, Resources, Access provided on, and Days since last access. The data is as follows:

S.no	User name	Resources	Access provided on	Days since last access
1.	jsmith	FileServer1	2023-01-15	75
2.	asmith	DatabaseServer	2023-02-10	220
3.	kdavis	WebServer	2023-03-05	95
4.	ljohnson	EmailServer	2023-04-20	180
5.	rwilliams	ApplicationServer	2023-05-12	250
6.	emartin	BackupServer	2023-02-25	160
7.	mmiller	PrintServer	2023-07-08	70
8.	dthomas	DatabaseServer	2023-01-14	290
9.	bgarcia	FileServer2	2023-03-02	110
10.	nwhite	WebServer	2023-10-01	75

In general, it's good practice to minimize the amount of users who have access to privileged accounts and keep the footprint exposure low. Keep an eye on the volume of users who end up having access to privileged accounts. Substantial increases in this volume could be detrimental to the organization in the longer run.

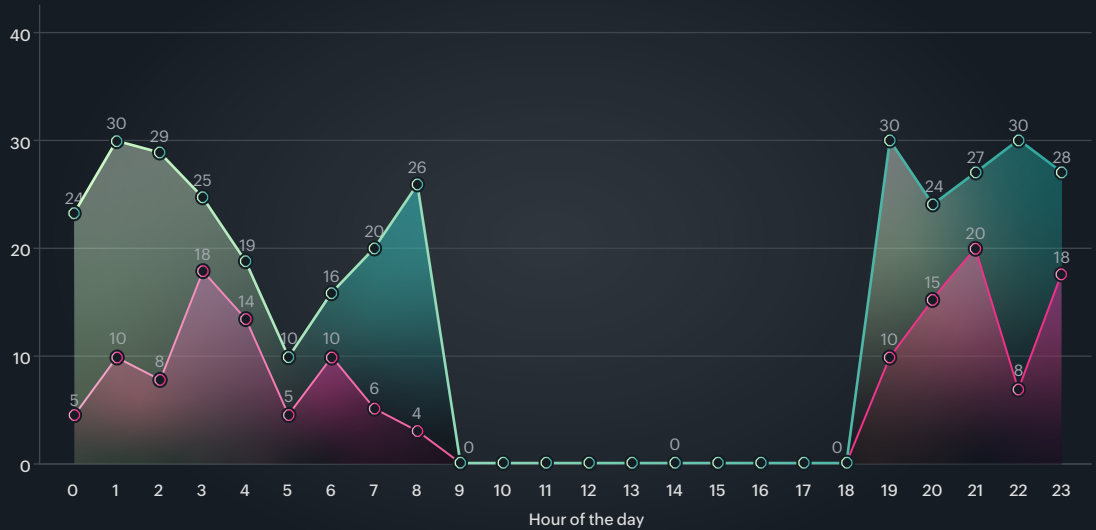


Besides protecting access to privileged accounts, security teams should monitor the reasons why users establish remote connections to endpoints and the time-frame when they do so. Access to critical resources during unusual or non-business hours should be treated as anomalies and investigated to establish valid reasons.



