2021 IT OPERATIONS SURVEY REPORT

Kaseya®

INTRODUCTION

Kaseya has been surveying IT professionals from small and midsize companies for over five years. Our survey covers the top priorities and challenges for IT teams, areas of technology investment, key metrics and more.

The resulting report provides insights into current trends and allows IT teams to see how they compare with their peers. Like all our previous years' reports, the Kaseya 2021 IT Operations Report also offers an in-depth analysis of the key security concerns, compliance challenges and backup strategies of IT professionals globally.

Read on to learn more about the key priorities, challenges and technology adoption of your peers in small and midsize businesses (SMBs).

KEY FINDINGS

Here are some of the key findings of the Kaseya 2021 IT Operations Report:

1. Improving IT Security – A Top IT Priority for Businesses

"Improving IT security" emerged as the top IT priority for 61% of respondents this year, with "Cloud migration" (e.g., IaaS, PaaS or SaaS) following close behind as a high priority for 36% of respondents. The third key priority for the respondents this year is "Increasing IT productivity through automation."

The top three IT priorities this year are in line with recent trends including, the sharp increase in cyberattacks over the past year, business transformation during the pandemic (shift to online and cloud), and the increased demands on IT that are outpacing growth in team size (i.e. need to do more with existing resources).

2. Cybersecurity and Data Protection – A Major Challenge for Businesses in 2021

When asked about the top IT challenges their IT departments are faced with, more than half of respondents cited "Cybersecurity and data protection" as their topmost concern. The second challenge that 30% of all respondents were concerned about was the problem of "Not enough IT budget or resources to meet demands," closely followed by "Legacy systems hampering growth and innovation" which was chosen as a major challenge by 24% of respondents.

3. IT Budget Growth – Getting Back on Track

More than a third (38%) of respondents said that their IT budget has increased in 2021. This is consistent with other surveys that are reporting an increase in IT spending this year. Many businesses are back in a growth mode post-pandemic. For 35% of the respondents, their IT budget stayed the same this year as compared to 2020.

4. Top Drivers for IT Budgets in 2021 – Where Businesses are Investing

"Updating outdated IT infrastructure" and "Business growth" are the top two drivers for IT budgets in 2021 according to 52% and 49% of respondents respectively. As noted above, among the top three challenges that businesses are faced with in 2021, legacy systems hampering growth and innovation was a top concern for 24% of respondents. So, more than half of the respondents are planning to invest in updating their outdated, legacy infrastructure to boost sustainable growth and innovation going forward.

5. Top Technologies to Invest in for 2021

When asked what technologies their businesses will invest in this year, more than half (53%) of all respondents will be investing in "Email security (including phishing prevention)" to bolster their cybersecurity stance. "IT automation" and "Ransomware protection" are the two other technologies that businesses plan to focus on in 2021. These top technology trends have emerged from the need for greater cybersecurity and higher IT operational efficiency to meet the increasing demands on IT.

Our Respondents

In this year’s edition of the IT Operations Survey, we received responses from a total of 943 participants.

Geographical Locations

The bulk of respondents for the 2021 IT Operations Benchmark survey were from the Americas (84%), with 11% from Europe, the Middle East and Africa (EMEA), and 5% from Asia Pacific (APAC).

Americas	84%
EMEA	11%
APAC	5%

Industries

Our respondents hailed from a wide range of industries. The spot for the most popular industry was shared by “Education” and “IT managed services provider” at 12% each, closely followed by “Manufacturing” at 11%.

⏩ IT managed service provider	12%
⏩ Education	12%
⏩ Manufacturing	11%
⏩ Healthcare	10%
⏩ Technology (e.g., software, hardware)	10%
⏩ Financial services	9%
⏩ Government/public sector	7%
⏩ Professional services	7%
⏩ Retail	5%

Company Size, Revenue and Number of Endpoints

The company size of the respondents varied from "Less than 50" employees to "More than 3,000." Nearly a third of our respondents came from companies with less than 100 employees while 40% of respondents came from organizations with 100 to 1,000 employees, and over a quarter of respondents worked at companies with over 1,000 employees.

Total number of employees in the company	Americas	APAC	EMEA	All respondents
Less than 50	19%	13%	27%	**19%**
51 to 100	11%	17%	16%	**12%**
101 to 500	26%	32%	15%	**25%**
501 to 1,000	16%	19%	11%	**15%**
1,001 to 3,000	14%	9%	9%	**13%**
More than 3,000	15%	11%	23%	**15%**

We also surveyed the respondents for the annual revenue of their organizations. Of the respondents, 43% came from organizations with annual revenue of up to $10 million. More than a quarter of the respondents came from companies with annual revenue between $50 million and $500 million while 7% of the respondents came from companies with over $1 billion annual revenue.

Company's annual revenue	Percentage of respondents
Less than $1 million	17%
$1 million to $10 million	26%
$10 million to $50 million	18%
$50 million to $100 million	12%
$100 million to $500 million	15%
$500 million to $1 billion	6%
Over $1 billion	7%

The number of endpoints managed by the companies that our respondents worked for ranged from "Less than 50" to "More than 5,000." Forty percent of the respondents work for companies that manage 50 to 500 endpoints. About a third of the respondents (33%) came from companies that manage 500 to 3,000 endpoints while 13% of the companies manage more than 5,000 endpoints.

Endpoints managed	Percentage of respondents
More than 5,000	13%
3,001 to 5,000	5%
1,001 to 3,000	16%
501 to 1,000	17%
101 to 500	29%
51 to 100	11%
Less than 50	9%

Job Titles

More than a quarter of the respondents (28%) held the job title of "System Administrator or IT Technician" at their respective companies while 24% of the respondents were "IT Managers/Supervisors" at their companies. Of the respondents, 10% held the title "Head of Technology or C-level IT Executive" and 15% were "Director of IT" at their respective companies.

