

Six ways analytics can facilitate **proactive IT operations management**



Introduction

IT operations management has traditionally taken a reactive approach. Issues such as application failures, bandwidth spikes, poor or intermittent network connectivity, and backup failures can hurt productivity and cause serious financial losses.

Utilizing a proactive approach can help you save a lot of time and money. Using an advanced analytics solution like Analytics Plus, IT teams can foresee these problems in advance by analyzing applications and network data for baselines, trends, and anomalies. This e-book covers six ways you can use analytics to proactively manage your applications and network.

1. Plan and optimize cloud infrastructure usage

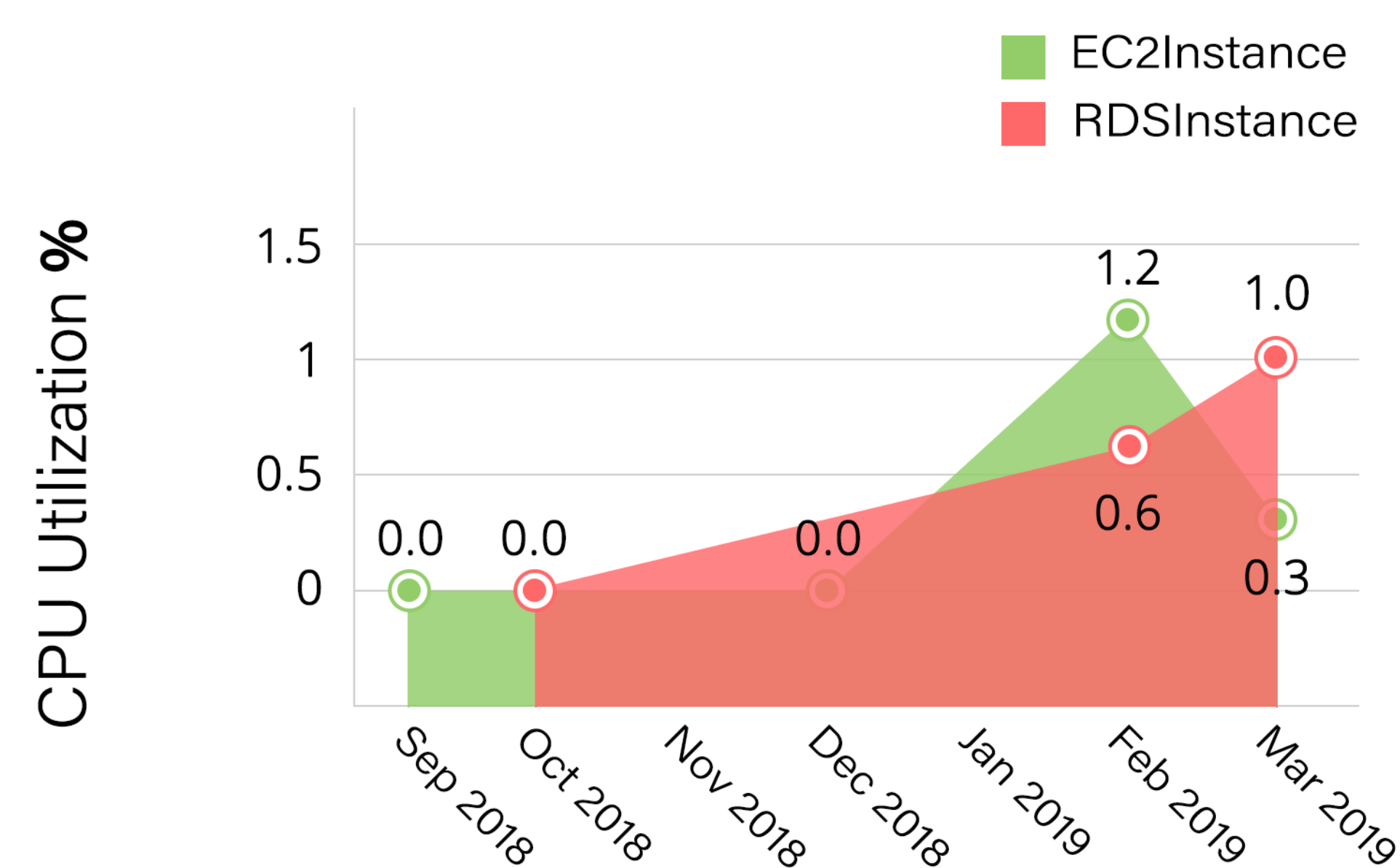
Adopting a cloud infrastructure helps organizations boost productivity while lowering costs. However, organizations often fail to consider historical usage patterns, which in turn, causes them to underutilize and overpay for their cloud infrastructure. A quick glance at past infrastructure usage trends helps you determine the right size of your IT infrastructure based upon your unique business requirements.

Here's a look at the Amazon Web Services (AWS) dashboard that gives you an overview of the AWS environment:

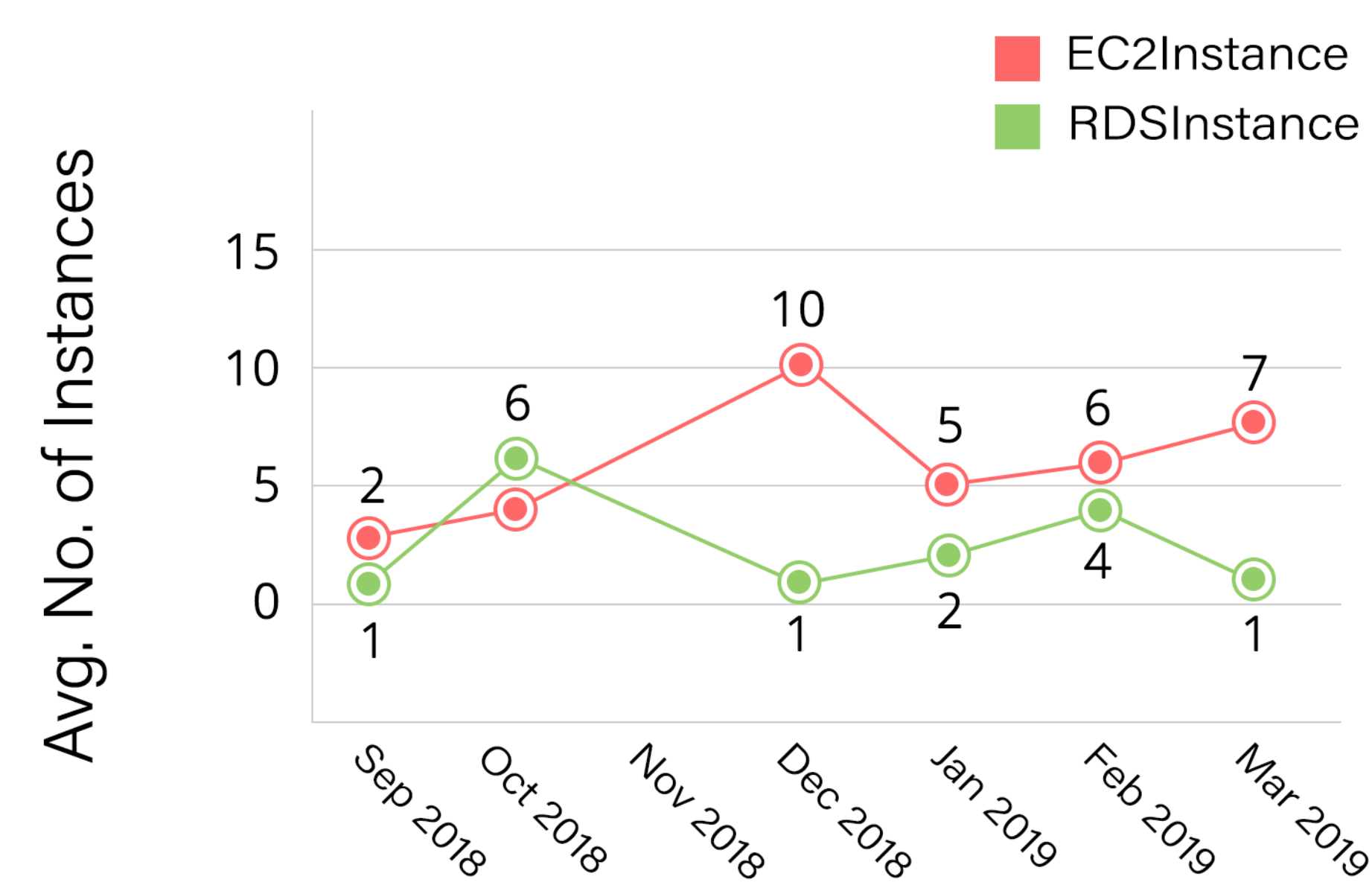
Amazon AWS dashboard

AWS monitors	EC2 instances	RDS Instances
18	14	2

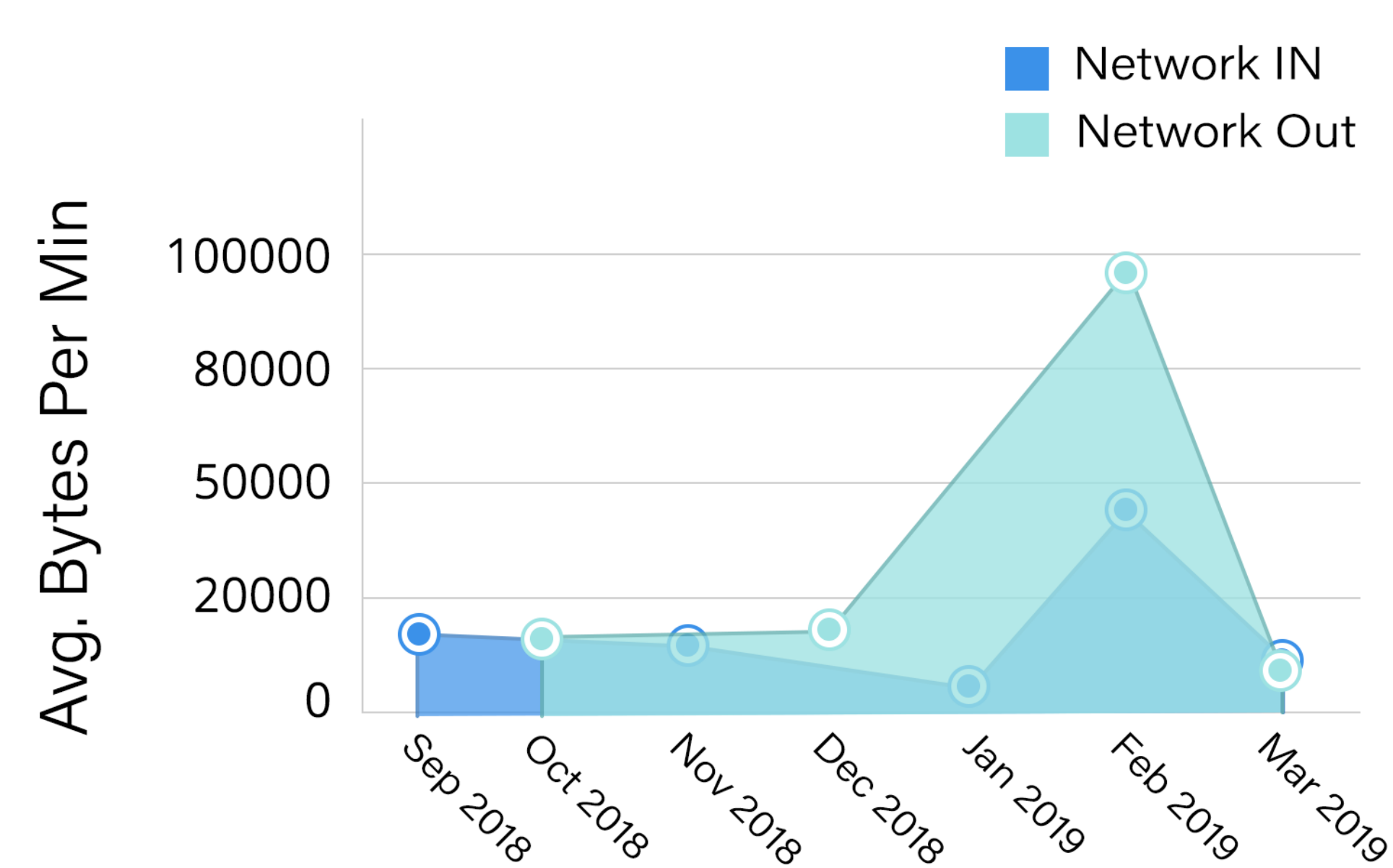
RDS and EC2, CPU utilization



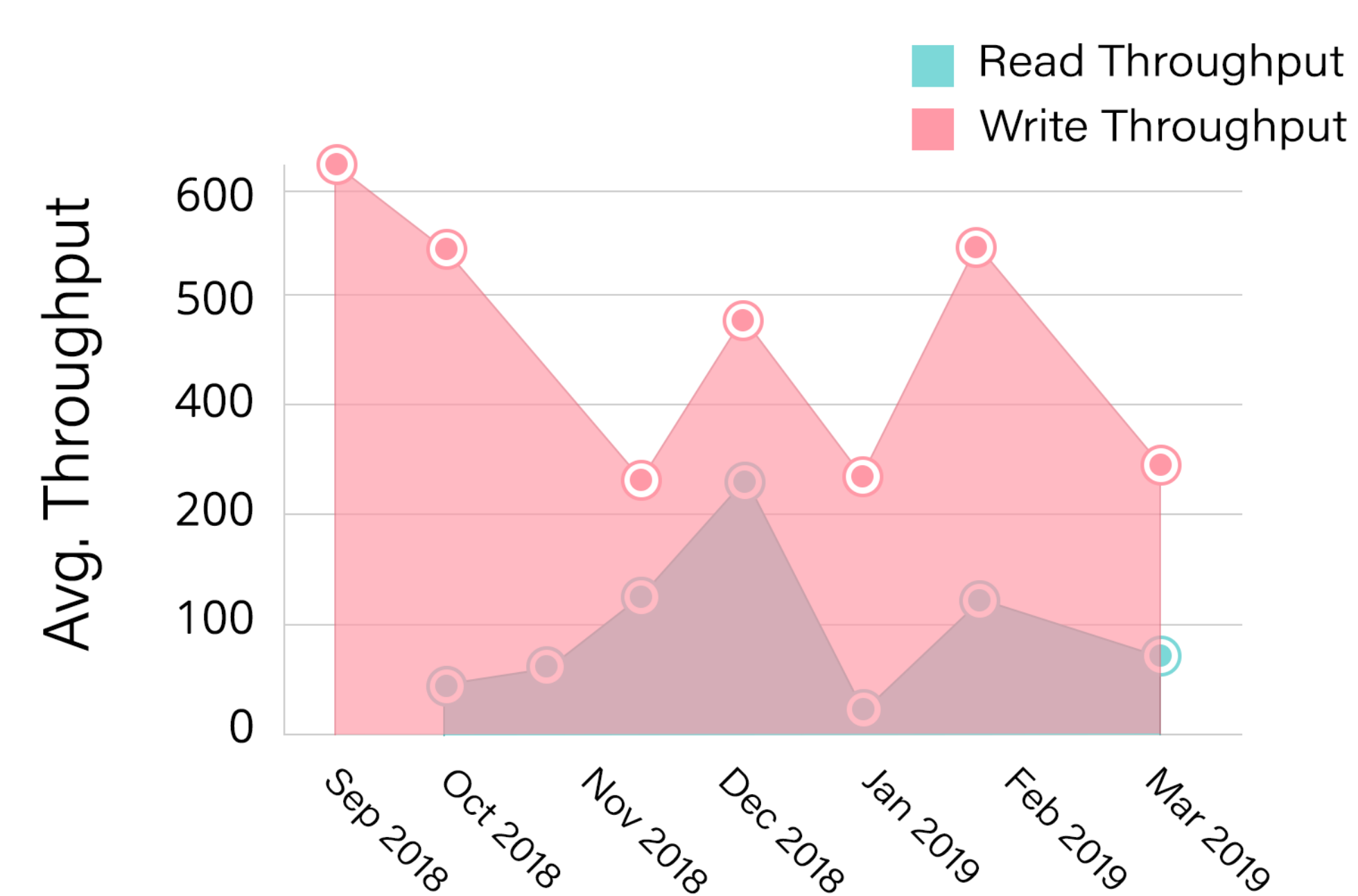
Avg. EC2 and RDS instances running



EC2 network traffic

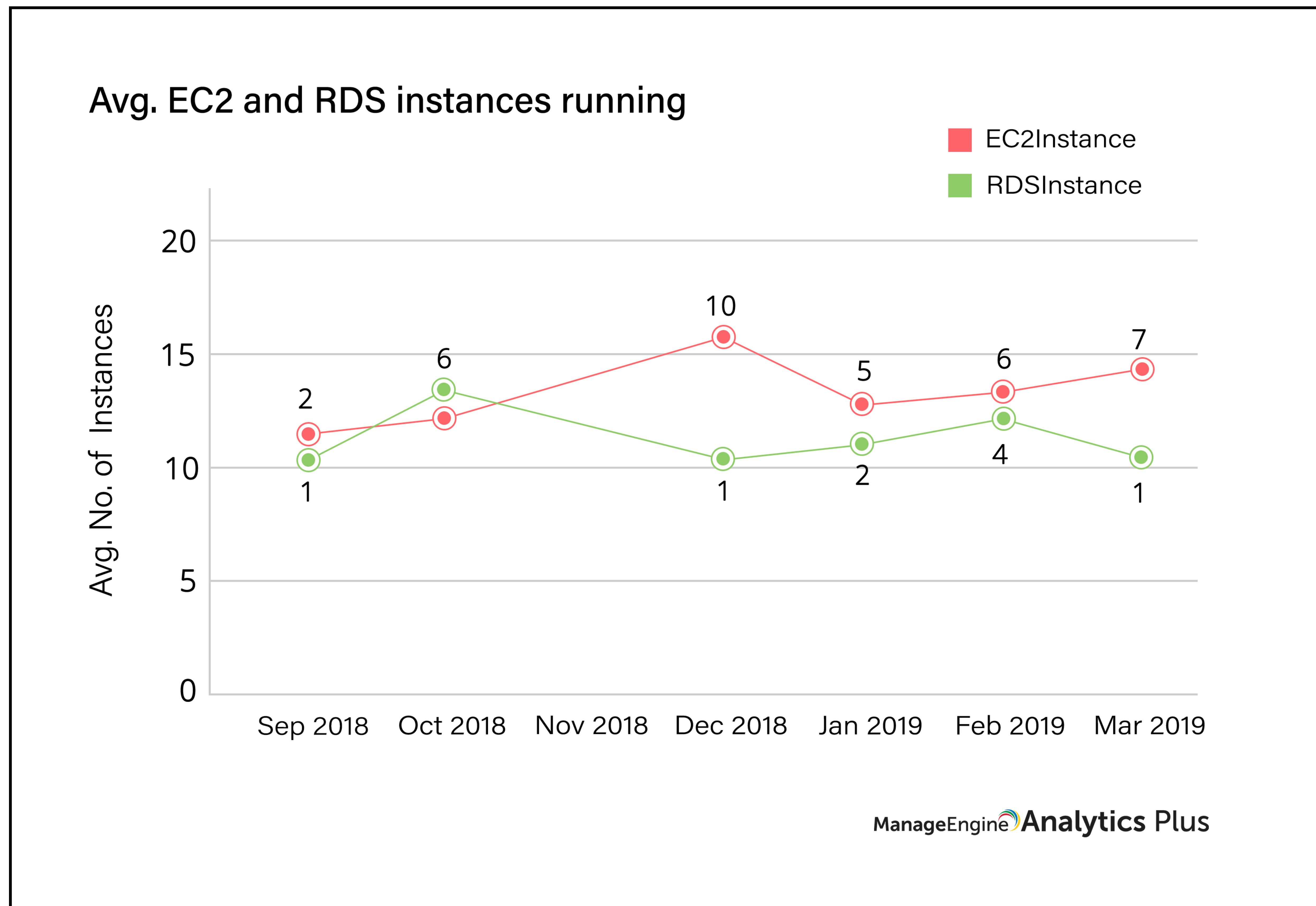


RDS network traffic



ManageEngine Analytics Plus

The widgets at the top display the number of available AWS monitors as well as EC2 and RDS instances respectively, while