### Non-business hour access

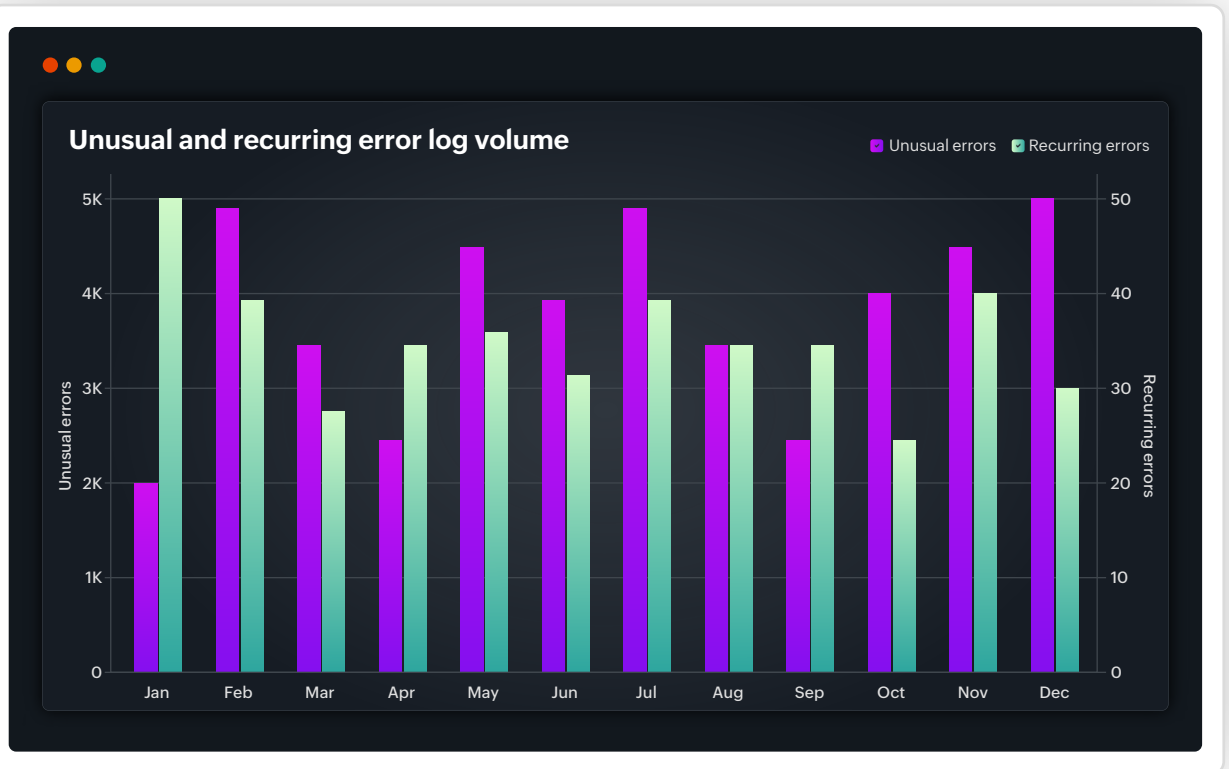
Resources accessed SSH sessions



## 04

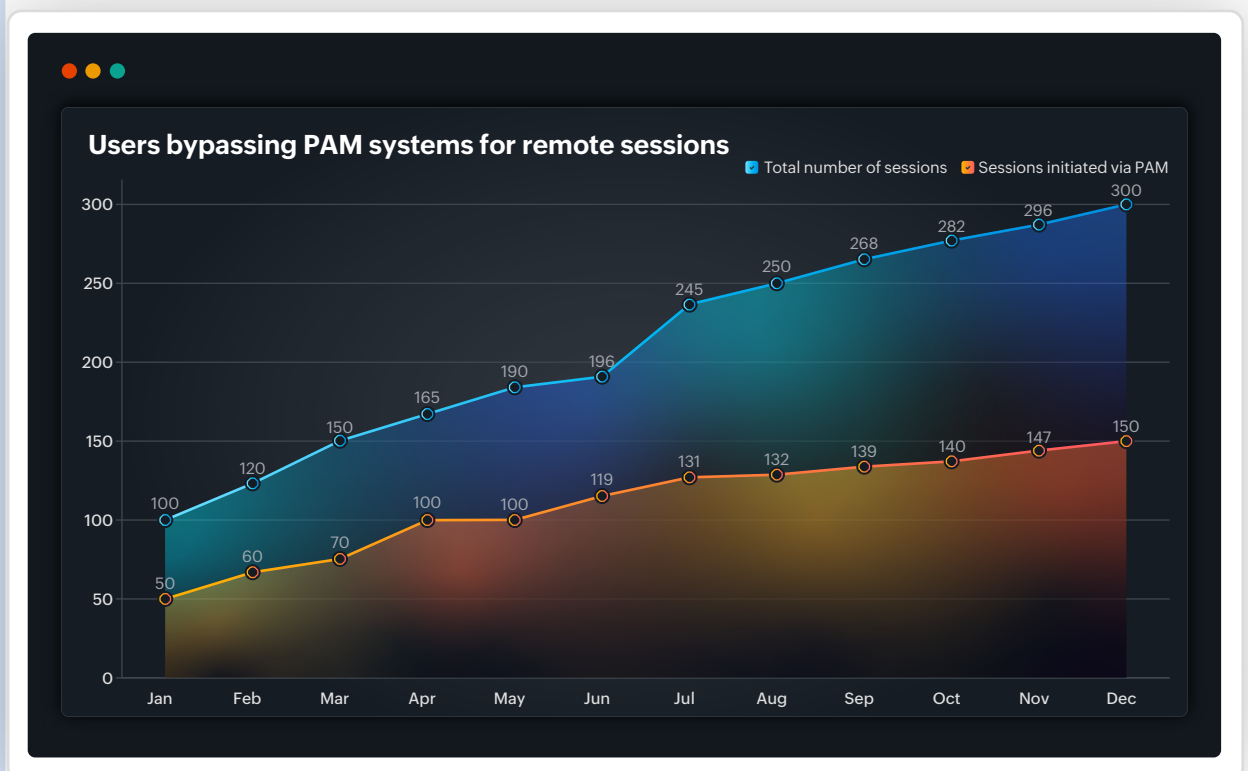
# Identity and access management

It's common knowledge that system logs are a great way to dissect and trace back the origin of a security breach. This also means that there are always tell-tale signs of an impending or an ongoing breach in the system logs. The biggest problem, however, is not knowing which specific error to look for. IT analytics solutions like Analytics Plus can be tuned to look for and flag spikes in unusual and recurring error logs, thus notifying you of potential issues that need to be analyzed. This approach casts a wider net, but security teams can gradually see patterns over time and zero-in on specific error codes that point to more serious risks.



Given the various ways to gain access to corporate data, it is no wonder that it is common practice for security to deploy several different tools to protect against all points of entry. This also gives rise to a challenging problem of data fragmentation within each of these specialized tools, which can be incredibly powerful when combined. IT analytics solutions are very handy when it comes to correlating data from two or more different sources. This aspect can be useful when you are looking to catch security flaws. One example is catching users who establish remote connections to endpoints without going through a PAM tool. This is also an example of the scenario we discussed in the previous section, where users don't adhere to security protocols laid out by the security team.

