

# 05 **HIDDEN IT CORRELATIONS** YOU'RE OVERLOOKING

- Your ultimate guide to identifying critical dependencies for smarter IT operations.

# Table of contents

■	Introduction	3
■	Centralized dashboards for every IT need	4
■	Consolidated scores to assess security posture	8
■	Curb unauthorized RDP sessions to secure privileged accounts	11
■	Improve patch management to deliver better ITSM	13
■	Address asset utilization to improve IT budgeting	17
■	Conclusion	20
■	About ManageEngine Analytics Plus	21

# Introduction

Imagine trying to complete a puzzle with missing pieces—you can never truly solve it, and trying to guess the full picture is all the more difficult and time-consuming. This is the daily reality for IT teams, who work with fragmented data across security, operations, service desks, and network monitoring systems. The result? Inaccurate insights, reactive troubleshooting, and costly inefficiencies.

The modern IT landscape is more complex than ever. Organizations rely on dozens of specialized IT applications, each generating valuable data—yet these systems don't talk to each other. Security logs sit in SIEM tools, performance data is locked in infrastructure monitoring platforms, and service incidents reside in help desk applications. When IT teams try to solve a problem, they end up jumping between multiple applications and reports, trying to piece together a complete picture—often after the damage has already been done.

To break free from these challenges, IT teams need a smarter, data-driven approach—one that enables cross-functional correlation of IT data across disparate applications into a single unified window.

This e-book explores five key scenarios where cross-functional data correlation—enabled by AI-powered analytics—helps IT teams solve major challenges that traditional siloed tools cannot address. By leveraging hidden IT correlations, organizations can accelerate decision-making, deliver seamless services, and optimize operational efficiency.

# Centralized dashboards for every IT need

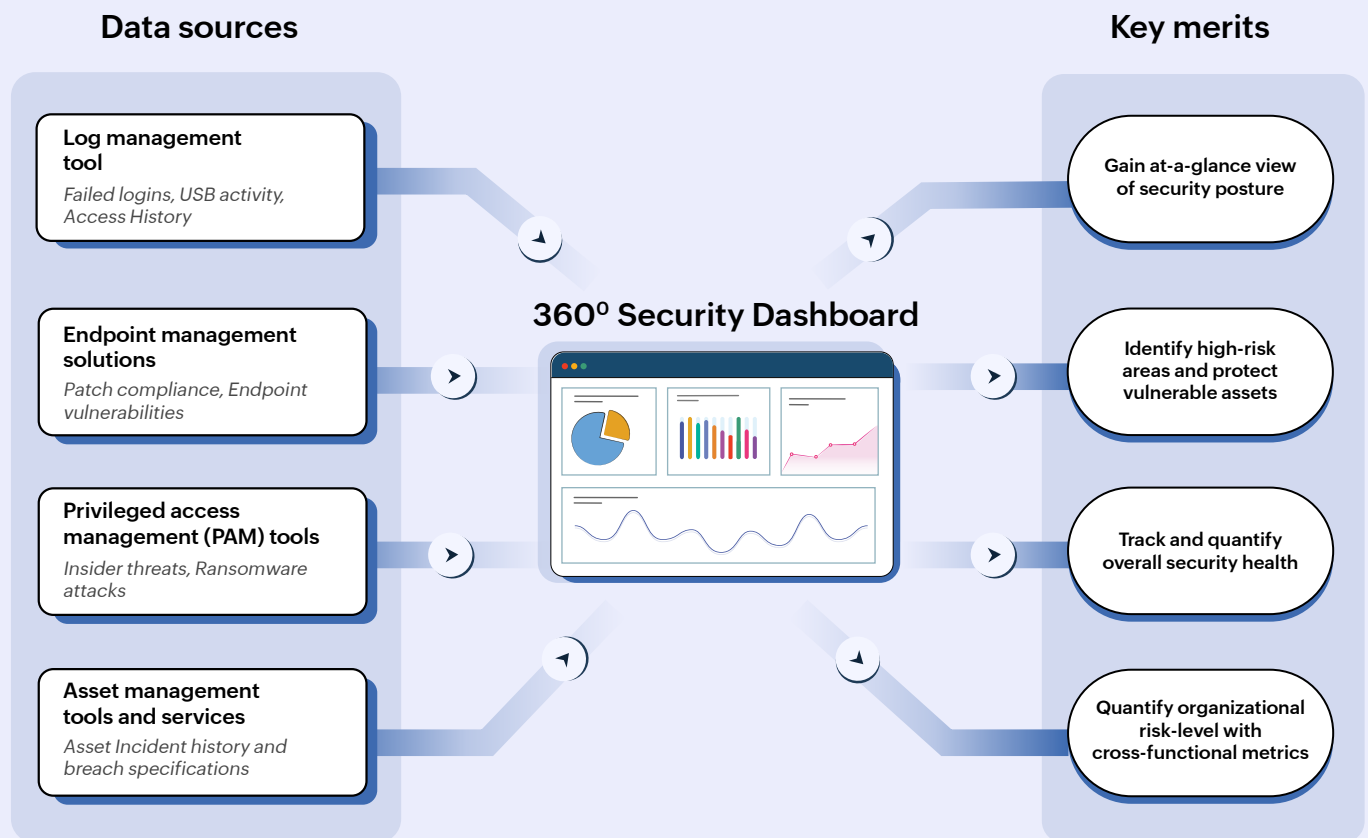
**IT** departments exist in a highly interconnected ecosystem where security, operations, and infrastructure continually influence one another. Delivering seamless operations mandates uncovering, and leveraging these dependencies. AI-powered analytics solutions enable this by correlating data from disparate tools and processes into powerful consolidated dashboards, providing a unified view of IT.

