



ManageEngine  
**Analytics Plus**

# **How to effectively correlate data to streamline IT operations**

Identify logical correlations or relationships in your IT data and visualize how individual events impact other IT subdivisions.



# How to effectively correlate data to streamline IT operations

**I**n theory, IT is a collection of multiple subsets or departments, each with its own set of processes, tools and technologies, that work together to keep the business operational. In reality, IT is a collection of extremely complex, disjointed tools and technologies that do not interact with one another. So, when a problem emerges in one of the IT subsets, it creates a ripple effect in other subsets too, resulting in multiple subsets working independently on the same set of problems at the same time. Without looking at the bigger picture, individual subsets lack context into problems so their troubleshooting is ineffective.

For instance, let's say you're the NOC manager of an organization and you've noticed a spike in MTTR in the last few months. You might dedicate additional IT staff, provide training, and shuffle resources around to tackle the influx. However, the real problem might be due to ongoing changes in production settings that's triggering a slew of related incidents. In this case, pumping in additional IT staff is not going to improve MTTR unless the root cause is addressed.

Data correlations enables you to pinpoint logical correlations and relationships within data, and isolate problems from their symptoms. In the example above, the spike in MTTR or the increase in incident volume are the symptoms, while changes in the production setting is the problem. By isolating the problem and symptoms, you can reduce many of the incidents to a single problem, and address the problem to resolve the issue quickly.

**The data correlation process used for troubleshooting issues usually involves these steps:**

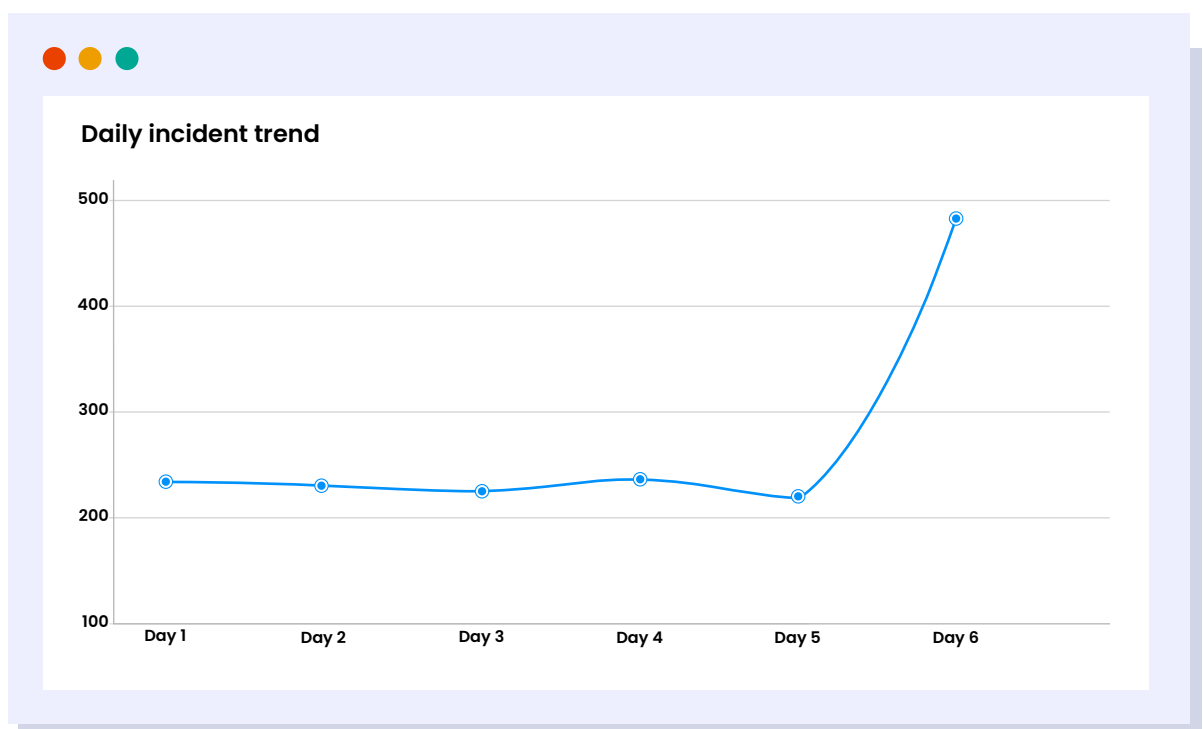
- Integrating IT data from multiple IT applications and analyzing event history.
- Root cause analysis to identify the underlying problems by looking into overlapping patterns, and trends. AI, and machine learning can fast-track this process by correlating log information from monitoring applications.
- Deriving actionable insights to determine remediation measures.