By comparing the number of remote sessions initiated through PAM systems with the total number remote sessions initiated to endpoints (which can be detected by looking for specific eventlogs or syslogs from the event monitoring systems), one can quickly derive the number of sessions established by bypassing PAM systems. This data also includes user information and it can be used to reach out to users who exhibit this behavior repeatedly and eventually put an end to this practice altogether.



A big gap in the total number of sessions and sessions initiated via PAM is an indicator to block access to direct remote sessions initiated from user's endpoints without going through PAM systems.



**Tip:** System logs are a rich source of information, which can be used to detect several other events that are signs of concern in a secured network. They haven't been covered in this e-book extensively due to sufficient awareness around such events among security personnel. Following are a few metrics that have sufficient importance:

- *Failed logons*
- *Failed password resets*
- *Incorrect password retries*
- *Volume of inactive user accounts*
- *Volume of users whose passwords don't expire*
- *Number of user modifications*

## Consolidated security dashboard

We've discussed key metrics in the various surface areas in which threat actors try to infiltrate an organization's sensitive and confidential data. IT analytics solutions such as Analytics Plus allow security teams to consolidate all this data into a unified security dashboard. These dashboards can serve as a window into possible signs of infiltration and can also help build awareness among the larger audience in the organization to take security seriously. IT analytics solutions allow the seamless incorporation of data from any IT source, making it the ideal candidate for consolidating security metrics. Analytics Plus also converts this data into easily digestible visual formats.