These dashboards can be built for every IT requirement, delivering real-time end-to-end insights.

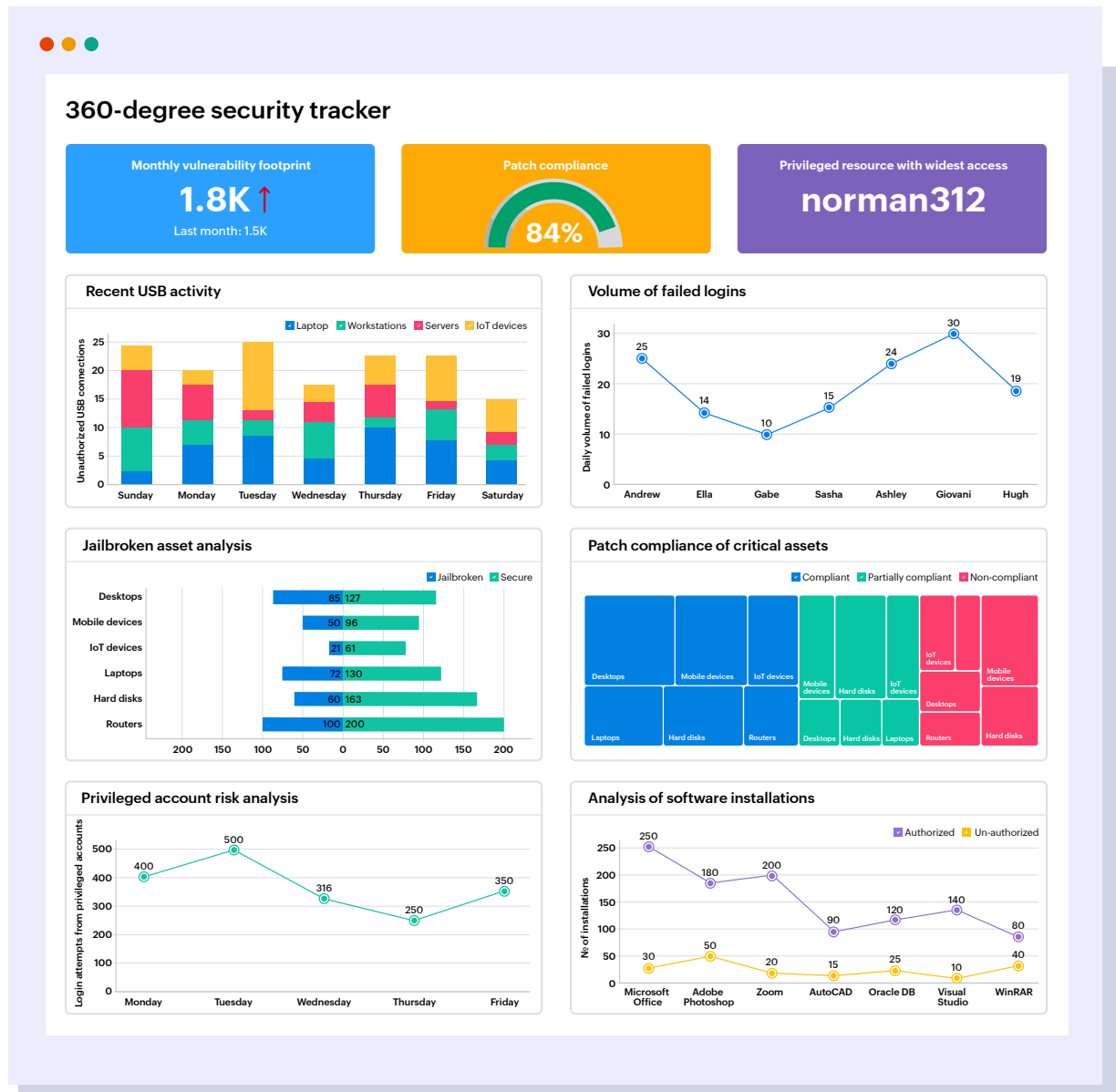
For instance, let's consider an organization's threat landscape, where there exists a relentless barrage of security risks. These risks—despite being interconnected—are often identified and monitored through multiple, disparate tools. This fragmented nature of IT operations often leaves security teams without a holistic picture of their security posture, hindering accurate, real-time risk assessment.

A 360-degree dashboard—which aggregates data from diverse IT tools into a unified view—offers a powerful solution. It acts as the foundation of proactive threat management by empowering IT teams to effortlessly identify dependencies, proactively analyze threats as well as vulnerabilities, and safeguard critical resources.

**Creating a robust 360-degree security dashboard requires cross-functional data correlation from various sources:**



The security assessment dashboard below provides unified, real-time visibility into an organization's IT security posture, aggregating risk indicators from various IT and security tools into an intuitive interface. Each visualization within the dashboard is designed to provide granular insights into critical vulnerability areas.



This comprehensive security dashboard empowers IT teams to:

- **Expedite incident response and threat detection:** Quickly identify compromised resources and high-risk vulnerabilities, enabling proactive isolation and remediation before critical breaches occur.
- **Ensure proactive compliance and audit readiness:** Demonstrate compliance with regulatory standards and policies. Generate audit reports instantly, reducing compliance overhead and saving time on last-minute analysis.
- **Optimize security initiatives with targeted strategies:** Prioritize vulnerabilities based on risk probability and impact, enabling targeted security fixes. Allocate security budgets based on real-time risk insights, rather than assumptions.

