

BACK TO WORK:

AN IT ADMIN'S GUIDE





Back to work: An IT admin's guide

Introduction

As confidence in the effectiveness of vaccination builds and restrictions on social gatherings ease around the world, several organizations are mulling over the idea of letting their employees return to the workplace. Though it may take a few more months to witness pre-pandemic occupancy levels in office buildings, it seems increasingly closer to the horizon. We are set to observe a variety of reopening strategies in play, which will be largely defined by the type of industry. While companies in the manufacturing sector that rely on physical labor go for full occupancy, technology companies can expect to start with a hybrid model—giving employees the choice of remote or in-office work.

IT teams played a pivotal role in enabling remote work and will similarly have a central part in facilitating the various return-to-work strategies. While the shift to remote work happened almost overnight, returning to work will be a gradual process, giving IT teams time to prepare. However, IT teams can expect this transition to be more challenging than the last due to the wide range of aspects they have to pay attention to, such as ensuring there's sufficient bandwidth to handle a hybrid work setup, handling higher incident volume, and ensuring network security.

This e-book outlines some challenges IT teams can expect and possible ways they can prepare for employees returning to work.

Run pre-checks to categorize endpoints by risk factor

With most of your endpoints reconnecting to the corporate network after a long gap, it is necessary to perform a pre-check before allowing them to access sensitive sections of your network or server infrastructure. Classify your endpoints into two sections: those that have passed a pre-check and those that have yet to do so. Endpoints that have passed the pre-check can be allowed to access sections of your network that hold sensitive corporate data.

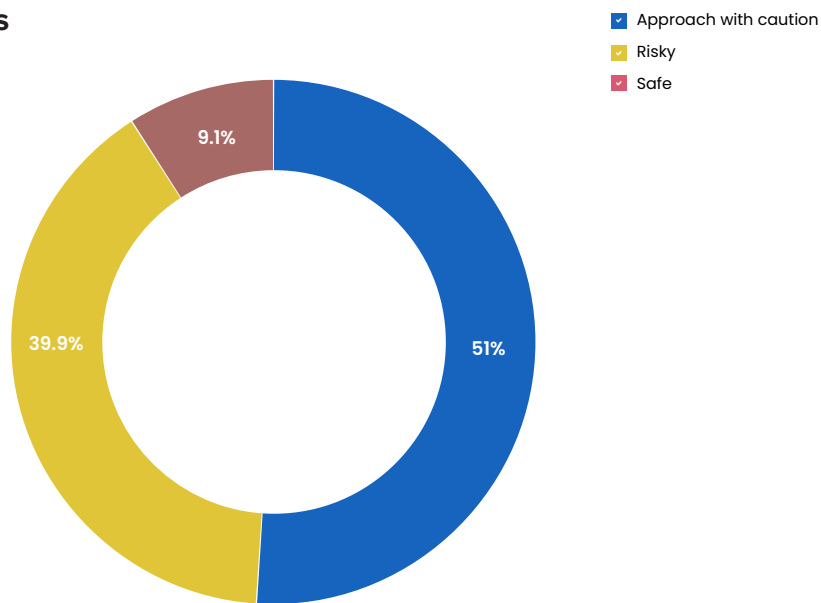
Two parameters that can be used for the pre-check are:

- Presence of critical patches.
- Antivirus and firewall status.