Zero-day  
responsiveness

30 hrs

Un-encrypted traffic

25%

Last quarter: 20%

Account access  
anomaly

34%

Last 24 hours: 41%

Error events

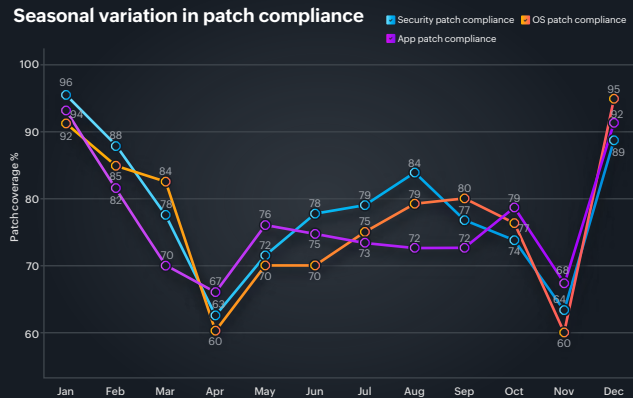
6K

Yesterday: 3K

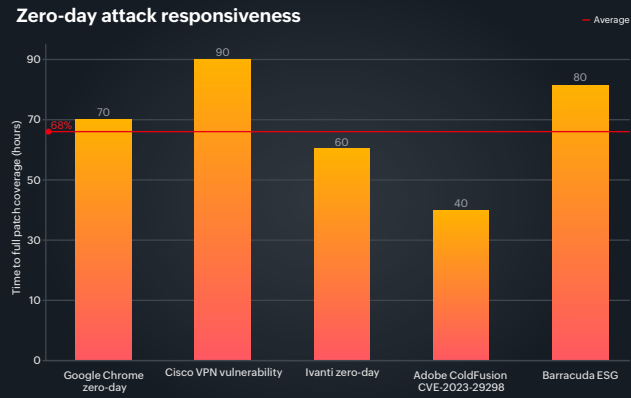
Security posture

Medium  
Risk

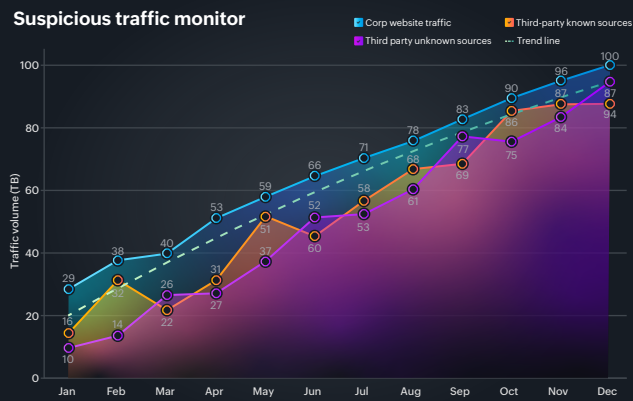
Seasonal variation in patch compliance



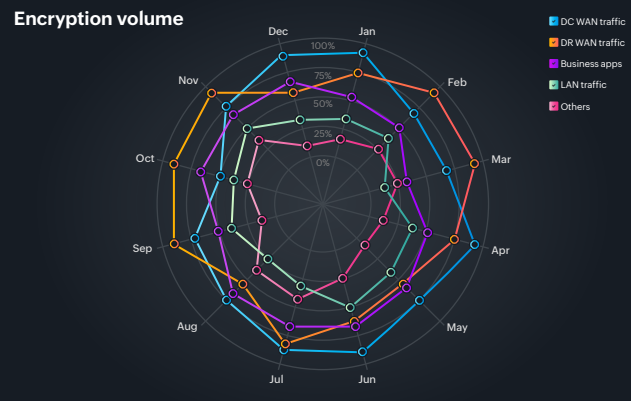
Zero-day attack responsiveness



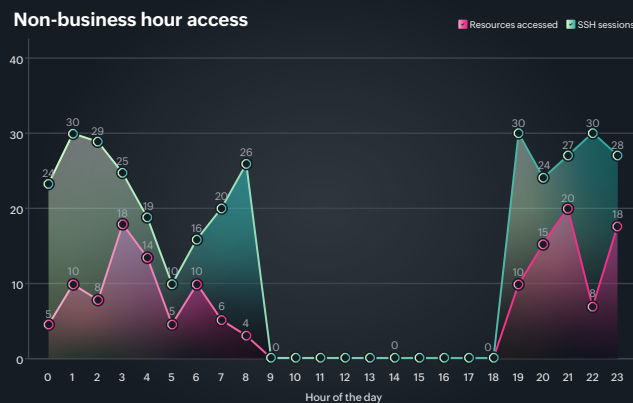
Suspicious traffic monitor



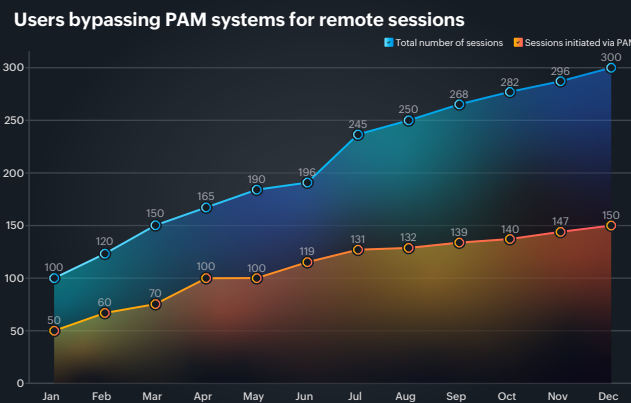
Encryption volume



Non-business hour access



Users bypassing PAM systems for remote sessions



# About

**ManageEngine Analytics Plus** is a self-service, AI-driven IT analytics solution that helps organizations implement complex initiatives that address requirements of expanding businesses. Available on-premises and on the cloud, Analytics Plus visualizes IT data from several applications and integrates out-of-the-box with several popular IT applications such as ManageEngine ServiceDesk Plus, Jira, Service Now, Zendesk, and ManageEngine Endpoint Central. Analytics Plus features an AI-powered analytics assistant that responds to voice and text prompts to provide meaningful visualizations. This eliminates the need for a data analyst to aid help desk managers and reduces report building time while enabling organizations to make faster, data-driven decisions.

**Kickstart 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.

**280K**  
customers  
across the world

**90+**  
products  
and free tools

**190+**  
countries  
served

**20+**  
years of IT  
management experience

**Analytics Plus** 

© ManageEngine, a division of Zoho Corporation