Cross-functional IT dashboards—like the one presented here—provide a comprehensive, single-pane view by aggregating data from diverse IT activities. This unified perspective empowers IT teams to proactively identify and resolve issues, optimize efficiency, reduce costs, and enhance user experiences.

Beyond monitoring security posture and vulnerabilities, correlated dashboards serve as a dynamic scorecard, enabling the assessment of critical KPIs, including:

- IT budget ROI
- Service-level compliance
- Customer satisfaction and user experience
- Infrastructure and operational stability

# Consolidated scores to assess security posture

**A**s established in the previous section, an organization's security posture is a multifaceted concept, requiring real-time visibility into numerous indicators across the IT landscape.

While 360-degree cybersecurity dashboards—which correlate data from multiple tools and IT domains—are invaluable for real-time vulnerability tracking and security fortification, IT and security leaders might sometimes require a concise, high-level overview of their organization's overall security health.

A tailored security score is vital for implementing timely security strategies, prioritizing relevant initiatives, and justifying security investments to business leadership. But traditional methods of calculating and tracking security scores are flawed. Manual aggregation is slow, and generic models lack accuracy. Organizations need automated, customized scores that reflect unique environments, avoiding time-consuming, inconsistent assessments.

A real-time, automated, and tailored ML model is the perfect solution to this conundrum.

A custom ML model can aggregate and correlate data from multiple security tools to generate a bespoke security score tailored to an organization's unique operating conditions, security standards, and policies.

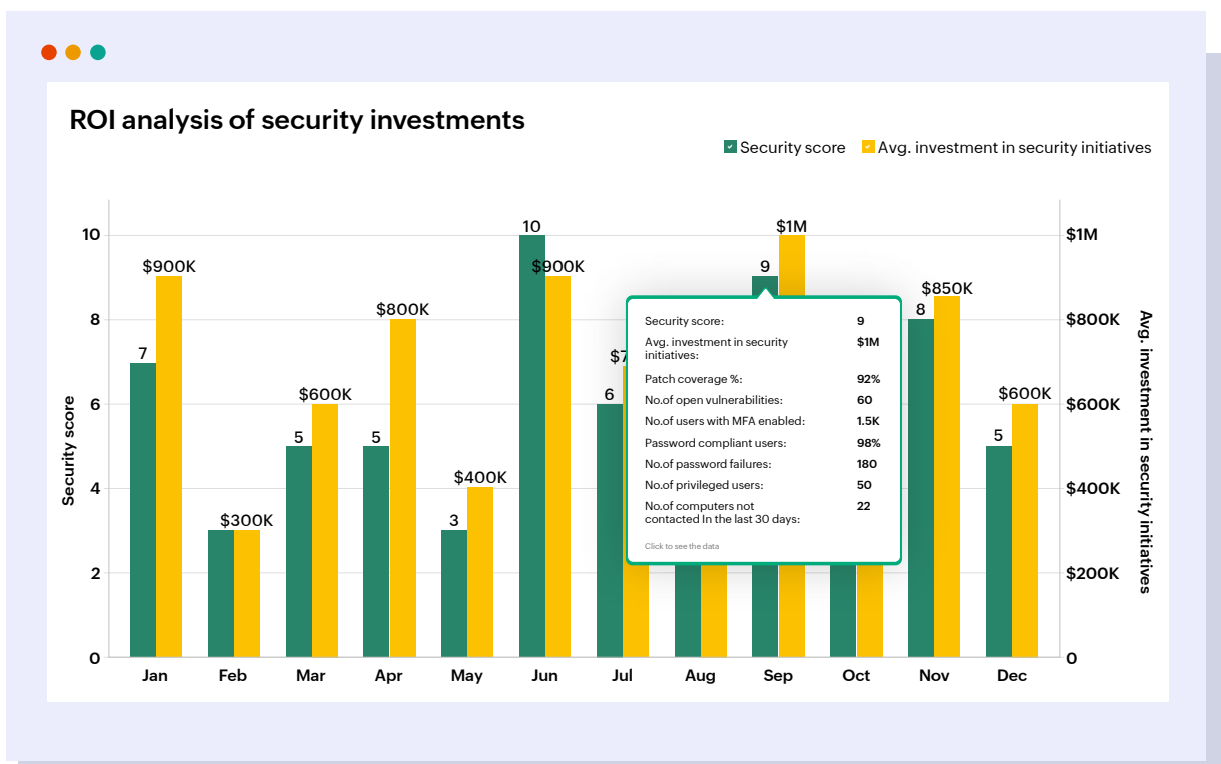


Traditionally, crafting such bespoke ML models demands specialized AI/ML expertise, significant development time, and substantial financial investment.

Analytics Plus addresses this challenge by enabling IT teams to create, train, and deploy no-code ML models capable of analyzing organization-wide security data and calculating accurate, custom security scores in seconds.

### Leveraging no-code ML for accelerated security score generation

Analytics Plus' automated machine learning (AutoML) capabilities enables IT teams to swiftly build custom security score models, eliminating the need for complex coding or data science expertise. By training models with historical data on patch compliance, IAM risk, vulnerabilities, and past incidents, the analytics platform can build ML models that can assess security posture at any instant. This allows for both real-time score calculation and future prediction. IT teams can tailor risk factor weighting based on past impacts, creating a dynamic, accurate security assessment method.