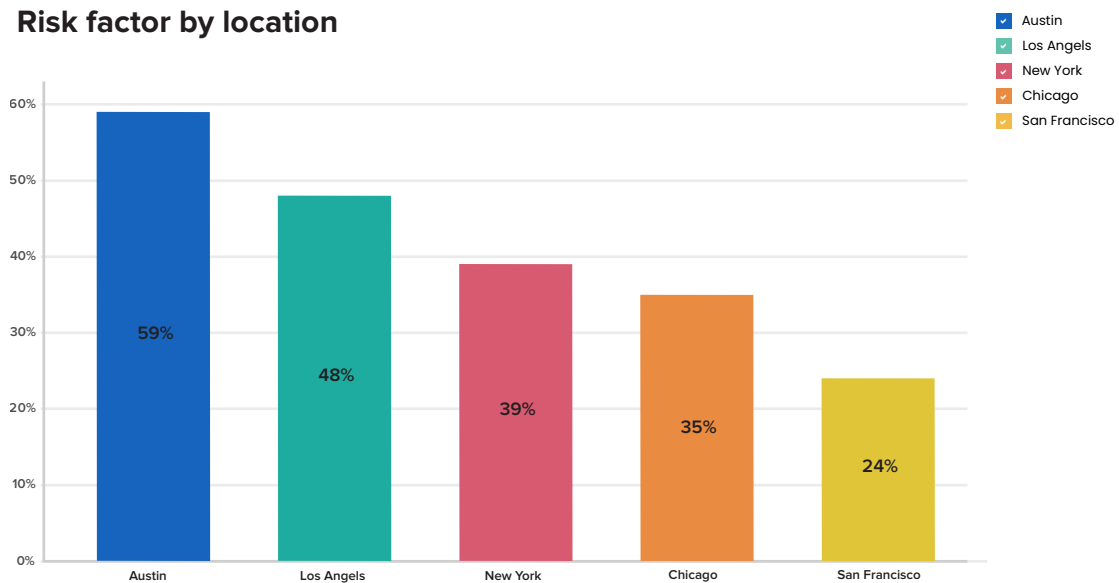
Security patches and antivirus applications are the first line of defense against malicious attacks. With remote work becoming the norm, the percentage of endpoints falling prey to external attacks has soared. Estimates show there were as many as 192,000 coronavirus-related cyberattacks per week in May 2020 alone, a 30% increase compared to April 2020 (Source: Unisys).

While there are various angles one can look at while trying to judge an organization's patch deployment posture, a good place to start is by looking at a distribution of endpoints that are missing critical patches. Categorize endpoints as "safe," "approach with caution," and "risky" based on the number and nature of missing patches. Then create a branch-wise report (or department-wise report, if you run operations only out of a single location) to pinpoint branch offices that have a bigger share of endpoints missing important security updates.

Risk categories



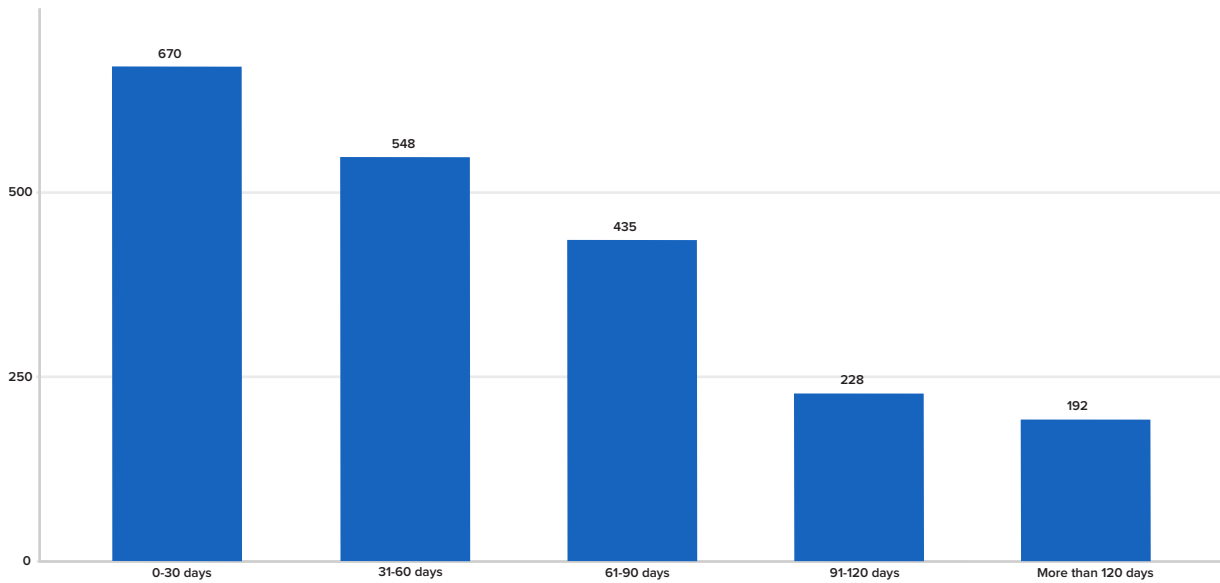
Risk factor by location



IT admins can dig deeper into the magnitude of this problem by looking at the age of missing patches.