Titles of Respondents	Americas	APAC	EMEA	Grand Total
Vice president	4%	0%	2%	**4%**
Head of technology or C-level IT executive	10%	4%	9%	**10%**
Director of IT	17%	2%	13%	**15%**
IT manager/supervisor	22%	43%	29%	**24%**
Project manager	5%	2%	5%	**5%**
Network engineer	6%	6%	5%	**6%**
System administrator or IT technician	28%	36%	26%	**28%**
Other	9%	6%	11%	**9%**

The State of IT Operations – Detailed Findings

Let's take a look at the key survey findings in detail.

Top IT Priorities in 2021

The top three priorities for our respondents in 2021 are "Improving IT security overall," "Cloud migration" (e.g., IaaS, PaaS and/or SaaS) and **"Increasing IT productivity through automation."**

Improving IT security has been the topmost priority for IT teams for the past few years. With the huge uptick in cyberattacks during the pandemic, enhancing IT security has become even more urgent. Cybercriminals are taking advantage of weaker security associated with work from home employees.

The second-highest priority, "Cloud migration," is aligned with digital transformation initiatives and brings multiple benefits to an organization. Cloud services allow IT teams to easily scale service delivery to meet organizational needs. Leveraging cloud infrastructure services helps reduce hardware and IT management costs associated with traditional on-premises equipment.

Essentially tied with cloud migration, another top priority was **Increasing IT productivity through automation**. The growth in the number and diversity of endpoints and devices that IT teams must manage is also increasing the demand on IT. This includes management of virtual machines, mobile devices, cloud infrastructure and commercial IoT. Automation is the key to increasing IT operational efficiency.

Following close behind were more strategic priorities such as reducing IT costs and supporting their company's business innovation initiatives. Business innovation is another key priority for companies that aim to sustain and grow in 2021 amid a fast-evolving market.

Top 3 IT priorities	Americas	APAC	EMEA	All respondents
Improving IT security overall	62%	50%	60%	**61%**
Cloud migration (e.g., IaaS, PaaS, or SaaS)	35%	43%	35%	**36%**
Increasing IT productivity through automation	35%	32%	32%	**34%**

Top priorities	Americas	APAC	EMEA	All respondents
Improving IT security overall	62%	50%	60%	**61%**
Cloud migration (e.g., IaaS, PaaS, or SaaS)	35%	43%	35%	**36%**
Increasing IT productivity through automation	35%	32%	32%	**34%**
Delivering higher service levels/IT service availability	33%	27%	38%	**33%**
Reducing IT costs	30%	27%	39%	**31%**
Supporting your company's business innovation initiatives	25%	23%	21%	**24%**
Compliance reporting	20%	16%	19%	**20%**
Supporting mobile devices and BYOD	15%	18%	9%	**14%**
Reducing unplanned downtime and disruptions	13%	11%	12%	**13%**
Improving help desk KPIs (such as MTTR, first contact resolution and ticket volume)	12%	9%	15%	**12%**
Implementing big data or data science and analytics	11%	14%	11%	**11%**
Outsourcing some core IT functions	5%	7%	4%	**5%**
Other	2%	2%	1%	**2%**

Key Challenges IT Departments Are Faced With in 2021

With the world gradually recuperating from the disastrous effects of the global pandemic, the worst seems to be behind us. Even as the dust settles, businesses are faced with a host of IT challenges that they must overcome to thrive in the recovering economy.

For IT departments, the focus has now shifted to adapting to the new normal and dealing with its challenges. More than half of the respondents (54%) cited "Cybersecurity and data protection" as their biggest current challenge.

Nearly one-third of respondents were also found struggling to meet current demands due to IT budget and resource constraints. This is a perennial problem for most IT departments. The pandemic has accelerated the need for digital transformation, which IT teams have had to accommodate, at times with fewer staff and smaller budgets.

Legacy systems hampering growth and innovation is the third key challenge that nearly one-quarter of the respondents (24%) are faced with in 2021. Modernizing legacy systems is another perennial IT problem.

Top 3 IT challenges	Americas	APAC	EMEA	All respondents
Cybersecurity and data protection	54%	55%	54%	**54%**
Not enough IT budget or resources to meet demands	30%	32%	34%	**30%**
Legacy systems hampering growth and innovation	24%	20%	20%	**24%**

IT Operational Maturity

IT Operational Maturity is defined by a collective set of IT management capabilities and is indicative of how effectively IT provides services and support to the business. Our 2021 IT Operations Survey results found more than a quarter of IT teams (27%) to be at the lowest level of maturity (Reactive) and nearly half of the respondents (47%) to be at the two lowest levels (Reactive and Efficient).

The highest percentage (33%) of respondents belong to the "Proactive" category where they are focused at streamlining IT operations by automating repetitive tasks and remedial actions.

In the last couple of years, small and midsize businesses have made slow progress toward achieving higher levels of operational maturity. Only 6% of the respondents indicated they are at the second highest level of operational maturity (Aligned), where they are tracking and managing against service-level agreements (SLAs).

And only 14% of the respondents said that they have a strategy in place to add value to their business, thus pinning them at "Strategic," the highest level of "IT Operational Maturity."