The provided visualization demonstrates a positive linear relationship between strategic security investments and the organization's security scores. As monthly investments in strategic security initiatives increase, the organization's security posture consistently improves, as reflected in rising security scores.

The security score is calculated by correlating data on high-impact security parameters from endpoint management, IAM, and PAM solutions.

With the aid of these custom-tailored security scores, IT leaders can:

- **Establish accurate, data-driven security bench marking:** Quantify and track security improvements over time.
- **Prevent incidents and achieve compliance readiness:** Identify and address vulnerabilities before they lead to incidents.
- **Justify ROI of security investments:** Use score improvements to justify security ROI and gain leadership buy-in on future security investments and increased resource allocation.

Furthermore, these no-code ML models can continuously adapt to the evolving threat landscape, ensuring the security scores remain accurate and relevant.

Beyond calculating organizational security scores, tailored, no-code ML models offer a versatile solution for a multitude of scenarios within the IT landscape. These models can be leveraged for accurate capacity prediction, proactive ticket escalation probability analysis, and precise downtime forecasting, which come together to enable IT teams to optimize resource allocation, enhance service delivery, and minimize disruptions.

# Curb unauthorized RDP sessions to secure privileged accounts

The preceding scenarios demonstrated the power of cross-domain insight correlation in streamlining, monitoring, and optimizing critical IT operational parameters. However, IT optimization is not a static achievement. To ensure sustained progress and maximize the impact of dashboards and tailored ML models, continuous monitoring and data-driven adjustments are essential. This section will delve into a real-world use case illustrating how ongoing data correlation facilitates continuous improvement.

Remote Desktop Protocol (RDP) has become an indispensable tool for IT administrators and support teams, facilitating remote system management. While increased remote work and digital transformation have expanded RDP use, it has also exposed key vulnerabilities. Publicly exposed RDP endpoints are targets for attacks, and despite advancements, comprehensive threat mitigation remains difficult.

Privileged access management (PAM) is a crucial authentication mechanism for securing RDP sessions. By requiring all RDP sessions to undergo authentication through PAM systems before connecting to servers or endpoints, organizations can prevent unauthorized users from directly accessing critical systems. This added layer of protection is often considered a cornerstone of secure RDP sessions.

However, attackers have evolved sophisticated techniques to circumvent traditional PAM controls and gain direct contact with servers through RDP. These methods include compromising VPN credentials, employing password spraying and credential stuffing, and manipulating privileged access controls to initiate unauthorized RDP sessions.

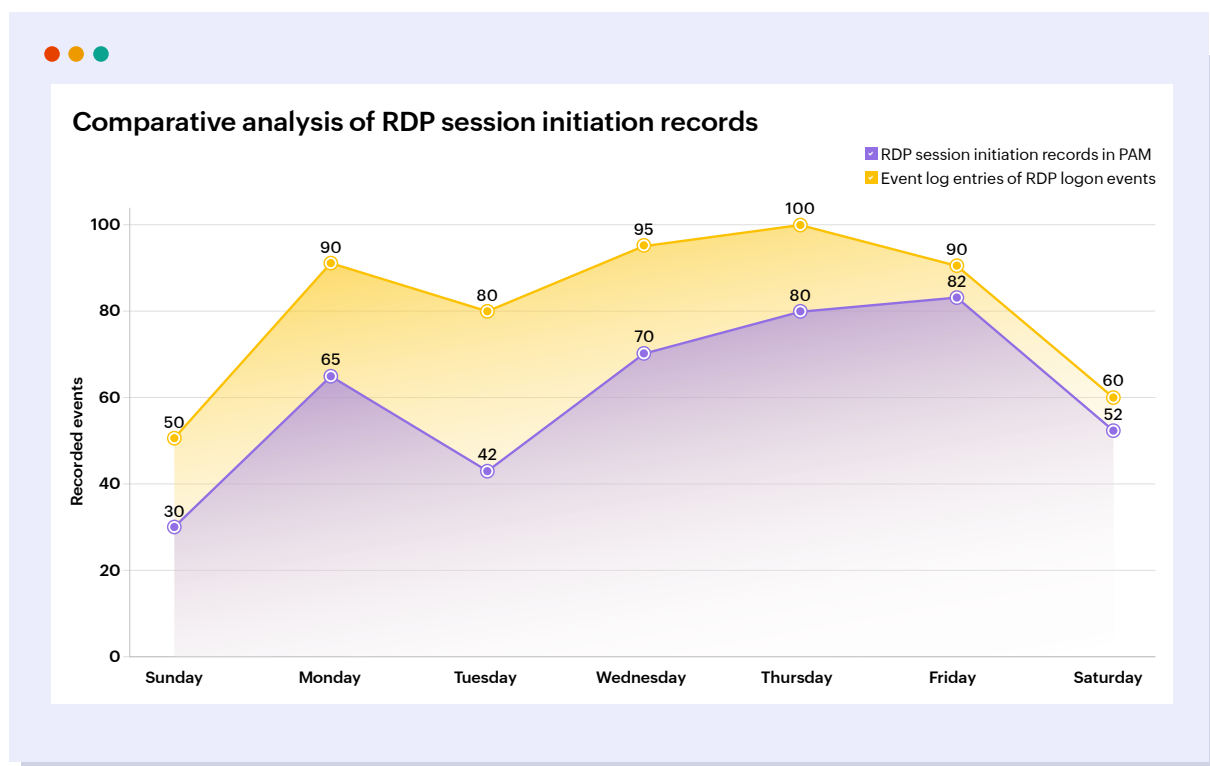
Compromised RDP sessions pose severe security risks including ransomware deployments and result in operational disruptions, regulatory non-compliance, and overall degradation of the organization's security posture

## Proactive threat detection: Closing the RDP security gap

The most effective way to mitigate RDP threats is to proactively identify suspicious or unauthorized RDP sessions that bypass established PAM protocols.