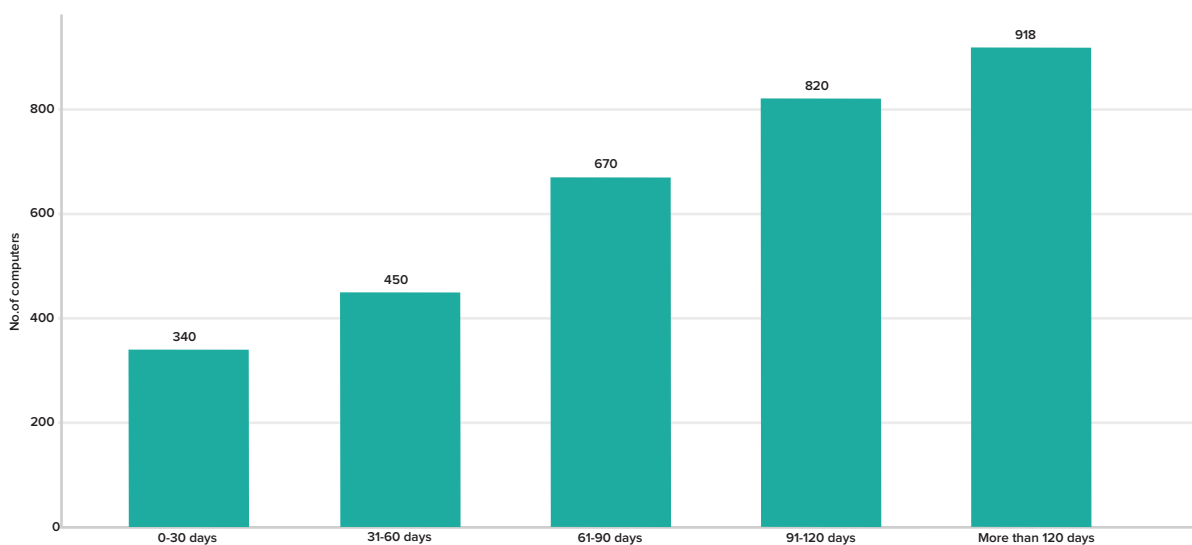
Missing patches by release timeframe



An endpoint running outdated antivirus software is as good as one that doesn't have antivirus installed. Antivirus software must be enabled on each endpoint and updated with the latest virus binaries.



Lapse in antivirus update



Flag all assets associated with a security-compromised user

In the event that a critical vulnerability is detected on a user's workstation or mobile phone, it is likely that all the other devices associated with the user are also exposed to the same vulnerability. Block all the devices the user owns from connecting to your corporate network.

A user entity relationship report can help quickly identify all the devices owned by a particular user. Components such as USB and network ports that will allow users to connect to the corporate network will have to be disabled until the devices are scanned for vulnerabilities.

Asset ownership

	User	Device type	Device name	Owned by	Ownership period (days)
1	Alice Simms	Desktop	Alice-412	Private	830
		Tablet	Alice-183	Private	390
2	Katniss Darr	Laptop	Karen-560	Corporate	430
		Laptop	Kat-120	Corporate	560
3	Sam Neils	Desktop	Sam-350	Private	450
		Tablet	Sam-148	Private	320
4	Karen Jacobs	Smartphone	iPhone480	Corporate	520
		Smartphone	iPhone228	Corporate	280

Review the software installation history on infected devices to check for unusual or unintended software that could have served as the gateway for infection. Software detected this way should be added to the prohibited software list to prevent other users from installing it.



Software audit history

	Asset name ↓	Update type ↓	Datetime of Time ↓	Action performed ↓	Performed by ↓
1	Alec-180	Software installation	18 May 2021, 12:16:22 PM	Microsoft Office Excel Viewer was Installed	Script scan
2	Greg-114	Software installation	29 Dec 2019, 03:09:20 PM	Adobe Flash Player 10 Plugin was Installed	Script scan
3	Jack-134	Software installation	30 Dec 2020, 11:12:39 AM	Kaspersky Security Center 10 Network Agent was Installed	Script scan
4	John-312	Software installation	10 Sep 2019, 04:35:52 PM	Microsoft OneDrive was Installed	Administrator
5	Kara-450	Software installation	07 Dec 2020, 10:12:39 PM	LibreOffice 5.1.3.2 was Installed	Script scan
6	Mac-140	Software installation	17 May 2021, 04:33:18 PM	Google Chrome was Installed	Administrator
7	Mills-320	Software installation	08 Feb 2020, 10:12:39 PM	Mozilla Firefox 47.0.2 (x86en-US) was Installed	Administrator
8	Neil-141	Software installation	18 May 2021, 12:18:44 PM	Realtek Audio COM Components was Installed	Administrator
9	Reid-345	Software installation	23 Jan 2021, 12:22:38 PM	Mozilla Maintenance Service was Installed	Administrator
10	Sam-120	Software installation	16 Feb 2021, 12:15:26 PM	Intel (R) Chipset Device Software was Installed	Administrator
11	Tara-167	Software installation	17 May 2021, 04:33:06 PM	Notepad++ (32-bitx86) was Installed	Administrator