IT operational maturity	Percentage
Strategic: Achieving IT operational excellence and taking a strategic role in driving business innovation	14%
Aligned: Tracking and managing against service-level agreements (SLAs) or availability/performance expectations	6%
Proactive: Proactive in our approach to IT management, automating repetitive tasks and many remedial actions	33%
Efficient: Systematic in our approach to solving known issues and dealing with daily tasks	20%
Reactive: Responsive to individual challenges and requests	27%

IT management capabilities	2021	2020	2019
Strategic/ Aligned	20%	22%	15%
Proactive	33%	33%	28%
Efficient	20%	21%	21%
Reactive	27%	24%	35%

IT Budget Trends and Allocations

We asked our respondents whether their company's IT budget has increased, decreased or stayed the same as compared to 2020. More than a third of the respondents (38%) said that their IT budget has increased in 2021. For 35% of the respondents, their IT budget stayed flat and another 13% said their companies cut down on their IT budgets in 2021.

2021 budget changes	Percentage of Respondents
Increased	38%
Decreased	13%
Stayed the same	35%
I don't know	14%

Top Budget Drivers in 2021

More than half of the respondents (52%) revealed that their company's top budget driver in 2021 was "Updating outdated IT infrastructure." Another major budget driver for 49% of the respondents was "Business growth."

"Remote workforce management" was an important budget driver for 42% of the respondents while both "Innovation and strategic initiatives" and "Security incidents or concerns" were each found to be major budget drivers for 38% of respondents. Over a third of the respondents (37%) plan to invest their IT budget in "Digital transformation" this year.

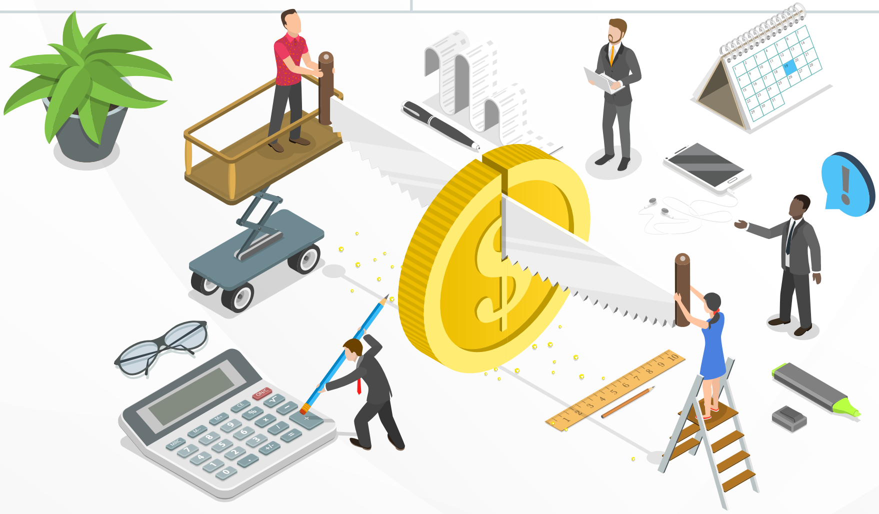
Top budget drivers in 2021	Percentage of respondents
Updating outdated IT infrastructure	52%
Business Growth	49%
Remote workforce management	42%
Innovation and strategic initiative(s)	38%
Security incidents or concerns	38%
Digital transformation	37%
Regulatory compliance	25%
Competitive pressure	11%
Other	4%

Size of the IT Budget

We asked our respondents to report the size of their IT budget in 2021.

About 20% of the respondents revealed that their 2021 IT budget was less than $100,000. More than a quarter of the respondents (29%) said their IT budgets were in the range of $100,000 to $500,000. Almost a quarter of the respondents (22%) came from companies with IT budgets ranging from $1 million to over $25 million.

Size of IT budget	Percentage of respondents
Over $25 million	4%
$10 million to $25 million	2%
$5 million to $10 million	5%
$1 million to $5 million	11%
$500,001 to $1 million	7%
$250,001 to $500,000	12%
$100,001 to $250,000	17%
Less than $100,000	20%



Top Technologies for Investment

The top technologies companies will be investing in 2022 are:

Email Security: More than half (53%) of the respondents said that they will invest in "Email security (including phishing prevention)." With the increase in cyberattacks in the past year, email phishing attacks have been on the rise. Investing in email security solutions and employee training are good ways to combat the problem of phishing attacks that can lead to security breaches.

IT Automation: Nearly half (49%) of respondents said that their IT budget will be utilized for "IT automation" technologies. IT automation is an important strategy for businesses that must improve operational efficiency and do more with existing IT resources. The number and diversity of new endpoints and devices to be managed is growing rapidly. This includes virtual machines, cloud infrastructure, IoT and mobile devices. In order to remotely manage your highly-distributed IT environment and increase IT operational efficiency, you need an endpoint management tool that allows you to "manage everything" and can automate all common IT processes.

Ransomware protection: A third of the respondents (33%) cited ransomware protection as a key technology their company will invest in this year. One approach to enhancing IT security it by l everaging managed security operations center (SOC) services.

Technologies SMBs will invest in 2022	All respodents
Email security (including phishing prevention)	53%
IT automation	49%
Ransomware protection	33%
AI and machine learning	23%
Containerization technology	21%
Customer experience technologies, including chatbots and mobile apps	20%
Data science and analytics	20%
5G technology	17%
Insider threat detection	17%
Serverless solutions	15%
Dark web monitoring	15%
Hyperconverged infrastructure (HCI)	12%
Edge computing	11%
Blockchain	9%
Low code tools	8%
Virtual reality or augmented reality	7%
Robotic process automation (RPA)	7%
Other	5%