This requires complex, real-time correlation between multiple IT tools. Relying solely on PAM log data can obscure critical indicators of RDP misuse, as PAM logs are often siloed from other systems in IT landscape. Aggregating RDP-related logs from various sources—including PAM tools, SIEM solutions, and log management applications—provides a comprehensive view of anomalous RDP activity.

Correlating RDP session initiation logs from PAM systems with syslog or event log entries from log management applications allows for the quick identification of unauthorized RDP sessions that circumvent PAM controls.



The analysis demonstrates the significant disparity between PAM-authenticated RDP sessions and RDP logon events in event logs. This disparity indicates that a significant percentage of RDP sessions bypass PAM modules, gaining direct access to privileged servers.

By consistently monitoring all RDP sessions within the organization's network, IT teams can gain deeper visibility into unauthorized connections that bypass security protocols.

Further analysis can identify RDP vulnerability indicators, such as:

- Sessions initiated outside of normal work hours.
- Logins from unusual geographic locations.
- High frequency of failed login attempts.

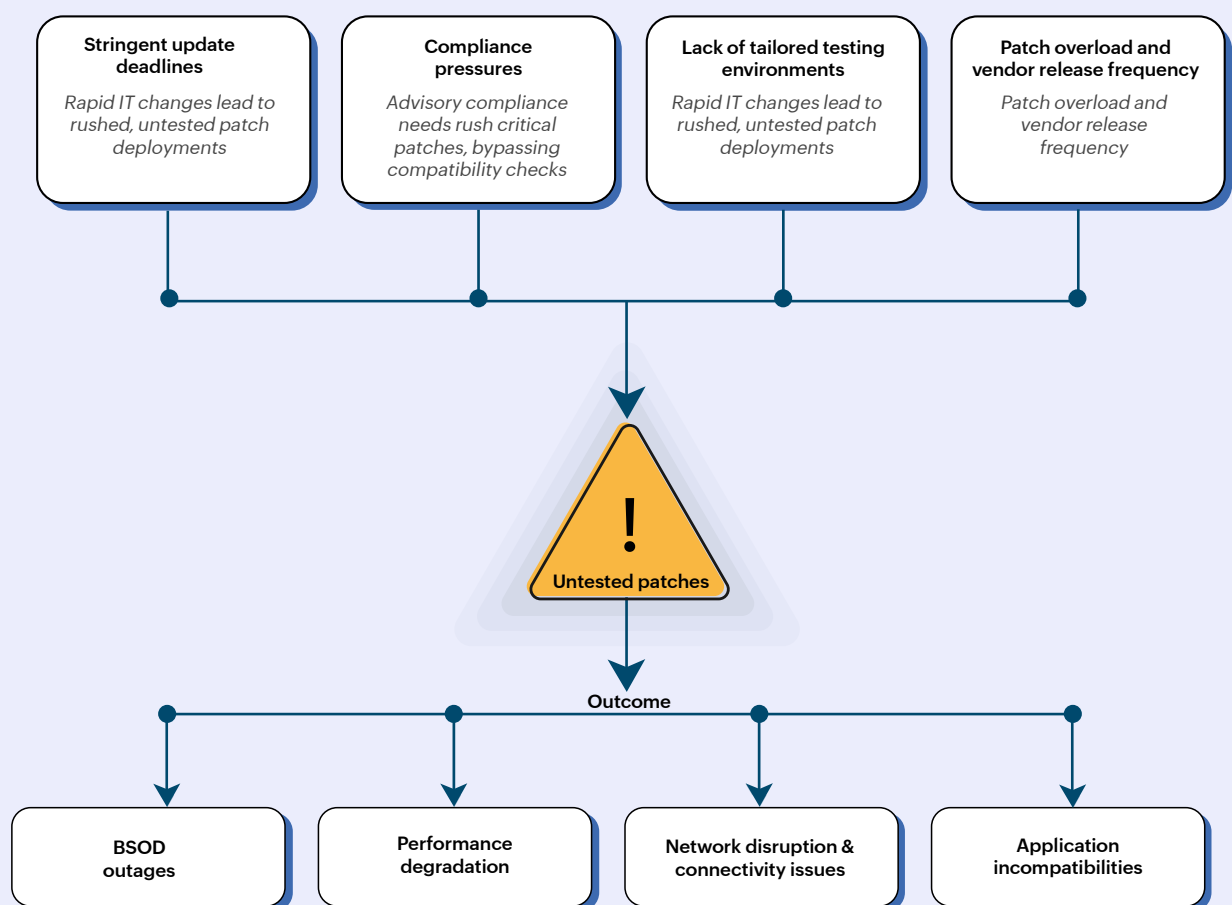
This correlation enables IT teams to identify and set alerts for high-risk RDP activities, proactively mitigating unauthorized RDP events and shutting down malicious sessions before they lead to critical security incidents.

## 04 Improve patch management to deliver better ITSM

**W**hile timely patch updates are indispensable for maintaining the security and performance of your organization's assets, deploying untested patches can trigger a cascade of system failures, application crashes, and a surge in service desk incidents.

A **BitSight study**<sup>[1]</sup> revealed that organizations with subpar patching practices were over seven times more susceptible to ransomware attacks compared to those with robust patch management. Moreover, **Microsoft's Patch Tuesday updates**<sup>[2]</sup>—despite their intent—have a history of causing widespread disruptions, including blue screen errors, performance degradation, and software incompatibilities.