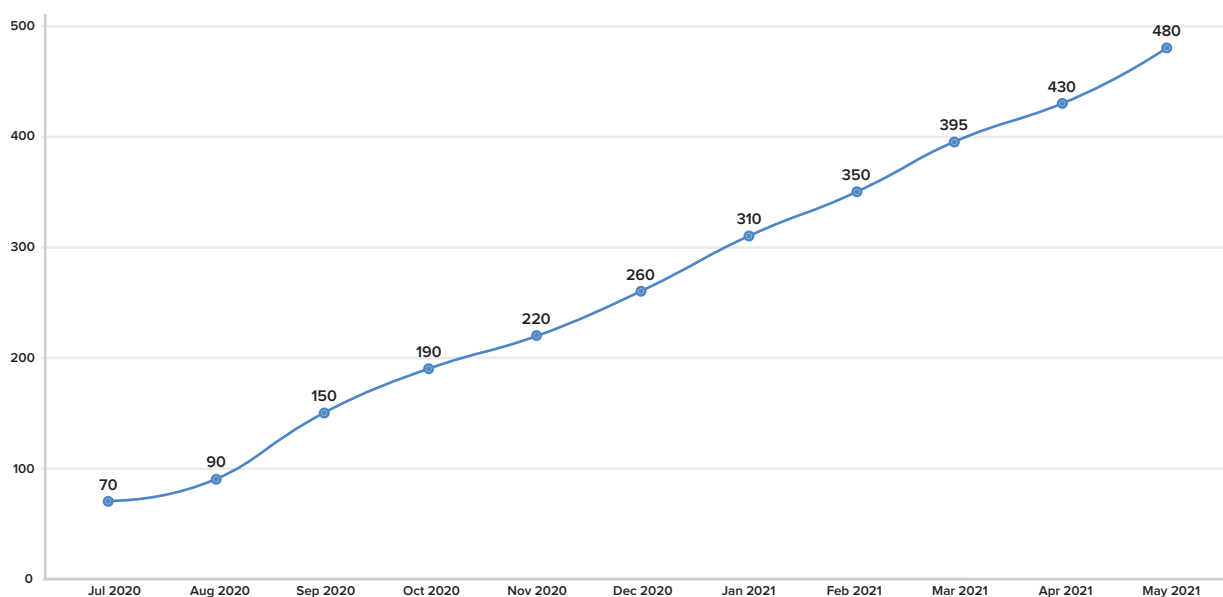
Clear backlogs before the office reopens

For IT admins and technicians, remote work has removed the convenience of walking up to a user's laptop and fixing issues in person. Though software-related issues can be troubleshooted remotely, hardware-related issues need to be dealt with in person. Owing to logistical challenges, such hardware fixes may have been put on hold in anticipation of remote work ending within a short span of time. With remote work extending beyond expectations, it is likely such requests have accumulated over time.

IT admins should review such backlogs and start chipping away at them before offices open permanently. Failing to do so will add to the daily workload, keeping technicians from getting to high-priority issues.



Backlog trend



Prepare for high incident volume

Accurately forecasting the volume of incidents IT help desks can expect upon a full-fledged reopening is quite difficult, especially in an unprecedented event such as a post-pandemic reopening. Needless to say, there will be a considerable increase in the flow of incidents once people return to the office.

This increase can be attributed to users putting up with minor issues with their corporate devices during remote work knowing very well that the problem might need hands-on troubleshooting. Such users can be expected to flood the help desk with issues once they resume on-premises work.