Areas of IT Spending

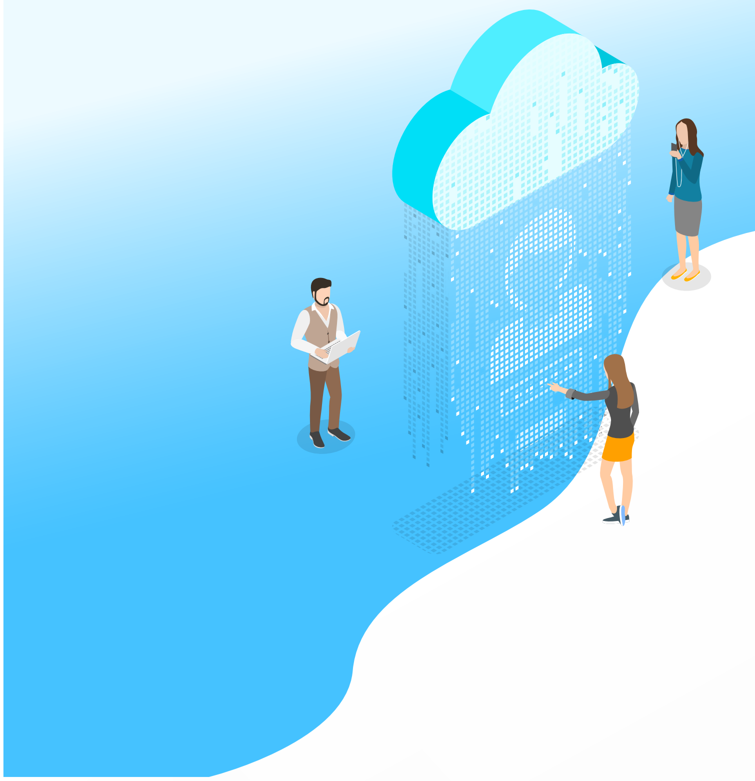
We asked our respondents about key areas of their company's IT budget to see which will increase, decrease, or stay flat in 2021.

Fifty-seven percent (57%) of respondents are planning to increase spending on IT security—no surprise there!

More than half of the respondents (54%) said that their IT budget allocation for "Cloud – IaaS (public, private, hybrid)" will increase in 2021. The migration to cloud services has also accelerated over the past year. Regardless of whether they invest in the public cloud, private cloud or a hybrid of the two, businesses benefit substantially in terms of scalability, reduced CAPEX costs, ease of access to systems and applications, and better service delivery.

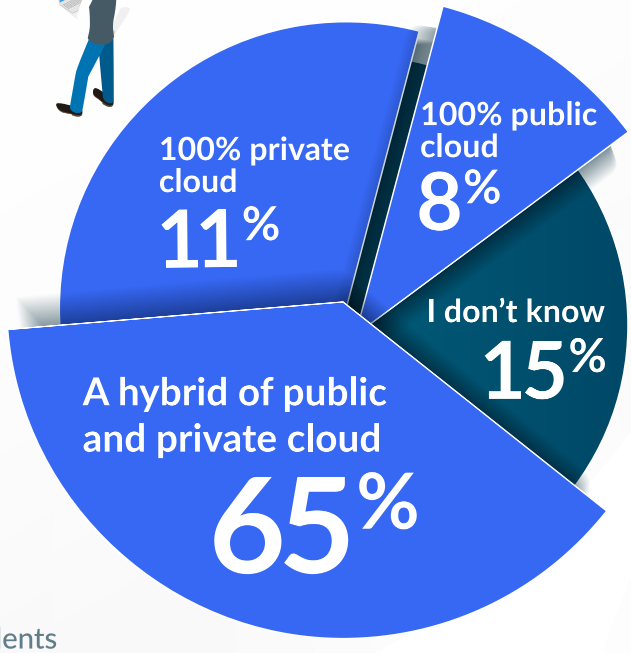
More than 40% of respondents expect to increase spending on both end-user hardware and IT management tools.

Status of IT budget in 2021	Increase	Decrease	Stay the same
Cloud – IaaS (public, private, hybrid)	**54%**	**3%**	**43%**
Containerization Technologies	24%	6%	71%
End-user hardware (e.g., desktops, laptops, tablets, or mobile devices)	42%	12%	45%
Installed software	29%	14%	57%
IT management tools	**42%**	**6%**	**52%**
IT staff	33%	9%	58%
IT security	**57%**	**4%**	**40%**
Managed service provider services	30%	10%	60%
SaaS applications	36%	5%	59%
Server technology (e.g., servers, storage, server backup, UPS, or hyper-converged infrastructure)	33%	18%	50%
Virtualization Technologies	37%	7%	56%
I don't know	10%	8%	82%



Cloud Strategy

In terms of cloud adoption, nearly two-thirds of the respondents (65%) revealed that their company utilizes a hybrid of public and private cloud services.



When asked about the SaaS applications that our respondents use, more than three-quarters (77%) cited Microsoft 365 as their go-to SaaS application suite. Just over a quarter of the respondents (28%) used Google Workspace (formerly G Suite) and another 26% used Salesforce.

SaaS applications	Percentage
Microsoft 365	77%
Google Workspace (formerly G Suite)	28%
Salesforce	26%
Dropbox	24%
Microsoft Dynamics	15%
ServiceNow	14%
Box	11%
Workday	10%
Netsuite	7%
Other	8%

Areas of Staffing Growth

In terms of IT staffing growth areas, nearly half of the respondents (46%) said that they anticipate staffing growth in the area of "IT security" in 2021. Another 40% of the respondents said that their company planned staffing growth in the area of "General IT technical staff" and 34% cited "Help desk."