the graphs below provide a visualization of their utilization patterns. Let's compare the EC2 and RDS instances usage patterns.



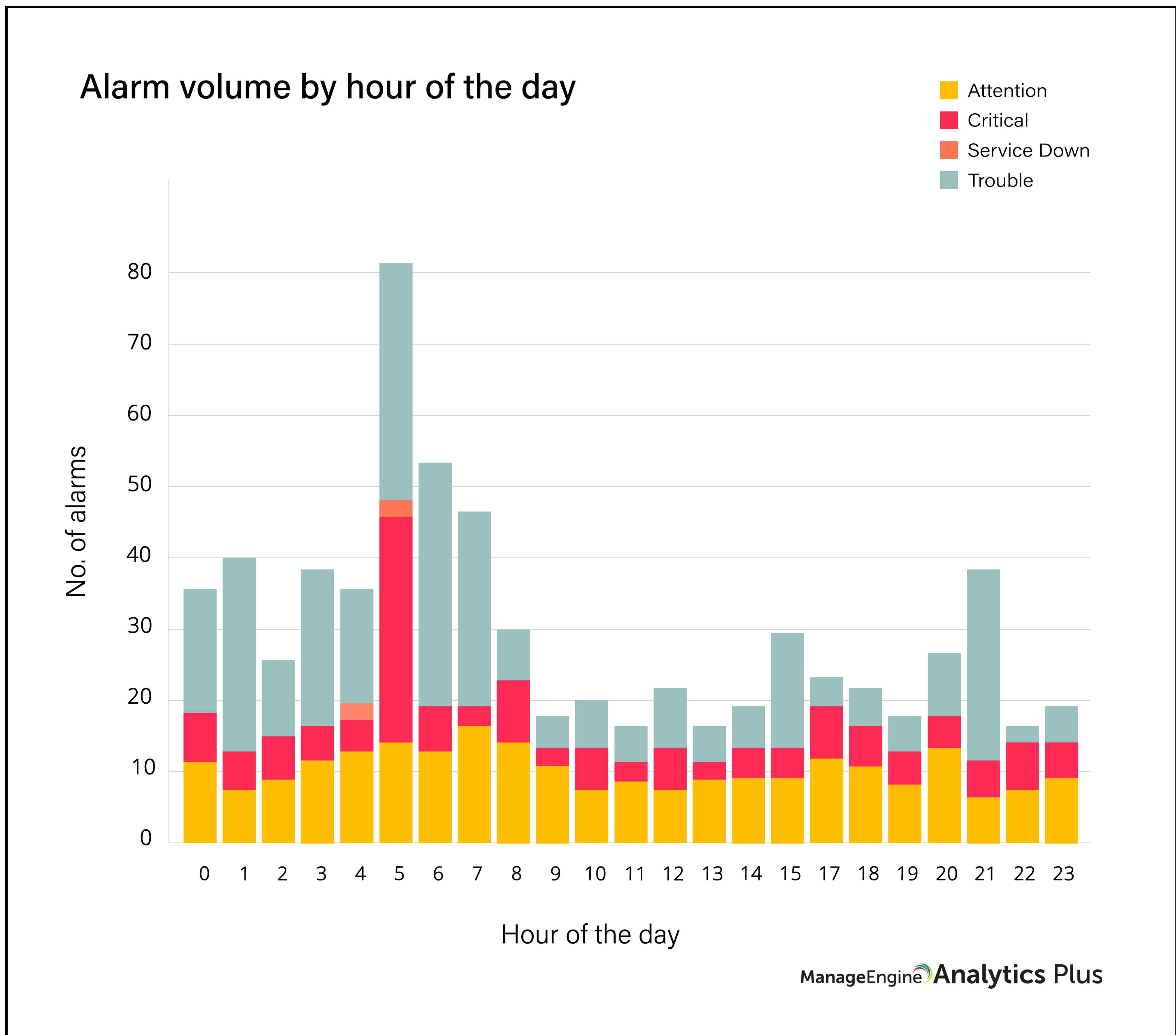
As you can see, with only 10 of the 14 available instances being used over an eight-month period, Amazon EC2 instances are underused, while there aren't enough RDS instances to meet requirements. Based on this information, actions can be established to shut down unused EC2 resources, or purchase additional RDS resources.