### The risk of untested patch deployments



The service desk inevitably bears the brunt of untested patch deployments, experiencing a surge in incident volume, leading to increased response times, higher ticket reopen rates, and ultimately, impacting productivity and strategic project progress.

### **Achieving holistic patch compliance visibility**

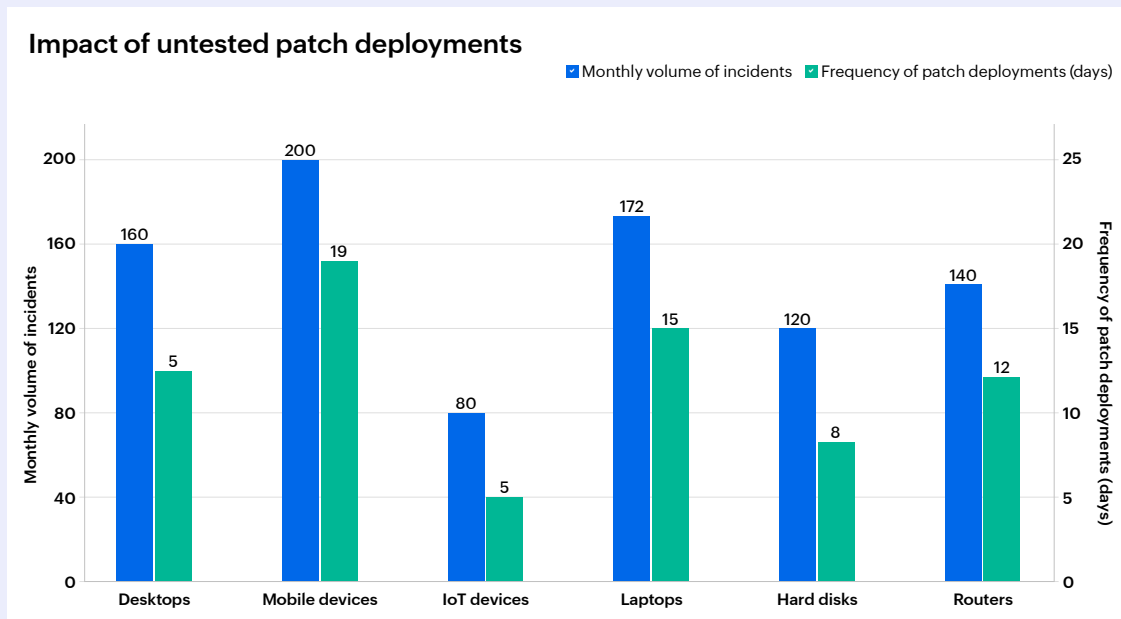
A major challenge in patch management is proactively identifying vulnerabilities or gaps caused by untested patches. The siloed nature of IT functions often obscures the root cause of service outages following patch deployments.

To address this, IT teams need a comprehensive, end-to-end view of their patch deployments. This can be achieved by consolidating patch-related insights from disparate monitoring tools, including:

- Endpoint management tools that track patch deployments.
- Service desks that manage the organization's incidents.
- Application performance monitors that detect system slowdowns and crashes post patch deployment.

An AI-powered IT analytics solution can seamlessly correlate this data, providing a real-time view of gaps in patch testing and management practices.

The following analysis demonstrates the cause-and-effect relationship between untested patches and service incidents.



The visualization reveals that device categories with high-frequency patch deployments experience significantly higher monthly incident volumes compared to those with low-frequency deployments. This clearly indicates that frequent patch deployments, when not properly tested, create a trend of incident spikes.

Based on these insights, IT teams can conduct further investigations into device categories with high incident volumes, including:

- Analyzing service desk ticket volumes before and after patch deployments.
- Identifying incident volume spikes within 24 hours of specific patch roll outs.
- Matching ticket descriptions with affected systems and patch versions to pinpoint problematic patches.
- Mapping affected devices to assess the impact of faulty patches.



This comprehensive, data-driven approach empowers IT teams to implement timely rollbacks of faulty, untested patches, thereby reducing patch-related downtime, accelerating incident resolution times (MTTR), and minimizing business disruptions.

05

## Address asset utilization to improve IT budgeting

**J**ust as cross-functional correlation provides comprehensive oversight of IT operations, it also plays a vital role in streamlining the entire IT asset lifecycle. This section will explore how data-driven correlation optimizes asset procurement, the foundational stage in any asset's journey.

Organizations waste thousands of dollars on underutilized assets. IT teams must become strategic stewards, maximizing ROI by optimizing software purchases and usage. Daily software license requests require scrutiny against actual usage to identify underutilization, a major IT challenge.