IT staffing growth areas	Americas	APAC	EMEA	All respondents
IT security	44%	64%	53%	**46%**
General IT technical staff	41%	44%	35%	**40%**
Help desk	36%	40%	21%	**34%**
Network engineering or network management	22%	52%	19%	**23%**
System administration	23%	36%	18%	**23%**
DevOps	21%	28%	27%	**22%**
Application development	20%	28%	21%	**21%**
IT service delivery	15%	32%	18%	**16%**
Administrative	15%	28%	13%	**16%**
Team management	9%	16%	5%	**9%**
Sales and marketing	7%	24%	11%	**8%**

IT Security, Backup and Compliance

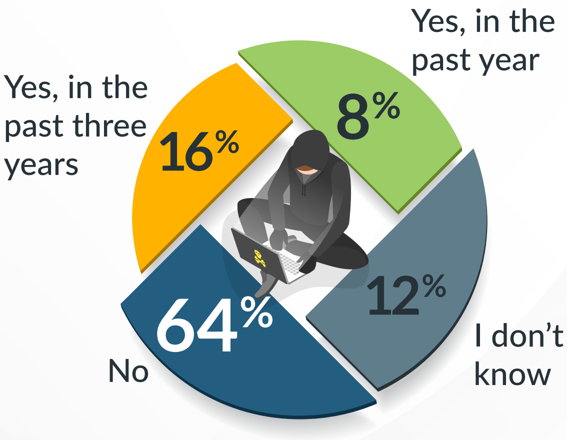
A shift to remote work paved the way for increased cyberattacks and security breaches over the last year. Ransomware attacks have been one of the top causes for businesses losing critical data and suffering the costly consequences of a security breach.

Security Breaches

Most of our respondents (64%) stated that they haven't experienced a security breach or ransomware attack in the last three years.

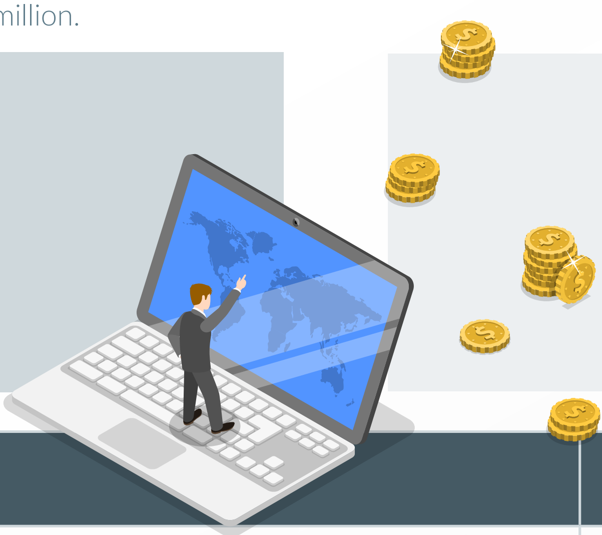
While 16% of the respondents experienced a security breach in the past three years, about 8% experienced one in the last year alone. We anticipate, however, that due to evolving cybersecurity threats, SMBs are likely to experience a much higher rate of security incidents over the next three years.

SECURITY BREACH INCIDENT



Cost of a Security Breach

According to a **study by IBM**, the average annual cost of a data breach is $3.86 million. Among respondents who experienced a security breach in the past three years, the cost to the business was less than $100,000 per annum for 47% of them. Another 21% said that the cost of the security breach ranged from $100,000 to $500,000. About 8% of the respondents reported the cost of security breach to be from $500,000 to a whopping $5 million.



Cost of the security breach	Percentage
$0 to $100,000	47%
$100,001 to $250,000	12%
$250,001 to $500,000	9%
$500,001 to $1 million	6%
$1 million to $5 million	2%
I don't know	23%

Patch and Vulnerability Management

Timely patching of IT systems reduces security risks and keeps hackers at bay. IT teams should strive to apply patches within 30 days of their release and test patches before applying them.

- When asked about the patch and vulnerability management policies at their organizations, more than two-thirds of the respondents (69%) said that they scan all servers and workstations for operating system patches regularly.
- More than half of the respondents (56%) also apply critical OS patches within 30 days of release.
- **Only around 44% have automated patch management.** This is an area where many organizations can improve both their security posture and their IT productivity through automation.
- **Only about 38% apply critical patches for third-party apps within 30 days of release** — not doing this exposes companies to higher security risk. Automated patch management can help IT teams meet this objective.
- **Less than one-third of respondents (30%) can patch remote, off-network devices**, which means that many companies are putting their business at risk due to the current prevalence of work-from-home employees and hybrid work models.

Cost of the security breach	Percentage
We scan all servers and workstations for operating system patches regularly	69%
We apply critical OS patches within 30 days of release	56%
We have automated patch management	44%
We scan all servers and workstations for third-party software patches regularly	43%
We monitor third-party software announcements and apply patches for critical issues within 30 days of release	38%
We can patch remote, off-network devices	30%
We don't have a patch and vulnerability management policy in place	8%
I don't know	9%

Backup Policies and Business Continuity

A backup policy highlights the need for data and system backups and lays the ground rules for its execution. It is a vital component of an all-encompassing business continuity plan – ultimately ensuring that all business operations run smoothly in the event of a security incident or disaster.
When asked what best describes their backup policy:

- A remarkable 82% of the respondents said that they back up their servers – physical and virtual.
- Only about a third of the respondents (36%) back up their SaaS application data. This is indicative of the fact that most businesses are still under the impression that their SaaS service providers are responsible for their SaaS data. In most cases, businesses have this responsibility, not the SaaS vendor.
- Nearly 24% of the respondents back up laptops running on the corporate network and 22% back up public cloud and VMs.

Backup Policy	Percentage of respondents
We back up servers (physical and virtual)	**82%**
We back up SaaS application data	**36%**
We back up physical desktops	**25%**
We back up laptops running on the corporate network	**24%**
We back up public cloud VMs	**22%**
We back up laptops running in home offices or elsewhere	**18%**
We don't back up	**1%**
I don't know	**6%**
Administrative	**15%**
Team management	**9%**
Sales and marketing	**7%**

Is SaaS Backup Important? Who Is Responsible for It?