Such insight into infrastructure utilization trends can help IT managers plan and optimize resource utilization to reduce billing overage and achieve a better price-performance ratio.

2. Analyze alarm trends to minimize downtime

Although application and network monitoring devices offer advanced features to improve alarm forecasting, IT managers often get misled by overinflated or underinflated forecasts. This is because alarm forecasting is based on historical volume and doesn't take the underlying root cause into account.

The report below shows the alarms generated by a router in the last 24 hours.



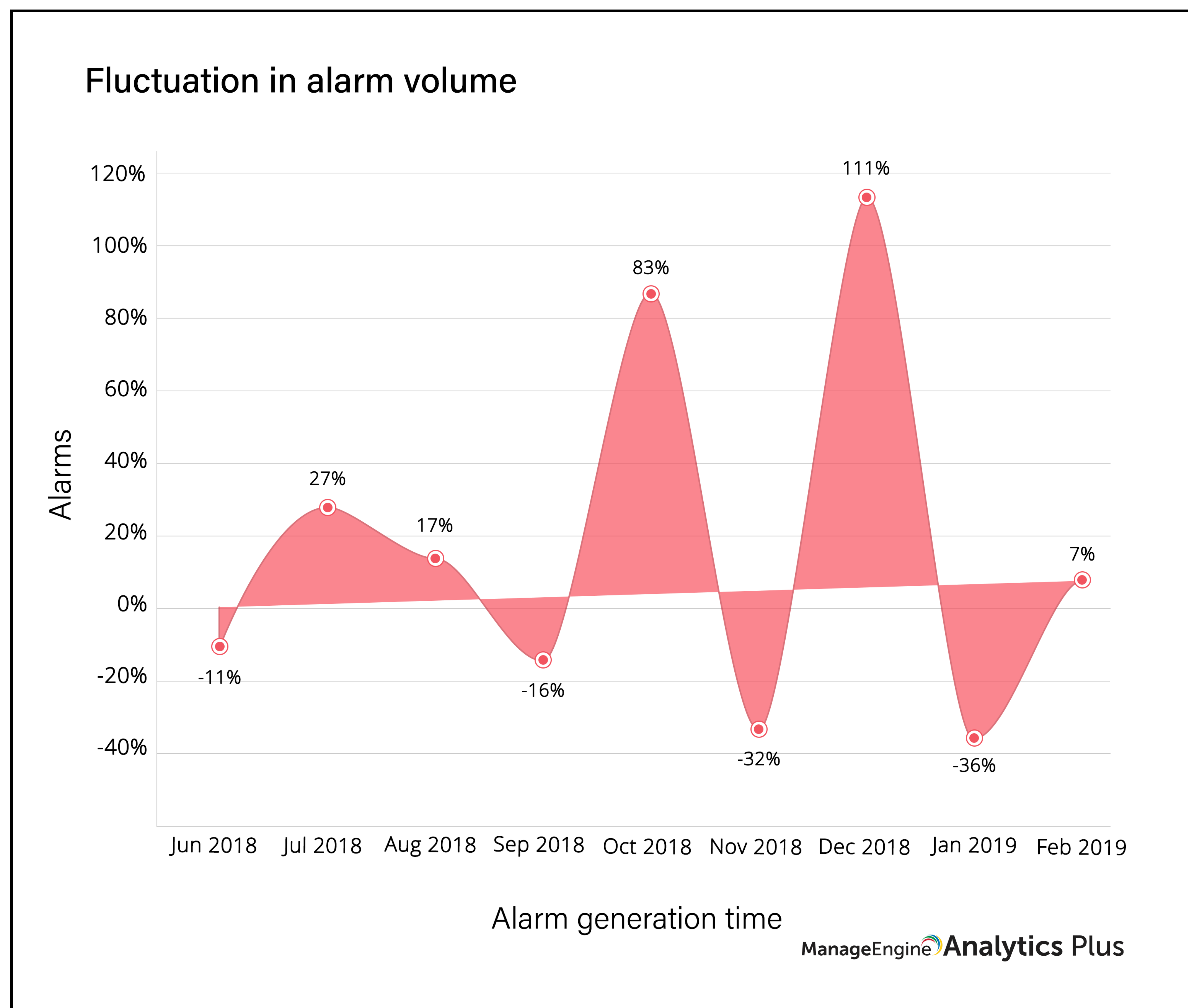
You can see an unusual spike in the alarm volume at 5am. This could be due to several reasons, including high CPU or memory utilization, huge traffic flow, or faulty configuration changes. Without knowing the proper root cause, it's impossible to predict the alarm volume for the next day. Let's look at the activity report for the last 24 hours to see if there's a correlation.

Hourly activity report

Hour of the day ↓	Top event ↓
0	SSLCertificate monitor
1	DB2 server backup
2	Cassandra server maintenance
3	Apache server maintenance
4	Linux install
5	Ghostscript security update (CESA-2019:0229)
6	Server monitor
7	Switch monitor
8	Tomcat server backup
9	IIS server update
10	Windows Malicious Software Removal Tool x64
11	AWS server backup
12	URL monitor
13	VMWare ESX/ESXi
14	Redis update
15	Load balance
16	Firewall installation
17	Windows 8 installation
18	Daemon and tooling that enable snap packages
19	PDF rendering library (USN-3886-1)
20	Library to read/write archive files (USN-3884-1)
21	Secure access to remote machines
22	Router monitor
23	SAP monitor

This report shows a scheduled patch running at 5am. Scheduled patches are known to cause high CPU and memory usage during updates, and understanding such underlying causes can help IT managers accurately predict alarm volumes.

Besides identifying and investigating anomalies, it's important to look into alarm fluctuations while analyzing alarm volumes. A steady volume of alarms with minor deviations is acceptable; however, drastic fluctuations in alarm volume is a cause for concern, and it points to failures in the network.