In this e-book, we'll explore a few common problems across IT subdomains, and investigate how those problems are related to events occurring in other subdomains using data correlations.

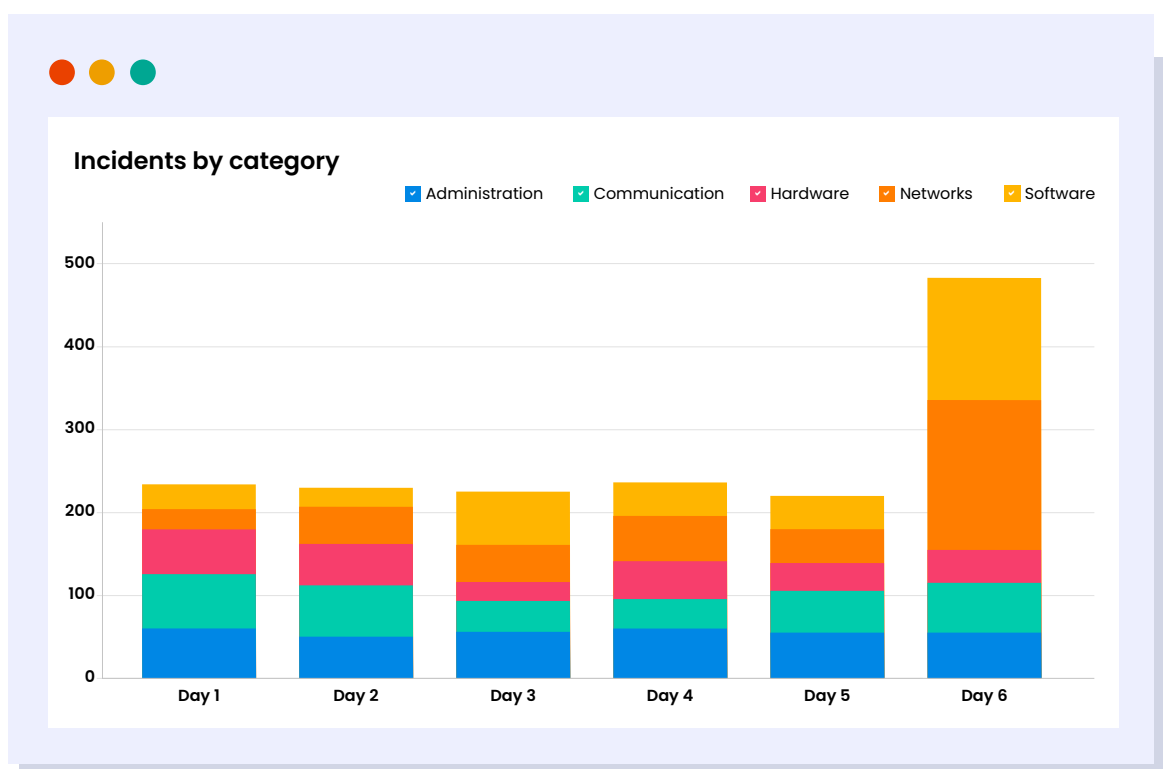
# Incident management

Of all IT subdepartments, data correlation is particularly critical for incident management. Without this, IT incident management teams will be stuck in a never-ending loop of "incident logging-response-resolution". Worse, they may not even realize that they're dealing with repeat incidents. For the organization, this can result in lost revenue, and spiraling operating costs.

Let's take a common incident management problem. Let's say there's a sudden increase in the incident volume on a particular day. Here's a sample report to explain the situation.



Without data correlation, incident response teams will go in turbo mode and try to resolve as many incidents as quickly as they can. With data correlation, incident teams can dig into the root cause of the sudden spike in incidents, and discover underlying problems that trigger these incidents. First, let's decode the nature of these incidents, such as hardware, software, networks, communications, or administration-related issues.



From the report above, it's clear that an increase in network and application-related incidents predominantly makeup for the sudden spike in incidents. Next, decode the network and application-related alarms using a keyword cloud report. This should tell you if the application incidents are related to just one or several applications.