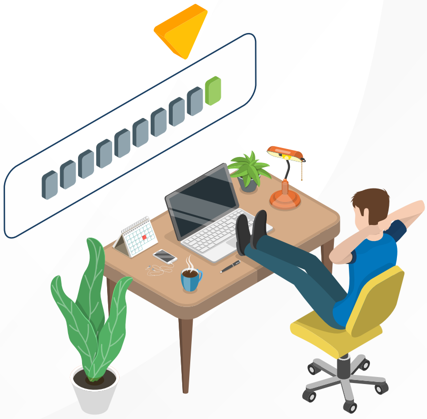
SaaS data backup is as important as backing up your on-premises data. More than three-quarters of the respondents (82%) understand the importance of this and believe that SaaS applications like Microsoft 365, Google Workspace and Salesforce need to be backed up. There are still a number of businesses (10%) that believe they do not need to back up their SaaS application data.

Importance of SaaS data backup	All respondents
Yes	82%
No	10%
I don't know	9%

However, about 60% of the respondents operate under the common misconception that SaaS providers are responsible for the protection of their data. While this may be true to a certain extent, there are significant limitations on SaaS data protection provided by the vendor. SaaS vendors typically follow a shared responsibility model when it comes to data protection. They will protect their customers from network, storage, server and application failures. However, the customer is ultimately responsible for protecting their own data from user and admin failures as well as cybersecurity attacks.

Hence, when it comes to keeping your SaaS data completely secure, relying solely on your providers is a mistake. Despite this, as noted above, only about 36% of respondents back up their SaaS data. Using a third-party SaaS data backup tool or service should be an important consideration for your business.

Responsibility of SaaS data protection	All respondents
Yes	60%
No	32%
I don't know	8%



More than three-quarters of the respondents (80%) surveyed said that they leverage a third-party backup tool to back up their Microsoft 365 data while less than one-quarter (24%) back up their Google G Suite data.

Third party backup tool/service for backing up SaaS data	Americas	APAC	EMEA	All respondents
Microsoft 365	80%	84%	78%	**80%**
Google Workspace (formerly G Suite)	24%	16%	19%	**23%**
Salesforce	15%	16%	3%	**14%**

Business Continuity Plan

A robust business continuity and disaster recovery (BCDR) plan is crucial for not only ensuring quick and efficient recovery after a security breach, but also for maintaining compliance with regulatory standards of your industry.

About two-thirds (67%) of the respondents have a formal BCDR plan in place that is approved by management. However, nearly a quarter (21%) of businesses still do not have a formal BCDR plan in place and are exposed to the risks associated with prolonged downtime and non-compliance with industry regulations.

Formal BCDR plan	Percentage
Yes	67%
No	21%
I don't know	12%

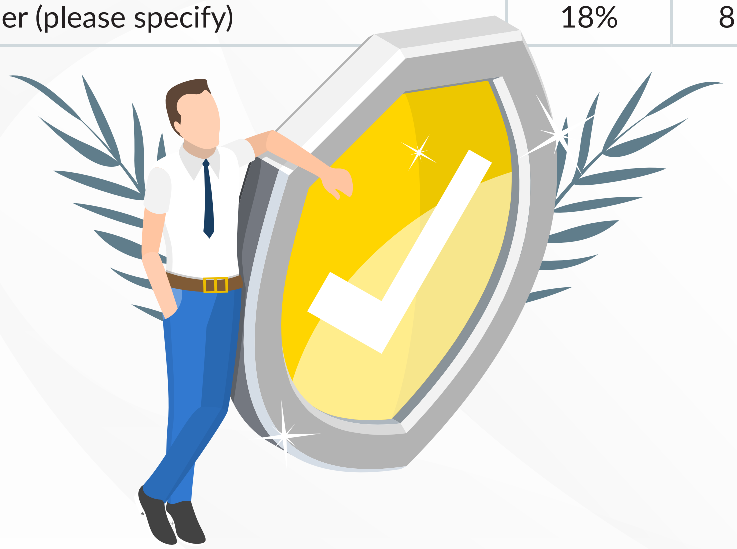
Compliance Standards

With nearly 10% of respondents working for companies in the healthcare industry, it isn't surprising that more than a third of respondents (38%) said they try to adhere to Health Insurance Portability and Accountability Act (HIPAA) regulations in their organizations.

About one-third of respondents (33%) adhere to Payment Card Industry (PCI) regulation standards and more than one-quarter (26%) comply with the General Data Protection Regulations (GDPR).

Compliance requirements continue to grow, with new regulations such as the California Consumer Privacy Act (CCPA) and the New York Stop Hacks and Improve Electronic Data (SHIELD) Act, coming into play. This makes it harder for organizations to keep up. Organizations would benefit from using a compliance management solution that automates much of the process.

Compliance requirements	Americas	APAC	EMEA	All respondents
HIPAA	45%	12%	5%	**38%**
PCI	37%	12%	19%	**33%**
GDPR	23%	16%	53%	**26%**
ISO 27001	20%	48%	37%	**24%**
CCPA	14%	32%	13%	**15%**
FERPA	18%	0%	0%	**15%**
NY SHIELD	4%	4%	0%	**3%**
Other (please specify)	18%	8%	18%	**18%**



IT Metrics and KPIs

Measuring and monitoring key IT metrics and KPIs is important to maintain optimal performance of your systems and resources.

Top KPIs

IT system downtime is bound to have a negative impact on any business. High system availability helps ensure that a business operates efficiently. Hence, it is incredibly important to keep IT systems up and running and resolve incidents as soon as possible to minimize downtime cost and risk.

As such, **system availability** was found to be the top IT operational KPI that more than half of the respondents (51%) measure on a regular basis.

When it comes to service and support metrics:

- About 41% of respondents measure service ticket volume per period.
- More than a third of respondents (39%) measure help desk agent utilization.
- More than a third of respondents (39%) measure first response time.