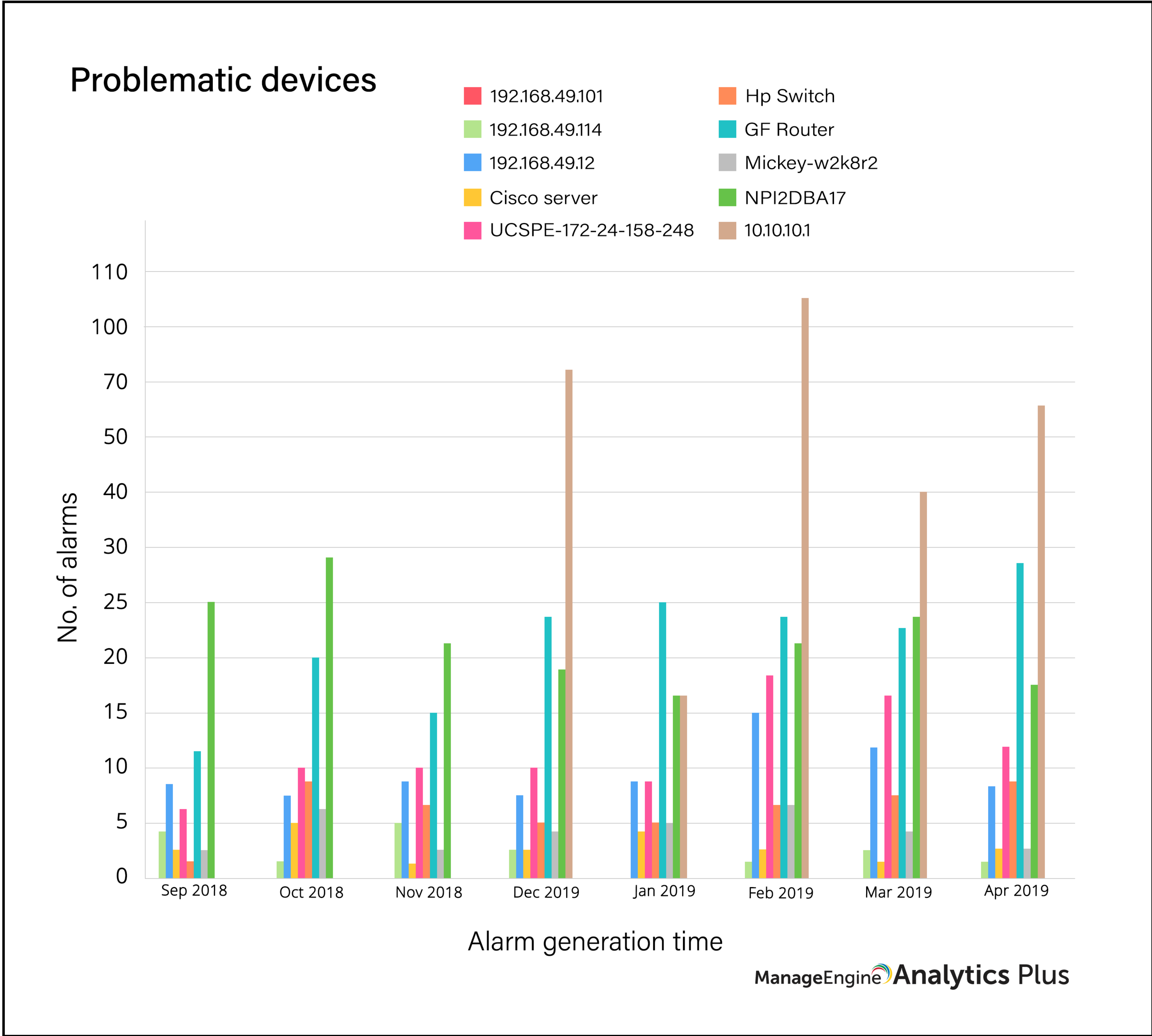


It's important to monitor anomalies in alarm patterns and fluctuations in alarm volume. The information collected from doing this, combined with the operational knowledge of what's causing these alarms helps you actively predict alarm volume and prepare for any failures that could disrupt your network or applications.

3. Identify and eliminate problematic devices

The number one cause of network failures are problematic devices. These include faulty devices, devices with incorrect configurations, and devices malfunctioning due to wear. Left unnoticed, these devices can hamper network performance and cause serious damage, including lack of access to mission-critical application or services, isolation of remote servers, and in worst cases, a complete shutdown of business operations. This is why it's vital to monitor such devices.

The report below gives you a list of devices generating the most alarms over a period of six months.

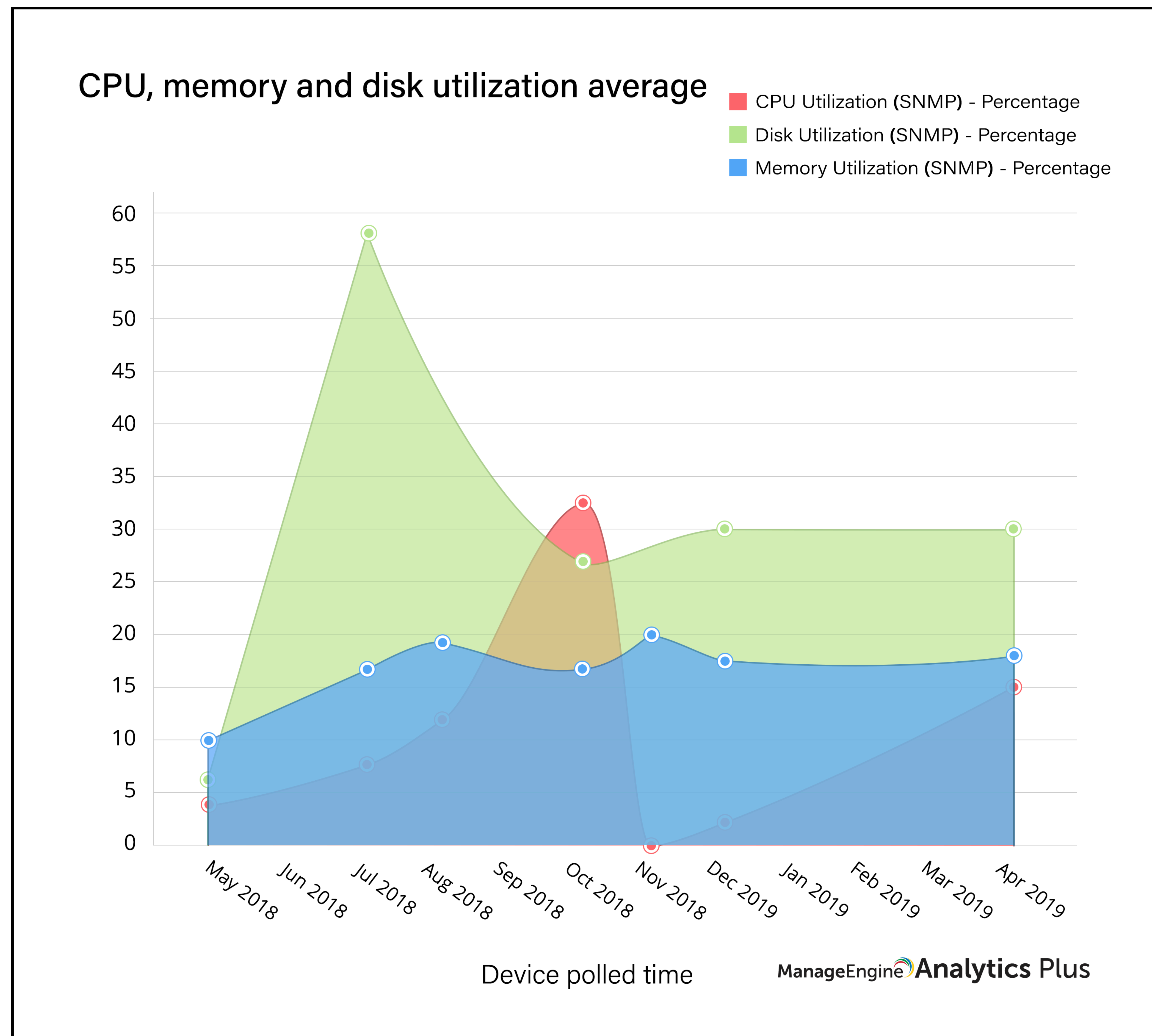


Based on this list, IT managers can identify the most problematic devices and do an inventory check to distinguish between devices causing network problems due to configuration errors and devices malfunctioning due to end of life. For example, a DNS server or a router may be causing problems due to improper configurations, whereas an OS could be causing problems due to being outdated.