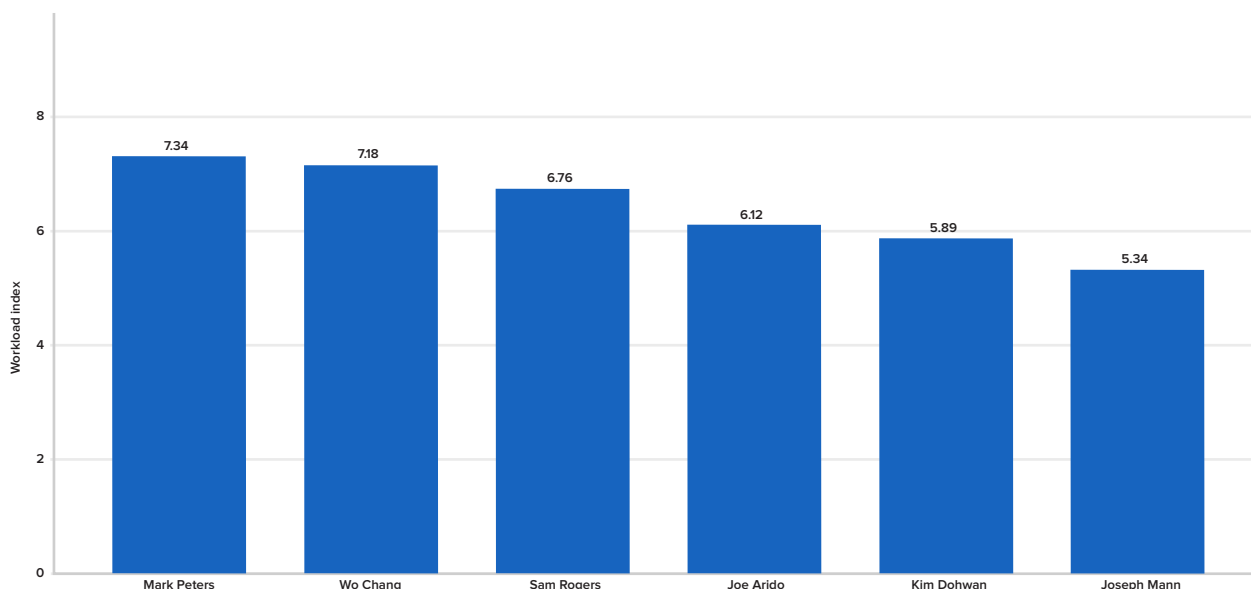
IT help desks can prepare by ensuring an adequate number of technicians are available to handle increased incident volume. The technician workload index is a good measure to check the current workload your technicians are handling and if there is room for additional tasks. If help desk technicians are already experiencing a higher workload, it is wise to hire more hands to handle higher incident volume.

The technician workload index can be calculated using the following formula:

$$\text{Technician workload index} = \frac{\text{Total number of requests assigned to a technician}}{\text{Average time available to resolve}}$$