IT operations metrics measured	Percentage of respondents
System availability	51%
Service ticket volume per period	41%
Help desk agent utilization	39%
First response time (from user inquiry to first response by a help desk agent)	39%
Mean time to resolution (MTTR) of service tickets	28%
First contact resolution (FCR) of service tickets	26%
Recovery time objective (RTO)	21%
Recovery point objective (RPO)	19%
Average cost per ticket	17%
Mean time between failures (MTBF) of IT systems	16%
Other (please specify)	8%

Critical System Availability Targets

Among all the respondents, 42% target 99.9% (three nines) or below system availability, which means they could face downtime of nine hours or more per year. This amount of downtime could prove costly to the business since the cost of downtime can be upwards of $100,000 to $300,000 per hour. So, these organizations are encouraged to increase their system availability targets.

Another 41% target 99.99% (four nines) and above availability, which translates to downtime of 52 minutes or less per year. This is a much better scenario.

Target system availability percentage for business critical systems	Percentage of respondents
I don't know	17%
Below 99 percent	4%
99 percent (2 nines)	18%
99.9 percent (3 nines)	20%
99.99 percent (4 nines)	23%
99.999 percent (5 nines) and above	18%

Support Tickets Per User

Nearly two-thirds of the respondents (63%) reported that the average number of support tickets generated per user, per month in their organization lies between 0 to 10. Around a quarter of the respondents (22%) have an average of over 10 tickets generated per user, every month.

Average number of support tickets per user per month	Percentage of respondents
0 to 4	39%
5 to 7	17%
8 to 10	7%
Over 10	22%
I don't know	15%

IT Management

Streamlining IT management is a major focus of most internal IT teams. The right IT management technology stack can have a big impact on IT operational efficiency. When asked about the IT management tools their companies use:

- Three-quarters of the respondents (75%) cited help desk/ticketing solutions.
- Nearly two-thirds of the respondents (63%) said that their organizations used an endpoint management solution.
- More than half of the respondents (55%) also use an IT documentation/knowledge management tool.

IT management tools used	Americas	APAC	EMEA	Grand total
Help Desk/Ticketing	77%	68%	65%	**75%**
Endpoint Management	64%	56%	63%	**63%**
IT Documentation / Knowledge Management	56%	44%	53%	**55%**
Network Management / Network Performance Monitoring	55%	56%	45%	**54%**
Mobile Device Management (MDM)	44%	40%	39%	**43%**
IT Service Management (something more advanced than a helpdesk tool)	36%	48%	40%	**37%**
Endpoint Detection and Response (EDR)	37%	36%	29%	**36%**
Security Information Event Management (SIEM)	35%	36%	27%	**34%**
Identity and Access Management (IAM)	36%	24%	27%	**34%**
Configuration Management Database (CMDB)	21%	16%	31%	**22%**
Cloud Cost Management	17%	20%	15%	**17%**
Other	2%	0%	3%	**2%**

Key Endpoint Management Use Cases and Integrations

An endpoint management solution is central to running any business today. It manages all devices on and off the network, enhances IT productivity and helps protect the business from cybersecurity attacks with automated software patching.

When asked to rate the importance of certain use cases for their endpoint management solution, the respondents selected **"Remote access and management of endpoints," "Software patch management,"** and **"Automation of IT processes,"** as their top requirements.

The use cases for "Backup management" and "AV/AM deployment and management" exhibited a strong correlation with the number one IT priority of small and midsize businesses this year — improving IT security.

Given the increasing number and diversity of endpoints and devices to be managed, "Discovery and inventory of hardware and software assets" and "Mobile device management" are two other important use cases for endpoint management that have emerged in 2021.

For today's complex IT environments, a traditional endpoint management solution is no longer enough. Businesses today need a unified endpoint management solution that enables them to monitor and manage not only their traditional endpoints but also the next generation devices such as VMs, cloud infrastructure and IoT devices.

Rating the importance of these use cases for your endpoint management solution from 1 to 5	1 (Most important)	2	3	4	5 (Least important)
Remote access and management of endpoints	31%	24%	18%	11%	17%
Automation of IT processes	30%	20%	24%	14%	12%
Software patch management	30%	24%	20%	13%	14%
Network monitoring	26%	26%	21%	17%	10%
Backup management	25%	24%	23%	17%	11%
Regulatory compliance management	24%	20%	26%	18%	12%
AV/AM deployment and management	22%	22%	30%	16%	10%
Mobile device management	18%	21%	31%	17%	12%
Discovery and inventory of hardware and software assets	17%	26%	31%	16%	10%
Network topology mapping	16%	20%	35%	21%	9%

IT teams typically use an endpoint management solution to run IT operations, a service desk solution to manage service requests and tickets, and an IT documentation solution to maintain accurate asset information and up-to-date IT procedures.

Native integration of these three solutions enables IT teams to have seamless workflows that save time and boost technician productivity. When asked about the importance of these workflow integrations, more than a quarter of the respondents (28%) rated “The ability to run automation scripts (agent procedures) in the IT documentation tool to resolve IT incidents” as most important.

Nearly 26% of the respondents cited “Access to IT documentation such as IT asset and organizational information, IT procedures, passwords and more, in the service desk” as most important. Another 26% of the respondents cited “One-click access to remote endpoint management from service tickets to troubleshoot issues” as very important for their organization.