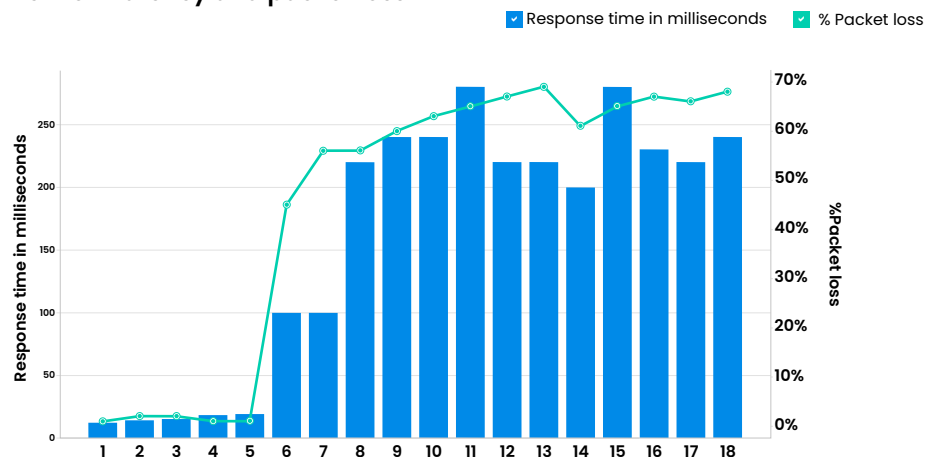
### Keyword cloud for network and application-related incidents

Not able to access Adobe  
Network issue  
Unable to access e-mail  
Login issue with E-mail  
**Internet is slow**  
**Not connecting to internet**  
Network slow  
Not able to login  
Network not reachable  
Not able to access CRM

From the keyword cloud report, it's evident that several applications are slow, or unavailable. In an organization that's using several applications to power its business, it's unlikely that all applications go down at once, unless there's a major network issue. A quick analysis on network latency and packet loss should give you more information on the status of networks across the organization.



### Network latency and packet loss



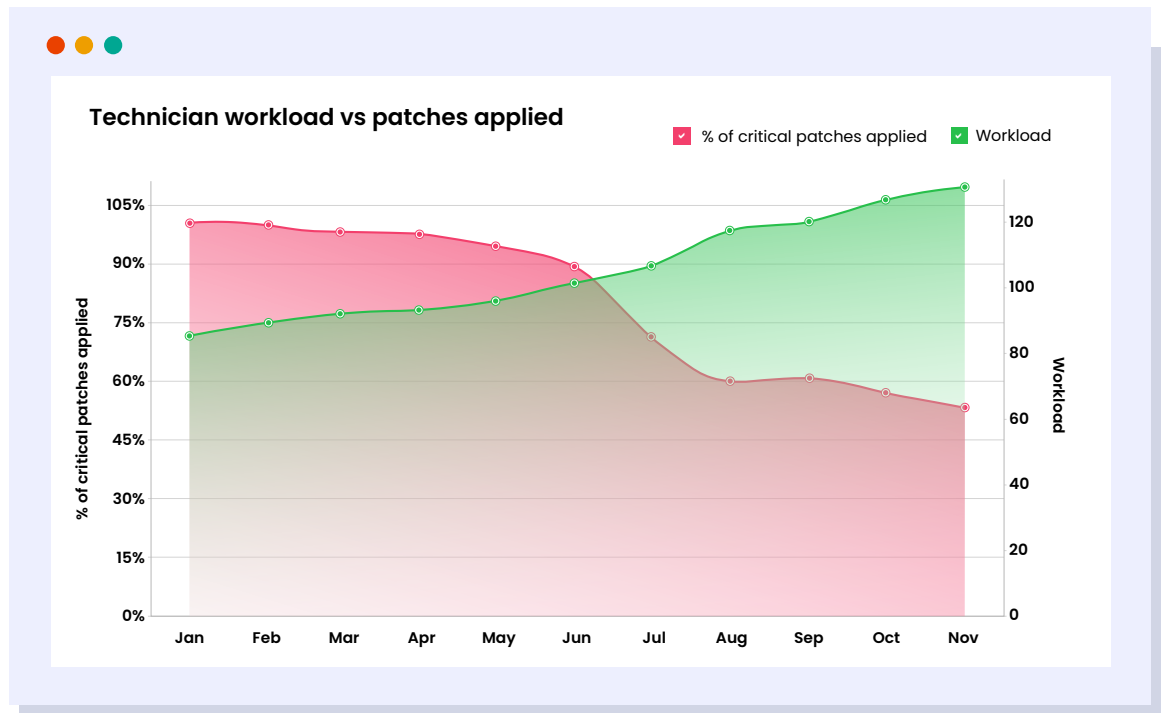
From the report, it's clear that the networks are slow. Fixing network latency should make the applications available, and enable users to access their applications. This should also cut down on network and application-related incidents, and in turn, reduce the overall incident volume.