Analyzing the historical trend of problematic devices helps you predict which devices are likely to fail and when, so you can proactively reconfigure or replace those devices in time to minimize the impact on business and ensure service continuity.

4. Forecast storage capacity needs

A [2016 survey predicts enterprise data](#) volumes will increase by 33 percent each year, and SMB data volumes are expected to more than double. While forecasting storage requirements, organizations take this ballooning data volume into account, but assume that existing servers are being used optimally; however, this might not be the case. A thorough analysis of past usage patterns can reveal drastic fluctuations in server usage over time.



The above example demonstrates a typical use case where memory utilization has been fairly consistent over the past year, while CPU and disk utilization patterns have experienced inconsistencies and sudden spikes.

Tracking memory and disk utilization trends can reveal specific patterns in your storage requirements, and it can also help you forecast your organization's storage capacity needs. For example, you may notice that storage systems are near their full capacity levels during a change implementation process. This could be due to different teams backing up applications. Understanding similar patterns in your storage capacity usage trends can help you predict your organization's data storage requirements, allowing you to create backup plans in case of emergencies.

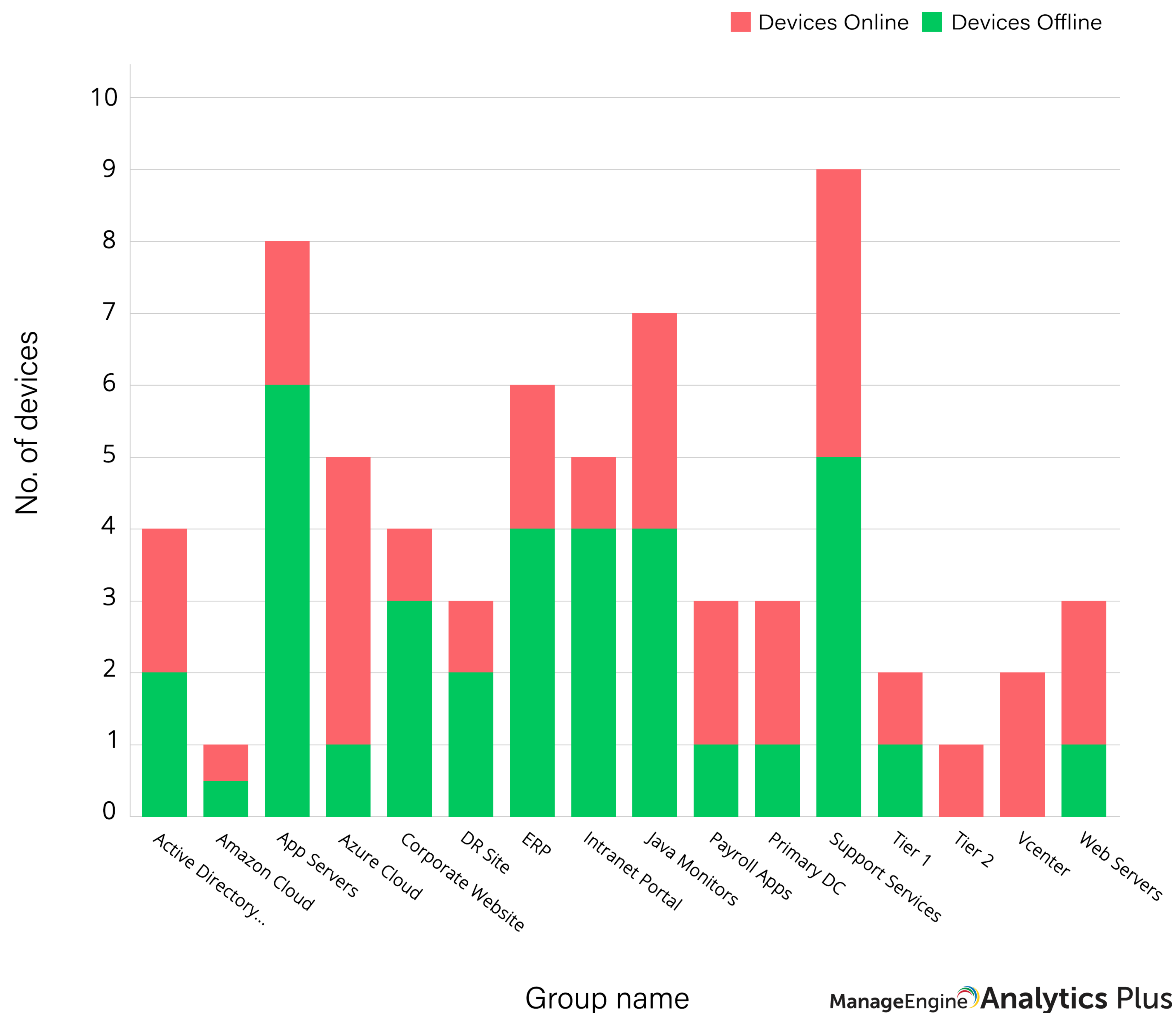
5. Avoid network disasters

Industry experts agree that typical network availability must always be at 99.99 percent. This means the allowed network downtime is about 1.01 minutes for a week and 52.6 minutes for a year. In such a competitive business landscape, it's important to adhere to these critical metrics, otherwise you could experience huge revenue losses.

The best way to proactively avoid such network disasters is to monitor these network devices for availability, and identify the ones that are frequently down; this way you can build a fallback mechanism for emergency situations.

Here's a sample report:

Monitor group by device availability



Viewing the number of devices available under each monitor group lets you clearly understand the current network service quality, and it enables you to estimate the impact on business when a device goes offline. This allows you to plan and embed fail-safe keys into your network devices as a stop-gap measure to avoid network disasters and ensure continued network availability.

6. Unify ITSM and ITOM for agility and service reliability

IT service management (ITSM) and IT operations management (ITOM) are the parallel tracks that power your business engine. Without proper coordination between the service and operations teams, your business can easily get derailed. For example, if there's a network outage, employees' inboxes will fill up with notifications from the different monitoring services, and both the Service and the Ops team may begin to work on the issue independently. This can lead you to believe that you're dealing with multiple incidents, when in reality, it's only one.

Tying in ITSM and ITOM metrics is the key to achieving operational efficiency. Once you understand how network activity is related to user-reported issues, it becomes easy to diagnose and quickly resolve issues.

Here's a combined ITSM and ITOM dashboard that offers a side-by-side comparison of alarm trends and service requests:

ITSM + ITOM

Incidents triggered by alarms

24

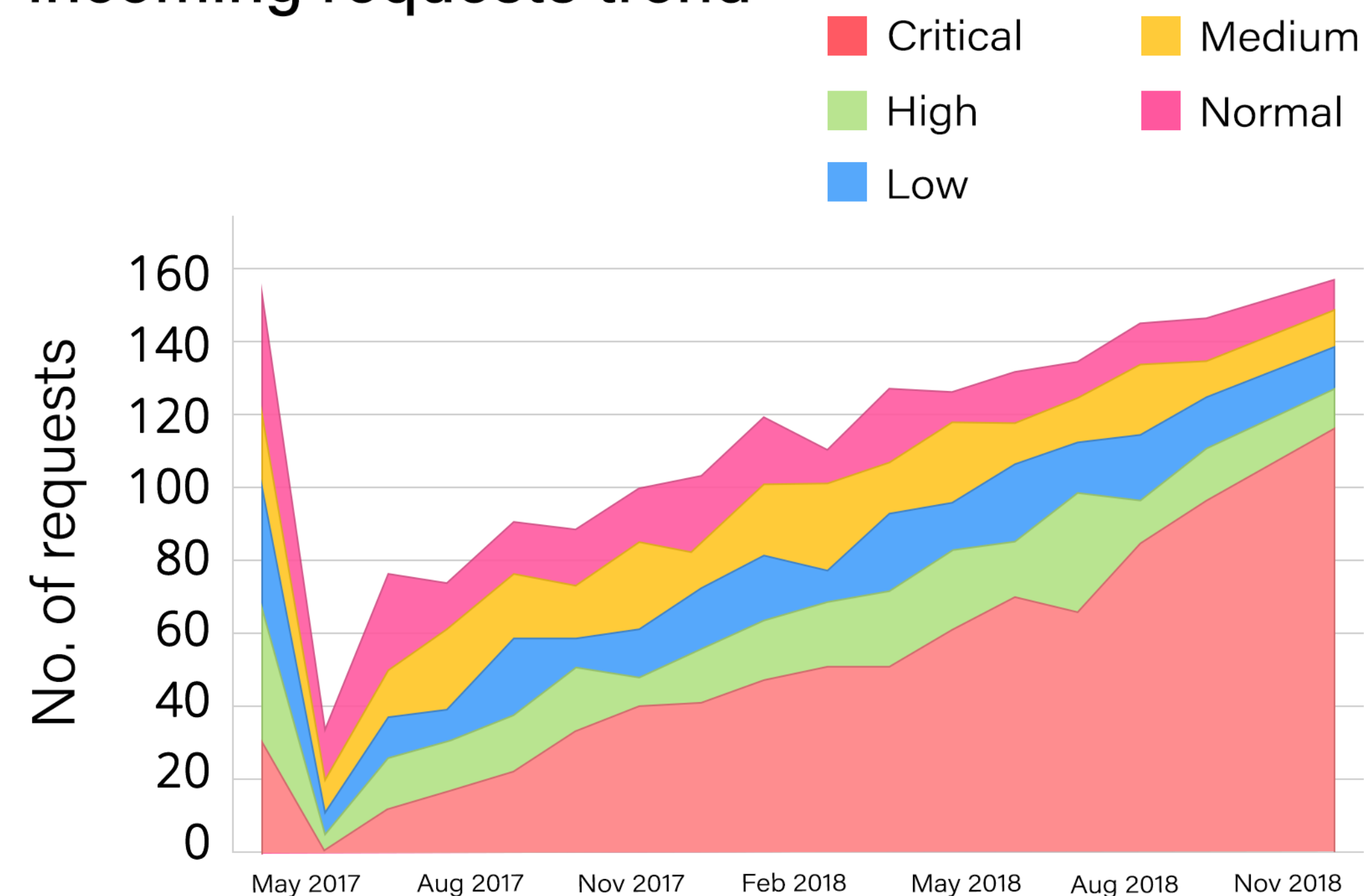
Incidents awaiting NOC update

3

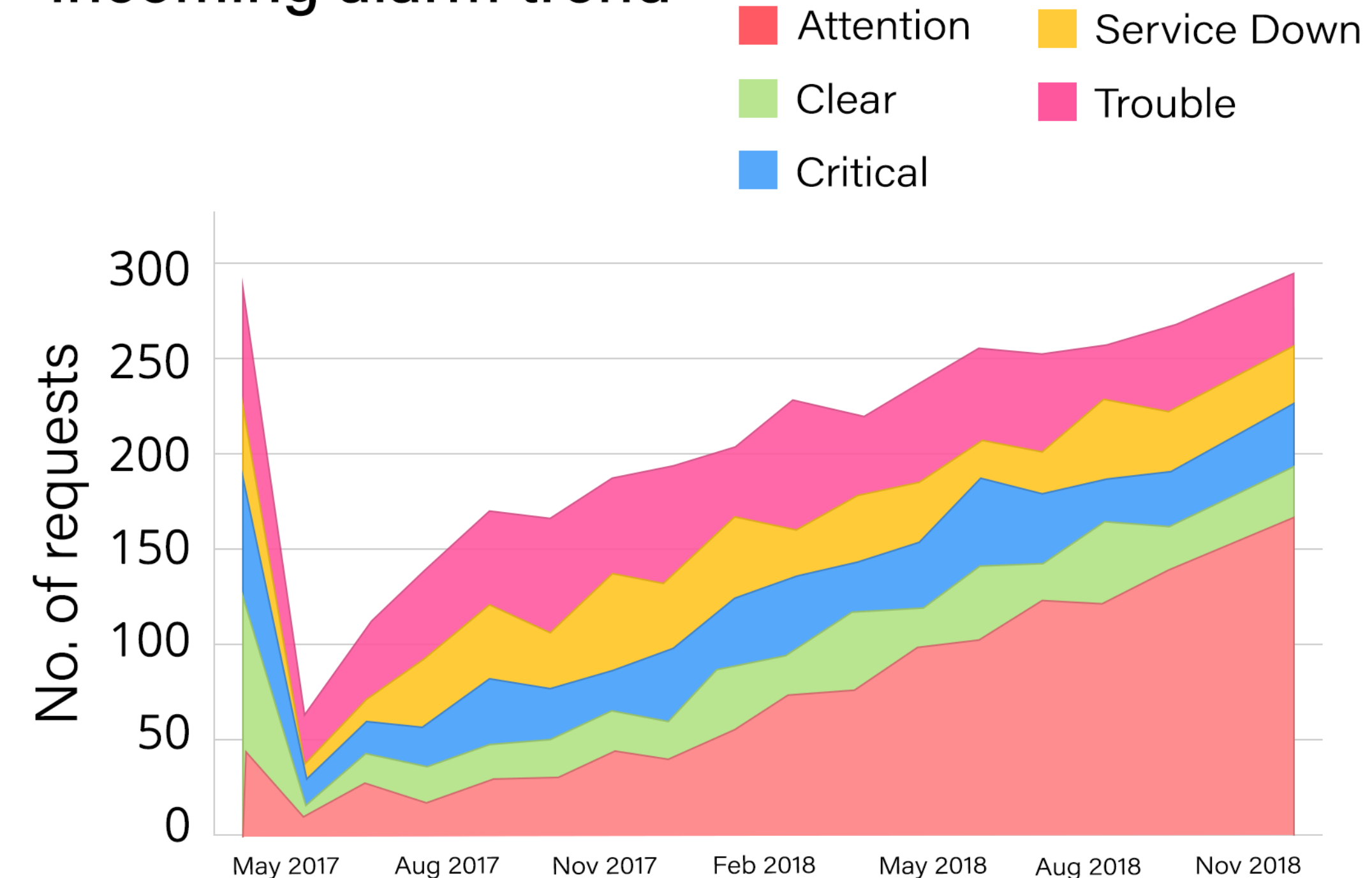
IT service most affected by downtime

Applications

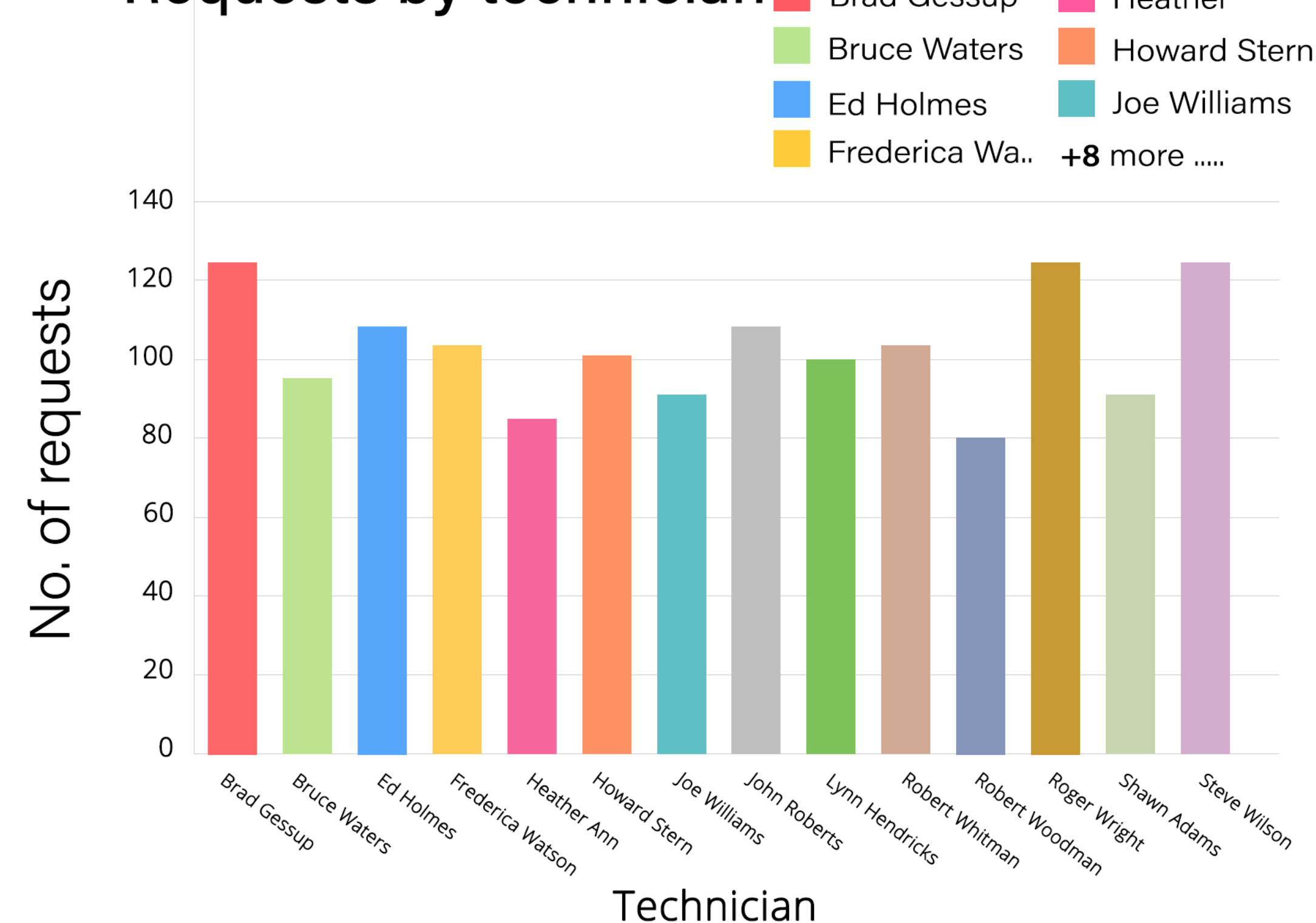
Incoming requests trend



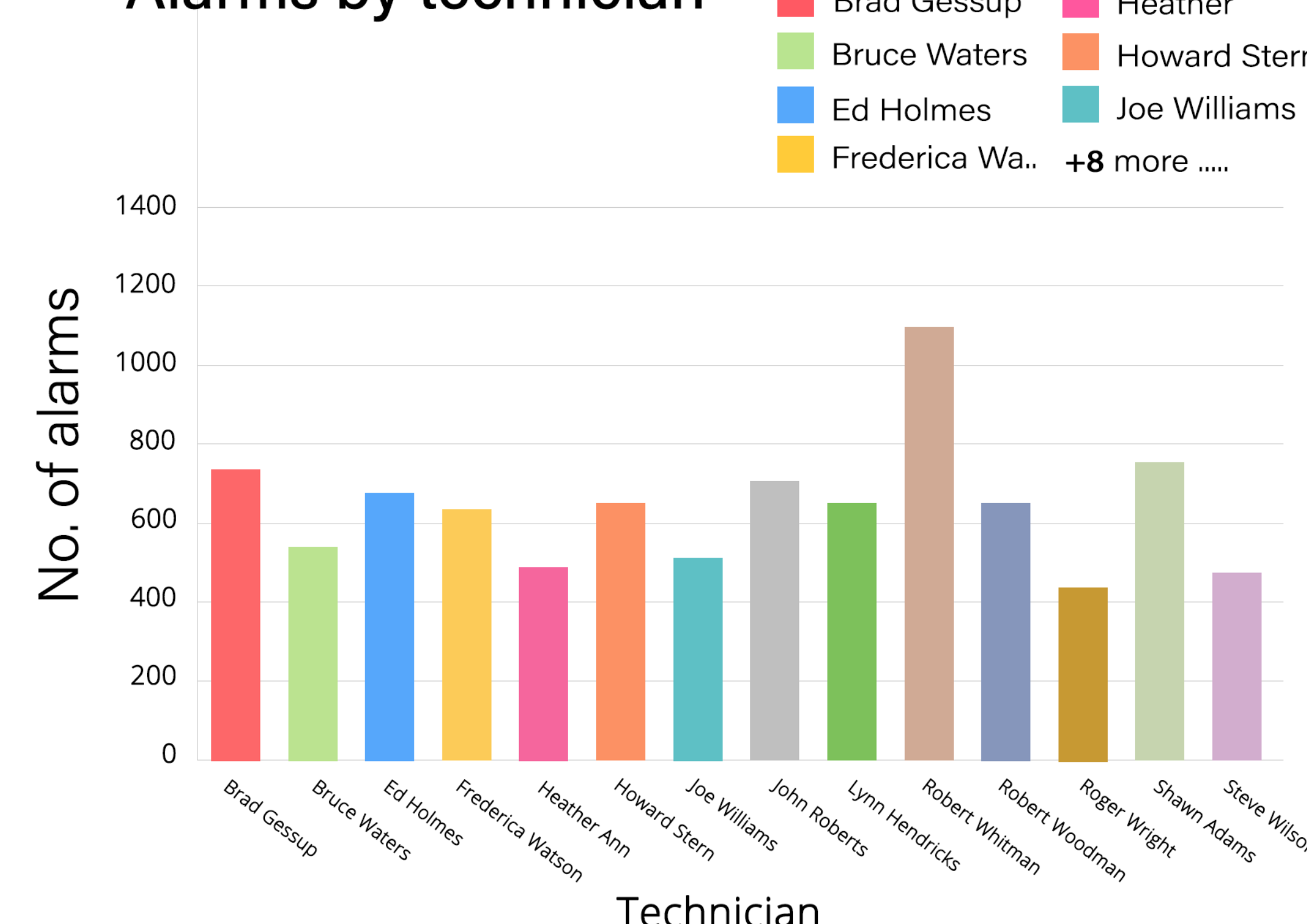
Incoming alarm trend



Requests by technician



Alarms by technician



ManageEngine Analytics Plus

As you can see, every time there's an increase in the number of alarms, there's also a corresponding spike in the incoming request volume as well. Seeing this can help you optimally plan resource allocation so that high-priority incidents are tended to immediately, and SLAs are maintained.

Moreover, having a deeper understanding of the relationship between IT incidents and the volume of service requests allows service teams to provide speedy resolution times.

For many IT teams, being proactive in operations management can be a challenge. However, by leveraging unified insights from ITSM and ITOM, IT managers can proactively improve service-level efficiency, as well as ensure high availability of business services.

Conclusion

Proactive applications and network management delivers numerous benefits to the IT department including:

1. Quicker identification and resolution of issues.
2. Reduced MTTR (mean time to repair) for incidents.
3. Increased network uptime and resource availability.
4. Improved compliance with SLAs.
5. Smoother customer experiences.
6. Increased productivity and service reliability.
7. Decreased total cost of ownership and maintenance.

About Analytics Plus

[Analytics Plus](#) is a self-service, IT analytics solution that lets you visualize your system data in the form of colorful charts, reports, and dashboards. It offers out-of-the-box integrations with ManageEngine Applications Manager, OpManager and other ManageEngine tools that give you an in-depth look at your IT infrastructure. It features a simple drag-and-drop reporting interface that eliminates the need for a data analyst to help your help desk managers optimize operations and improve service delivery.