Importance of integrations between endpoint management, service desk and IT documentation solutions	1 (Most important)	2	3	4	5 (Least important)
The ability to run automation scripts (agent procedures) in the IT documentation tool to resolve IT incidents	28%	19%	27%	14%	11%
One-click access to remote endpoint management from service tickets to troubleshoot issues	26%	22%	24%	18%	10%
Access to IT documentation such as IT asset and organizational information, IT procedures, passwords and more, in the service desk	26%	26%	26%	15%	8%
Access to IT documentation, such as IT asset and organizational information, IT procedures, passwords and more, in the endpoint management tool	24%	25%	27%	15%	8%
The ability to set up workflows in the service desk to auto-remediate IT incidents by running scripts (agent procedures)	23%	25%	27%	16%	10%
The ability of the endpoint management solution to automatically create service tickets based on monitored events/states	20%	25%	29%	15%	12%

Functions Offloaded to MSPs

We asked the respondents about the functions that they outsource to managed services providers (MSPs). Almost 60% of organizations in this survey outsource some function(s) to MSPs.

- 21% of the respondents said that their companies outsourced backup management to an MSP.
- 19% outsourced cloud infrastructure management to MSPs.
- 17% of all respondents said that they outsourced IT security and the same percentage said that they had outsourced network monitoring to an MSP.

Functions outsourced to MSP	Americas	APAC	EMEA	All respondents
Backup management	20%	33%	21%	21%
Cloud infrastructure management	18%	19%	24%	19%
IT security	15%	33%	17%	17%
Network monitoring	16%	33%	11%	17%
Help desk	11%	26%	14%	12%
Security operations centre	13%	19%	5%	12%
Patching and software management	10%	11%	14%	10%
Endpoint management (e.g., desktops, laptops, and servers)	9%	22%	11%	10%
Compliance reporting	9%	11%	10%	9%
Onboarding or offboarding of users and devices	5%	4%	8%	5%
Other	8%	0%	6%	8%
We do not outsource any services to an MSP	41%	33%	44%	41%

IT Purchasing

We asked the respondents how many people in their company were involved in decisions pertaining to IT purchases. Nearly 41% of the respondents said that their companies have four or more employees involved in IT purchases.

Number of people involved in IT purchase decisions	Respondents
1	34
2	100
3	138
4	44
5	66
More than 5	77

Primary Financial Decision Maker

Nearly one-third of the respondents (32%) said that the primary financial decision maker for IT-related purchases in their companies is a C-level executive. Another 30% revealed that director-level executives were the primary financial decision makers for IT-related purchases.

Primary financial decision maker for IT-related purchases	Americas	APAC	EMEA	All respondents
C-level	34%	20%	21%	32%
Director-level	29%	24%	42%	30%
VP-level	24%	8%	13%	22%
Manager-level	12%	48%	24%	16%

Roles Involved

More than half of the respondents (56%) said that the director of IT was the topmost role involved in IT purchasing decisions in their company. An additional 47% of the companies involved C-level executives in their IT purchasing decisions. The IT Manager or Supervisor role was instrumental in making IT purchase decisions in 41% of the companies.

Roles involved in IT purchasing decisions	Americas	APAC	EMEA	All respondents
Director of IT	58%	32%	53%	56%
C-level Executive	50%	28%	34%	47%
IT Manager or Supervisor	40%	52%	44%	41%
Finance Vice President or Director	33%	36%	32%	33%
System Administrator or IT Technician	31%	20%	31%	30%
IT Vice President	27%	16%	11%	24%
Procurement Manager	15%	28%	26%	17%
CISO (or other security executive)	10%	4%	10%	10%
Other (please specify)	4%	0%	8%	5%

CONCLUSION

Improving IT security is the top priority for a majority of the companies surveyed. Protecting data and keeping IT environments secure has always been challenging for IT departments. As IT departments struggle with resource constraints and growing demands, organizations are embracing IT automation to increase productivity and reduce costs.

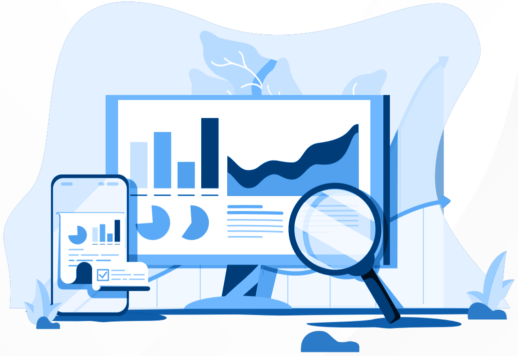
For all of these reasons, an endpoint management solution that lets IT teams "manage everything" (traditional endpoints and next generation devices), automate common IT processes, patch OSes and third-party apps, and manage backups and AV/AM deployment from a single console, is a must-have.

Kaseya VSA, a truly unified endpoint management (UEM) solution for small and midsize businesses, is a powerful platform that enables IT teams to remotely manage traditional endpoints (laptops, servers, desktops) and network devices, with support for VMware and Microsoft Hyper-V VMs and cloud infrastructure coming soon.

Kaseya VSA proactively resolves issues and automates common IT processes, including software deployment, patch management, antivirus and anti-malware deployment, and routine maintenance. It provides seamless integration with other solutions in our IT Complete portfolio that allow technicians to work efficiently across tools and access the right information when and where they need it.

"MANAGE EVERYTHING" FROM A SINGLE CONSOLE WITH KASEYA VSA.

REQUEST A DEMO NOW!



METHODOLOGY

Kaseya conducted its 2021 IT Operations Survey using a structured questionnaire in May 2021. All participants were asked if they were primarily employed in IT operational role with some responsibility for IT infrastructure or IT services deployment, operational, management or support.

Only responses from those who answered in the affirmative were included in the survey results. Among those, 57% of the final respondents identified their primary responsibility as “all of IT.” In total responses were received from 943 IT professionals. The focus of the survey was IT operations (individual and groups) at midsize organizations, which we define as organizations with up to 3,000 employees. Only companies in this range are included in the survey results.

06242021