# Patch management

**P**atch management is one of the most critical departments within IT. Timely application of critical security patches can keep the organization's data secure, and prevent costly data breaches, loss of reputation, and even loss of revenue. Without timely patching, organizations are just one step away from a security threat that can cost them millions of dollars. Take the **Equifax**<sup>[1]</sup> data breach for instance. The company lost the data of about 145 million people due to a delay in patching a security vulnerability in Apache Struts. Similarly, Carphone Warehouse lost the data of about 1.27 million people due to delay in patching a vulnerability in WordPress.

Although the patch management process has been fully automated through the use of endpoint management applications, technicians are still needed to perform preliminary tasks such as sandbox testing patches before org-wide deployment. The unavailability of technicians, due to excessive workload, poor resource management, or lack of training can delay the patch application process, leaving several security vulnerabilities exposed.

Here's a report that shows how technician workload and patching are correlated.



It's clear that when the technicians' workload increases, there's a significant delay in the percentage of critical patches applied. Ensure the technicians' workload is always at an optimum so that they are available to handle critical tasks such as patching. In the rare occasions where workload exceeds planned numbers, additional resources should be deployed to ensure timely application of patches.

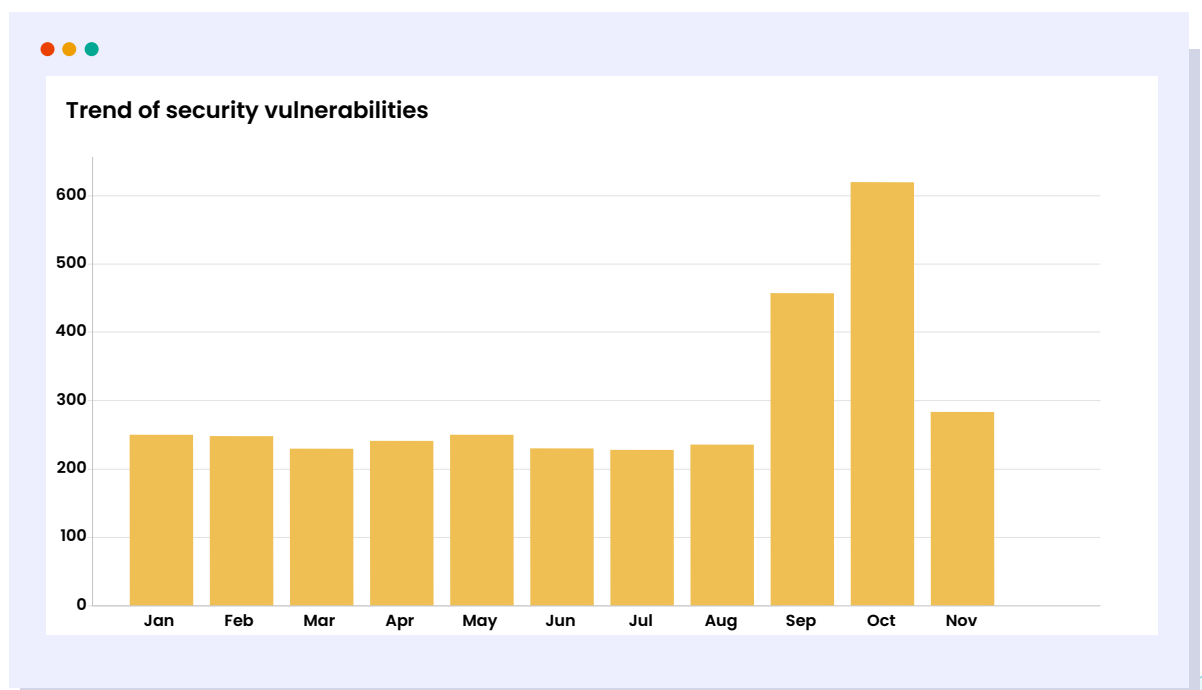
# Project management

Organizations cannot thrive in a competitive business landscape without adopting the latest technologies. However, this should not come at the cost of security. Seemingly minor actions, such as opening up a secure gateway for a developer to test the latest app and not locking the gateway afterwards, can leave a gaping hole in your cybersecurity stance.



