THE 2018 STATE OF
IT OPERATIONS FOR MIDSIZE ENTERPRISES
IT Operations Benchmark Survey Results Report

Kaseya®

Introduction

For the fourth consecutive year, Kaseya surveyed midmarket internal IT professionals throughout the world about their organization's IT operations and practices.

The Kaseya IT Operations Benchmark Survey was designed to find out how IT groups at midsize businesses — which we define as organizations with up to 5,000 employees — are faring as IT management demands grow in number and complexity. By focusing on such organizations, we are able to better evaluate the trends in resource allocation, planning, and operation challenges these IT groups face. These trends and issues are markedly different from those of IT groups at Global 2000 enterprises.

Like in years past, we found responsibilities that fall under IT to be as wide and varied as the organizations themselves. IT carries a heavy burden. It is tasked with everything from project management to cloud infrastructure operations to mobile device management and more. IT organizations are expected to maintain and secure the current infrastructure, perform upgrades and expansion as needed, sustain high levels of service availability and aid users, provide technology advice and support for new business requirements, configure and manage new applications and the list goes on.

At the same time, IT organizations must increasingly contend with tighter budgets, fewer resources, increased security threats, and an expectation to contribute strategically to the business.

This year's results reveal a number of trends emerging in response, indicating change is afoot in the IT operations landscape.

Let's see what we discovered.

Key Learnings

IT has long argued that the concept of "IT maturity" is key to stakeholders viewing the organization as a strategic contributor of the business. As a result, IT has relied heavily on automation and an ability to tackle new technology implementations as the proof of its value.

But 2017 will likely be seen as the year IT earned its new badge of value: protecting the business from the modern threat landscape. The 2018 IT Operations Benchmark Survey indicates that IT is indeed seen as strategic, but this is increasingly attributable to its ability to secure and protect the network against outages. In response, IT's priorities have shifted to be almost singularly focused on network and data protection.

Why?

2017 was a remarkable year with global-scale threats like the WannaCry, Petya and Bad Rabbit ransomware attacks, Equifax' data breach, potential election meddling, and the list goes on. The stories were numerous and obvious at the end-user level, not simply in the realm of IT. With so many concerned, organizations looked to IT to be the hero. And IT's focus notably complied. Consider that among respondents who experienced a security breach in the past year, nearly half were impacted by ransomware. At the same time, vulnerability management across Windows, Mac, and third-party applications became differentiator, as those with policies in place experienced fewer
security breaches.

▶▶ **The relationship between breaches and outages cannot be underestimated.**

Among respondents who experienced a data breach during the past year:

45% had 2 to 4 outages
70% experienced a data breach

So what are midsize enterprises doing about it?

1. **Focusing heavily on backup**
On average, respondents rely on 4 backup and recovery technologies.

2. **Developing expertise and automation in key areas**
When asked to rate effectiveness in optimizing IT efficiency, more than three-quarters are performing regularly scheduled centralized antivirus/antimalware scanning and data storage backup.

3. **Embracing SaaS**
Whether it's the low maintenance or scalable costs to widespread accessibility, nearly 3 out of 4 respondents rely on SaaS-based productivity software and nearly 1 in 3 use SaaS-based storage.

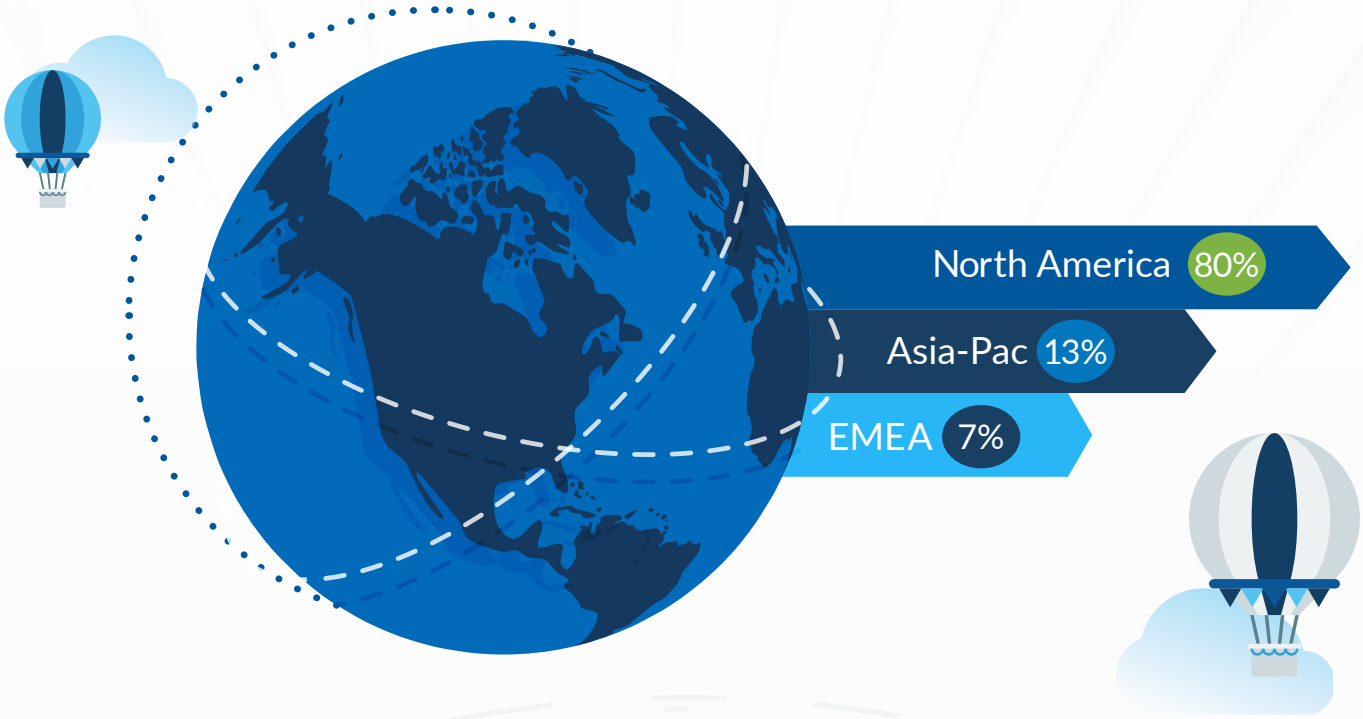
4. **Paying close attention to compliance requirements**
From healthcare to retail to financial services, regulatory compliance requirements are a fact of life that cannot be ignored.