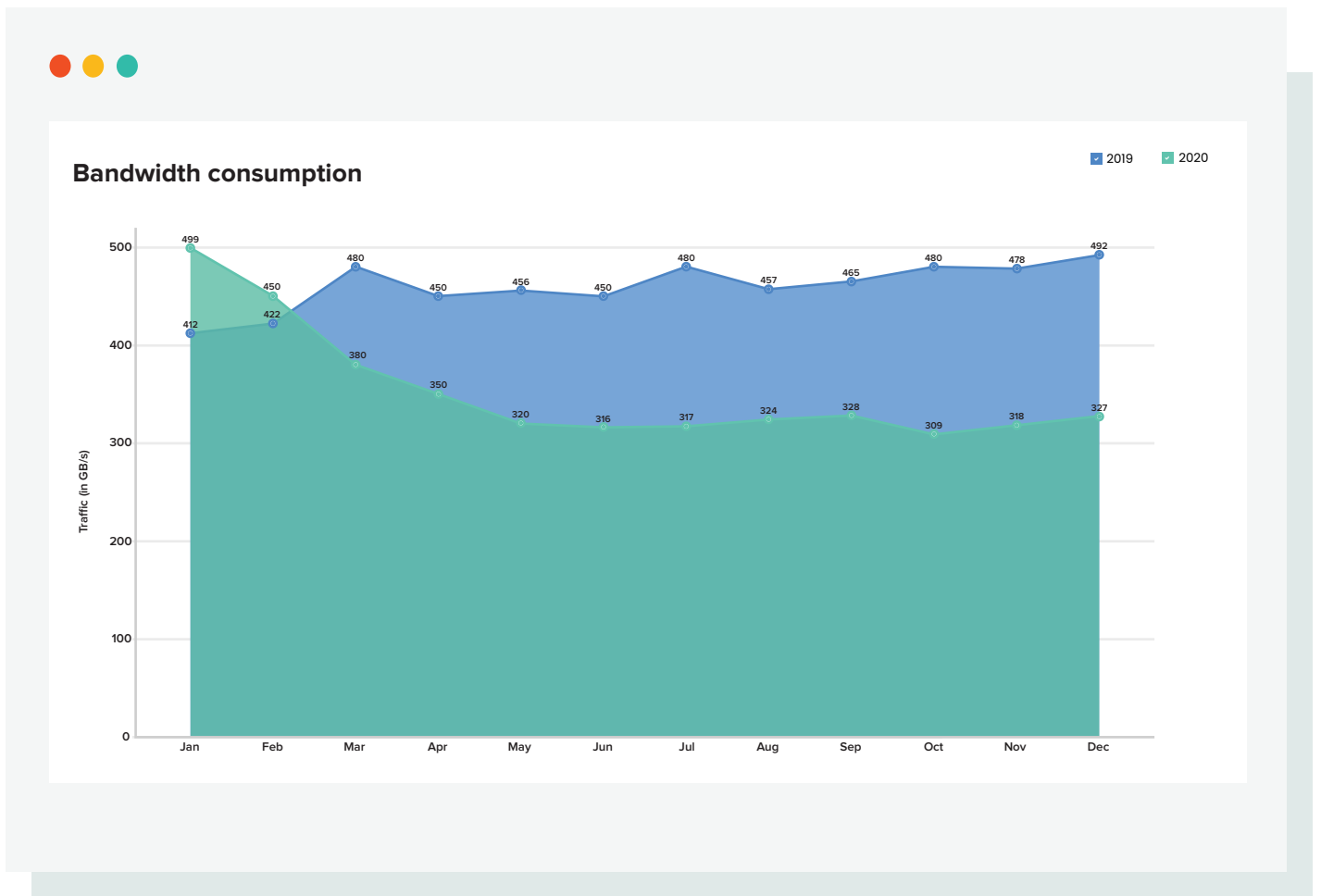
Technician workload



Plan for increased bandwidth requirements

When employees shifted to remote work, several organizations redirected their network resources to support services such as VPNs to let users connect to corporate infrastructure from remote locations. While this was a no-brainer, network planning for a return-to-work process might not be so straightforward.

With several organizations experimenting with a hybrid work model, IT teams have to ensure there is sufficient network bandwidth to support employees in the office as well as remote users. IT teams have to look at historical bandwidth consumption before and during remote work and use this data to calculate bandwidth requirements.



Increasing bandwidth capacity to about 1.5 times the average consumption in 2019 and 2020 can help organizations meet the demands of a hybrid work model.

Bandwidth calculation = $((\text{Average traffic in 2019} + \text{Average traffic in 2020})/2) \times 1.5$

Build a back-to-work dashboard

We've identified a key set of metrics and best practices that organizations should keep in mind while getting their back-to-work game plan in place. These metrics may vary in level of importance from one organization to another, and metrics are only as effective as how they're put to use. As organizations progress through supporting either a full-fledged work-from-office model or a hybrid one, it is important that IT admins keep track of all these important metrics.

A back-to-work dashboard can collate these KPIs in a central pane of glass, helping IT teams keep track of progress and perform course corrections when needed.

Applications that specialize in IT analytics, such as Analytics Plus, can not only offer the metrics discussed in this e-book out of the box but can also help IT teams build customizable back-to-work dashboards for organization-wide visibility.