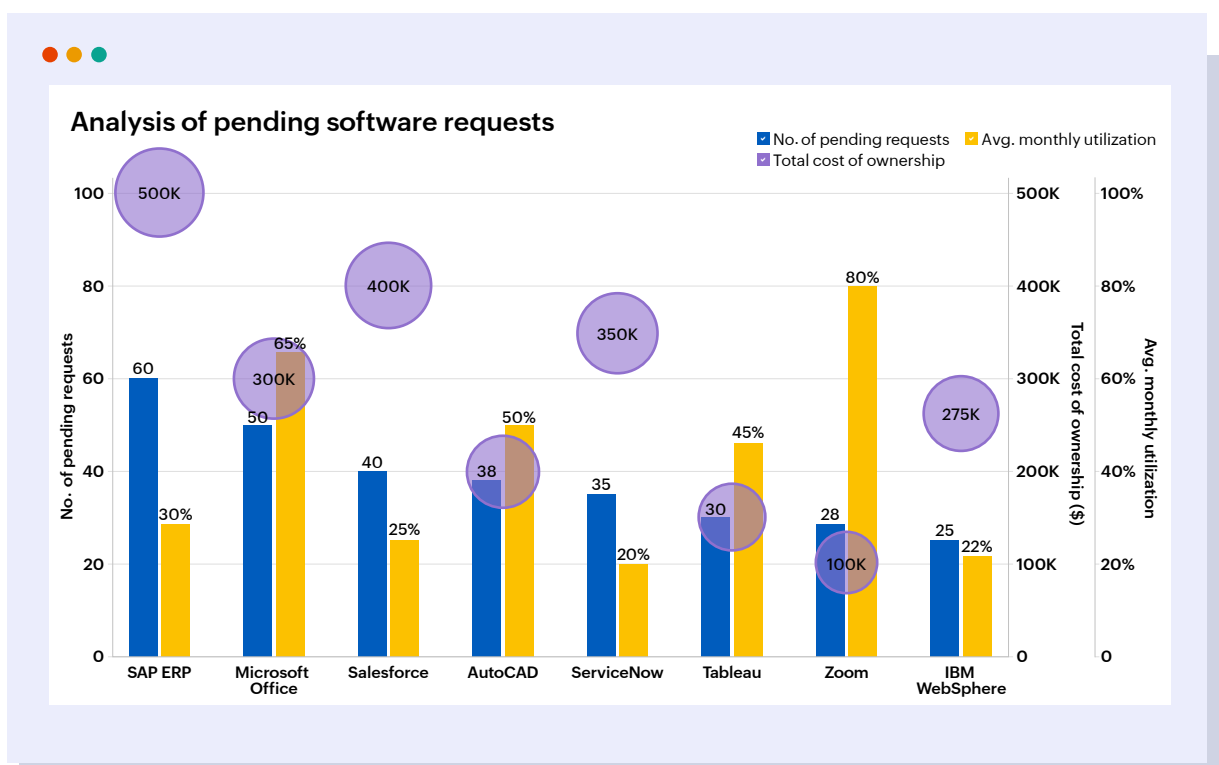
To prevent budget drains, software investments must align with organizational needs. Tracking unused licenses is crucial, while insufficient licensing risks lowered productivity, leads to revenue loss, and creates issues during asset audit.

IT managers face a delicate balancing act: curbing over-provisioning while ensuring availability of essential software. Analyzing usage patterns is key to making informed decisions and preventing unnecessary expenses.

However, discerning software license utilization requires a sophisticated approach, correlating data from diverse IT systems to establish accurate usage patterns and distinguish between actively used, necessary, and redundant licenses.

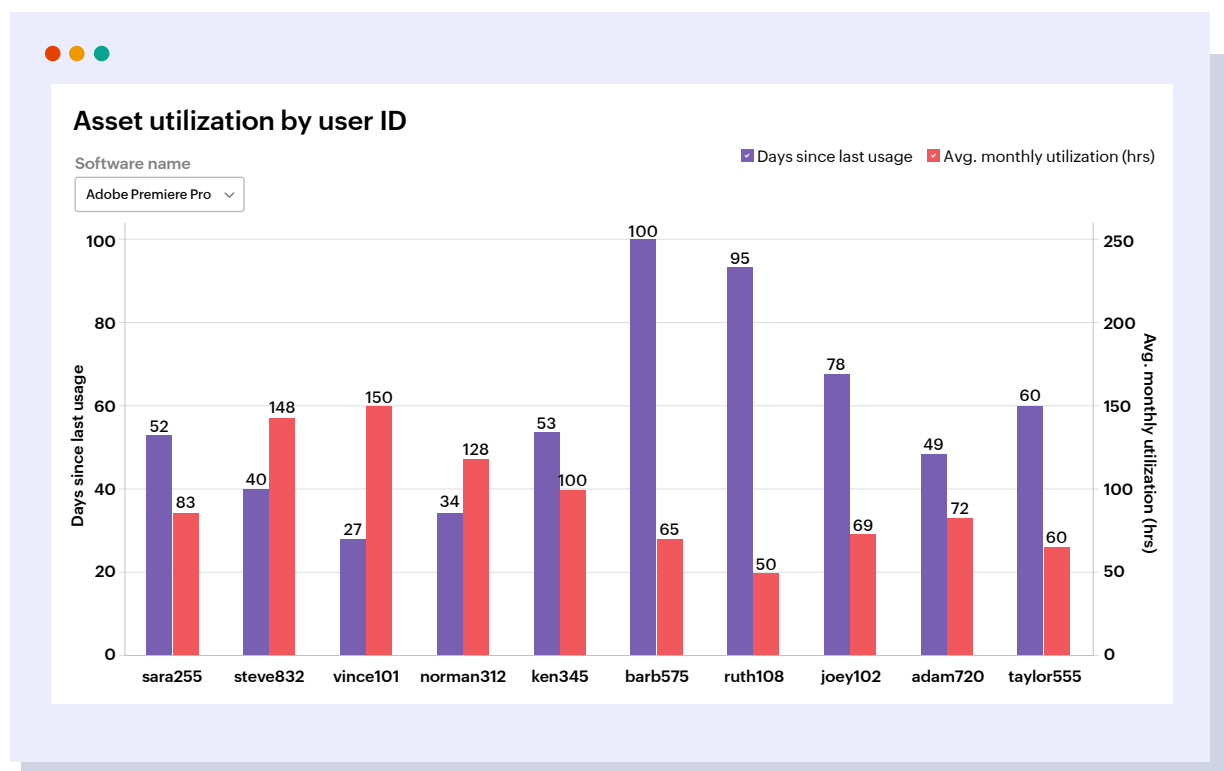
A detailed comparative analysis of software needs and utilization patterns can be achieved by integrating data from various applications within the IT ecosystem, including endpoint management systems, service desks, software access logs, and financing and procurement tools (e.g., Xero, Exact).