While adopting these newer technologies, it's important to reduce security risks and amplify the benefits. This is possible only when project leaders perform in-depth impact analysis and sufficient testing before adopting any new technology. Take the Covid-19 crisis for instance. When the entire world was forced to work out of home offices, organizations essentially had to condense a multi-year digital transformation process into a span of a few months. This resulted in **several security threats**<sup>[2]</sup>, and organizations lost data worth billions of dollars, and paid millions in ransom.

Keeping security in mind, IT leaders embracing new projects such as digital transformation or new technology adoption, should factor in the impact of their projects on security. A historical comparison of digital transformation initiatives alongside known vulnerabilities will reveal a direct correlation. Here's a sample graph that shows the trend of known vulnerabilities in the last few months, and a pivot report that shows the timeline of new projects undertaken.





### Project timeline and status

	Project names	Product manager	Start date	End date	Duration	Status
1.	Data warehouse set up	Shawn Adams	03 Feb 2022	19 Feb 2022	16 days	Completed
2.	Data migration from Oracle Cloud	Victor Johnson	01 Apr 2022	15 May 2022	40 days	Completed
3.	Web application enhancement	Heady Kings	03 Jun 2022	15 Jun 2022	8 days	Completed
4.	Create e-commerce portal	Vernon Marks	05 Jul 2022	25 Jul 2022	16 days	Completed
5.	IT asset inventory mapping	Cooper McMohan	14 Aug 2022	28 Aug 2022	8 days	Completed
6.	Payment gateway set up	John Smith	01 Sep 2022	13 Sep 2022	8 days	Completed
7.	Global HR application set up	Nick Morgan	01 Oct 2022	19 Oct 2022	16 days	Completed

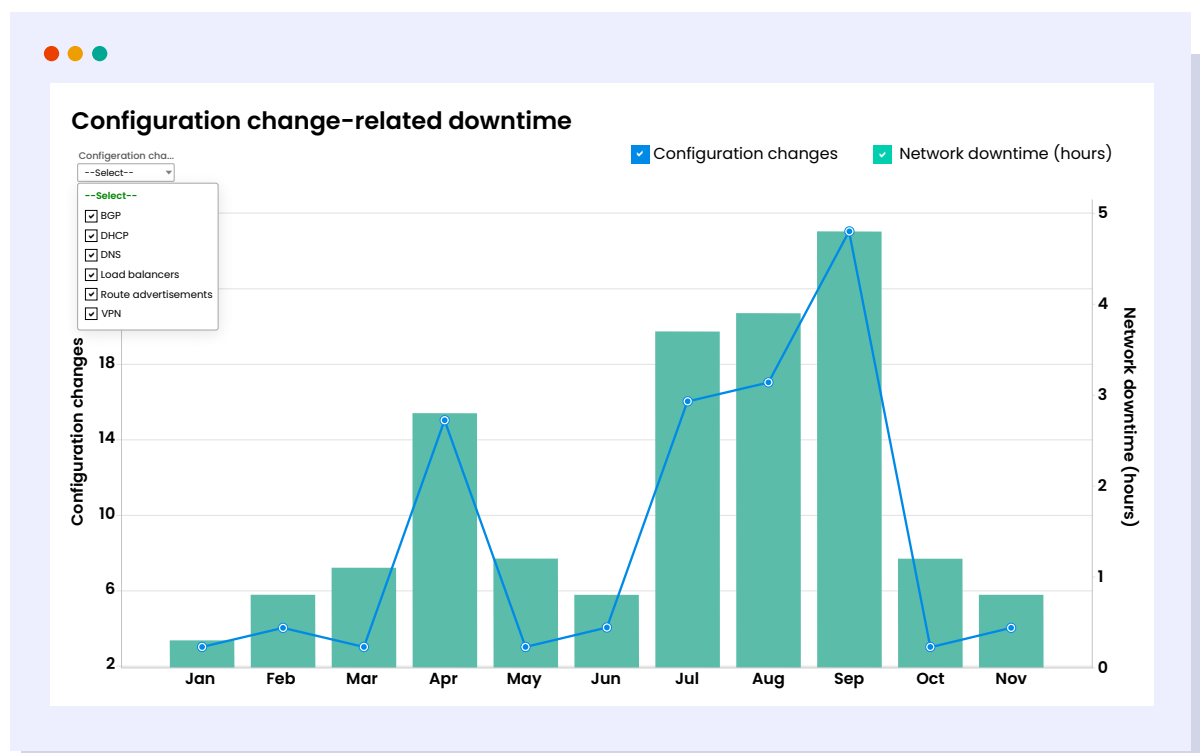
Analyzing the two reports reveals that creating any new workflows or setting up applications, such as setting up a payment gateway or a new HR application, results in a spike in the number of known vulnerabilities. Generally, setting up new applications involves opening secure gateways for the applications to access your data, and likewise, opening the application for access to people with different access levels. This can unravel existing cybersecurity protocols and expose some known vulnerabilities. Refining the application setup process, performing a security-impact analysis when taking up new projects or initiatives, and maintaining a checklist of 'things to watch out for' while setting up new projects are ways to minimize the impact of new projects on cybersecurity.