Here's an example of a dashboard that IT teams can use to track their back-to-work preparedness and progress



Back-to-work tracker

Employees on site
413

VPN users
2356

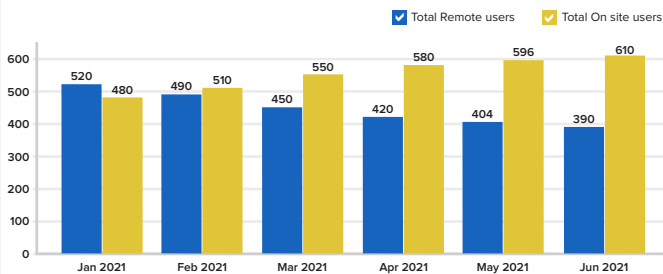
% of endpoints at risk
36.0%

Antivirus up-to-date
28.0%

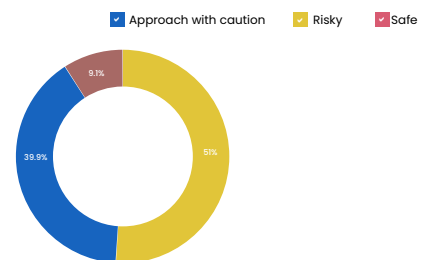
Backlog queue
134

Password reset skipped
1289

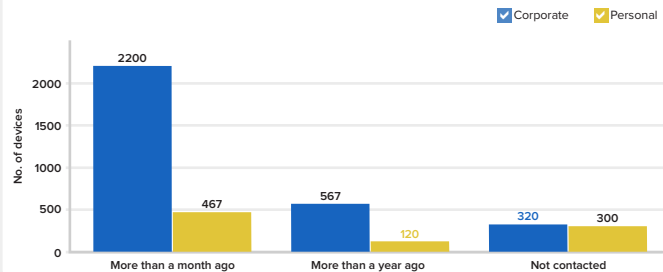
Trend of on-site vs remote users



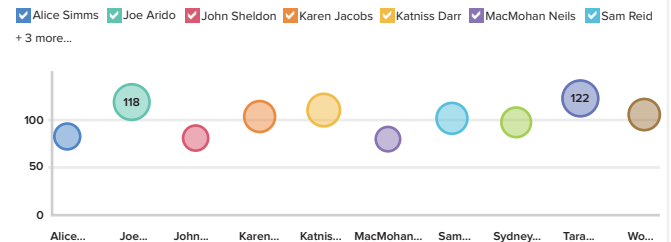
Risk categories



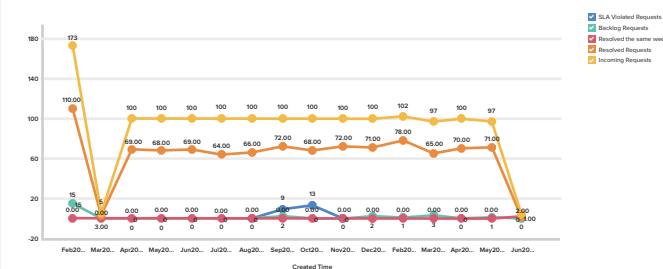
Device contact time frames



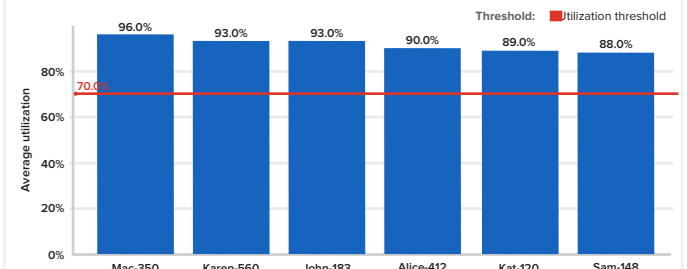
Technician load



Incoming, Resolved, Backlog and Same Week Resolution b...



Network resources needing capacity upgrade



Conclusion

As employees return to work, IT departments need to arm themselves to ensure the transition is smooth and secure. This e-book outlines provides detailed steps for IT departments gearing up to take on this challenge.

Want to learn how analytics can help you with your back to work strategy?

[Sign up for a 1-on-1 session with our experts.](#)

About

ManageEngine Analytics Plus

ManageEngine Analytics Plus is a self-service business intelligence and IT analytics solution that integrates with several popular help desk applications such as ServiceNow, Zendesk, and ManageEngine ServiceDesk Plus. It also integrates with other IT applications used for network and application management, project management, endpoint security management, and more. Powered by artificial intelligence, 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 also features capabilities such as importing data from multiple sources, data blending, trend forecasting, real-time sharing and collaboration, and advanced computing and analysis.

[Download a 30-day trial of Analytics Plus](#)

180K
customers
across the world

18+
years of IT
management experience

90+
products
and free tools

190+
countries
served

ManageEngine Analytics Plus

© ManageEngine, a division of Zoho Corporation