The analysis below, which aggregates data from these diverse sources, empowers IT managers to efficiently monitor software utilization, pinpoint cost inefficiencies, and make informed renewal decisions.



This analysis unveils a glaring picture of significant software underutilization that pervades IT landscapes. By comparing the top 10 software licenses with the highest purchase or renewal requests in the service desk against their total cost of ownership, it becomes evident that many high-cost licenses are critically underutilized, leading to substantial, hidden cost drains.

IT teams can delve deeper to identify specific users contributing to asset underutilization. For instance, the below detailed analysis can reveal devices or users that under-utilize expensive software like Adobe Premiere Pro.



By performing this line of analysis, IT teams can cancel unnecessary renewals and reallocate licenses to users or initiatives where demand and utilization are demonstrably higher.

This cross-functional correlation of software asset purchase and usage patterns empowers IT teams to:

- **Achieve immediate cost reduction and budget optimization:** Identifying and reclaiming unused or underutilized software licenses allows organizations to achieve immediate cost savings.
- **Align software procurement with business needs:** Eliminating redundant licenses allows IT teams to align software purchases with actual business requirements, preventing over-licensing, reducing operational complexity, and minimizing support costs.
- **Optimize IT resource allocation:** Reallocating licenses from underutilized areas to high-impact initiatives with genuine needs prevents unnecessary budget expenditures.

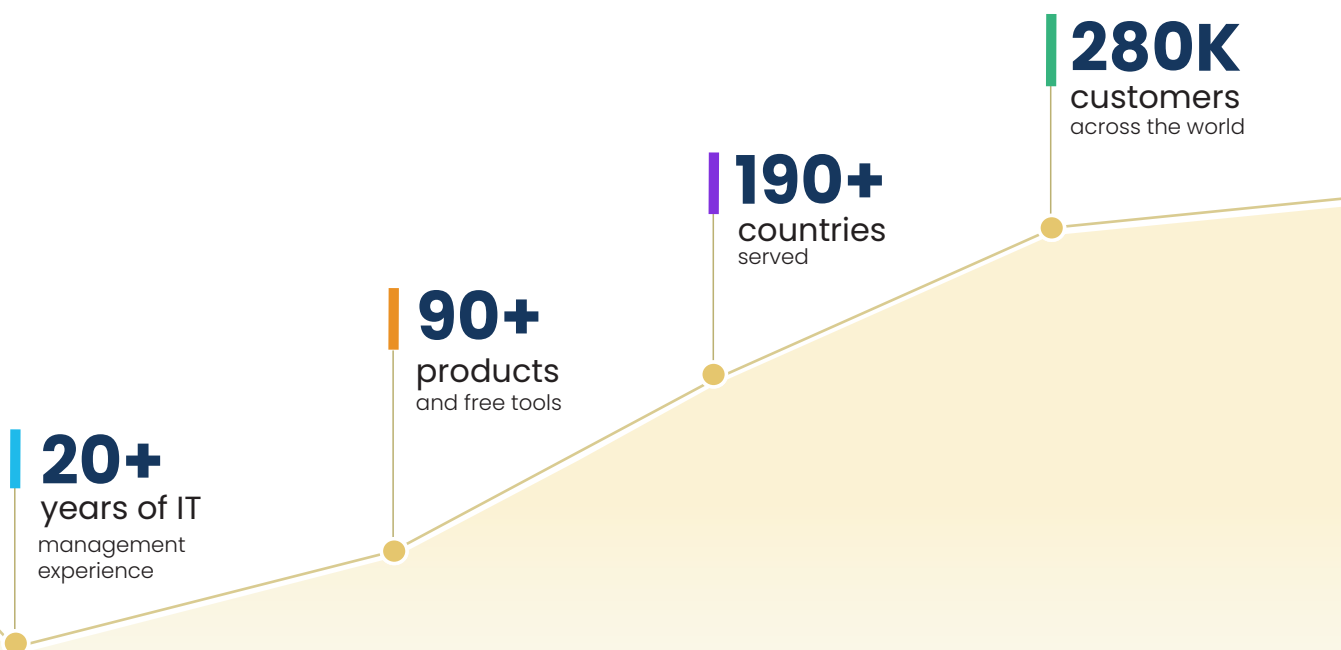
## Conclusion

By leveraging AI-powered correlation across key IT domains, IT teams gain a strategic advantage in mitigating service inefficiencies, security risks, and unnecessary costs. AI-powered IT analytics platforms, such as Analytics Plus, empower IT teams to make faster, data-driven decisions, fostering a more resilient and efficient IT ecosystem.

# 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.

For more information about Analytics Plus,  
visit: [www.manageengine.com/analytics-plus/](http://www.manageengine.com/analytics-plus/)



## Reference

1. <https://www.bitsight.com/blog/outdated-software-issues>
2. <https://support.microsoft.com/en-gb>



© ManageEngine, a division of Zoho Corporation