# Network Management

**N**etworks form an integral part of your business. When networks go down, they can take the entire business down with them.

While it's not rare to experience network-related issues, it's incredibly rare to have networks go offline completely for hours without a poorly executed change preceding it—such as configuration changes, hardware changes, and software updates. Change-induced network downtime accounts for nearly **80% of network outages**<sup>[3]</sup> across the globe. For instance, a Gigabit network port mistakenly configured for Megabit network speed can slow down the entire network and take services offline. While this is a simple issue, configuration changes to DNS, BGP, DHCP, VPN, route advertisements, and load balancers can cause complete network shutdown. **Facebook**<sup>[4]</sup> experienced a six-hour network outage in October 2021, due to changes to its network configuration. In July of that year, several major websites including **Amazon and Costco**<sup>[5]</sup> were down for several hours because Akamai (a content distribution network) made some DNS configuration changes.

Network downtime typically shows up as network alarms. A comparison of network downtime and network-related configuration changes shows a direct correlation.



It's evident from the report that network downtime is longer whenever there's a change in the network configuration. For this report, we've considered configuration changes to DNS, BGP, DHCP, VPN, route advertisements, and load balancers.

The best way to tackle configuration change-related downtime is to fine-tune the configuration change management process to ensure seamless change management with minimal to no disruption to network availability. In our example, it would help to have an inventory of network systems and to standardize configuration changes. Build a template for network configurations and set up alerts in your configuration management tool to detect deviation from these standards. Once you protect your network from unauthorized or non-standard configuration changes, it'd be much easier to minimize downtime. As a precautionary measure, frequently audit your networks to ensure they remain compliant with preset configuration standards.

## Conclusion

IT can seem like a tightly integrated suite of tools and technologies working together to keep the business in operation. However, the reality is that IT often struggles to make connections between events occurring among its subdepartments, leading to downtime, network or app-related incidents, recurring problems, and security threats. Data correlations can help break these silos and bring clarity into chaos. That is, highlight internal relationships between two or more subdepartments within IT. In this e-book, we've discussed a few examples to demonstrate how data correlation can be deployed to solve problems within IT. We hope you found those examples helpful and relevant. If you have more questions, **please write to us at [analyticsplus-support@manageengine.com](mailto:analyticsplus-support@manageengine.com)**

# About

**ManageEngine Analytics Plus** is a self-service business intelligence and IT analytics solution that integrates with several popular IT service management applications, such as ServiceDesk Plus, ServiceNow, Zendesk, Teamwork Desk, BMC, Splunk, SolarWinds, and Ivanti. Analytics Plus also integrates with other IT applications used for network and application management, project management, endpoint security management, and more. Powered by AI, machine learning, and natural language processing, Analytics Plus features an AI assistant that can display stunning visual responses to voice and text comments. Analytics Plus can also import data from multiple sources, and perform advanced analytical functions such as data blending, and trend forecasting.

[Start a free trial of Analytics Plus today.](#) Want to know more about the product? [Sign up for a virtual tour with our experts.](#)

**280K**

customers  
across the world

**20+**

years of IT  
management experience

**90+**

products  
and free tools

**190+**

countries  
served

## Reference

1. <https://www.pandasecurity.com/en/mediacenter/security/consequences-not-applying-patches/>
2. <https://www.cybergfx.com/resources/research-and-insights/blog/cyber-threats-on-the-rise-due-to-covid-19>
3. <https://www.manageengine.com/network-configuration-manager/challenges-in-managing-configurations.html>
4. <https://engineering.fb.com/2021/10/04/networking-traffic/outage/>
5. <https://www.npr.org/2021/07/22/1019333663/internet-outage-dns>

**Analytics Plus** 

© ManageEngine, a division of Zoho Corporation