Midmarket IT is coming into its own and fully embracing its role and technologies centered around holistically managing the network, guarding against outages, recovering instantly, and showing results via compliance.

Meet our Responders

Geographic Region

Although respondents hail from 20 countries, more than three-quarters of respondents work at U.S.-based companies.



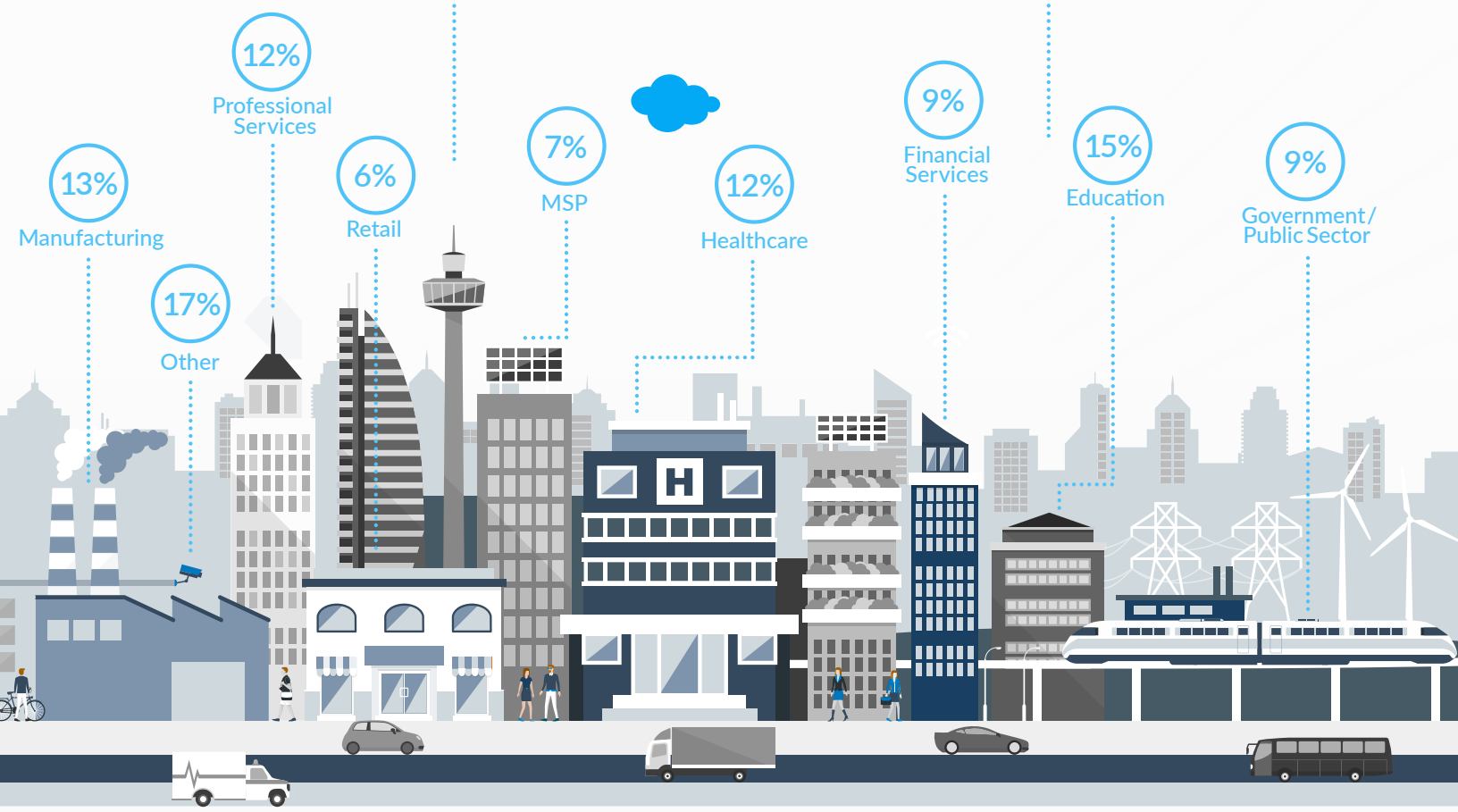
Respondents come from over

40 industries

but the most popular are:

- Education - 15%
- Manufacturing - 13%
- Healthcare - 13%

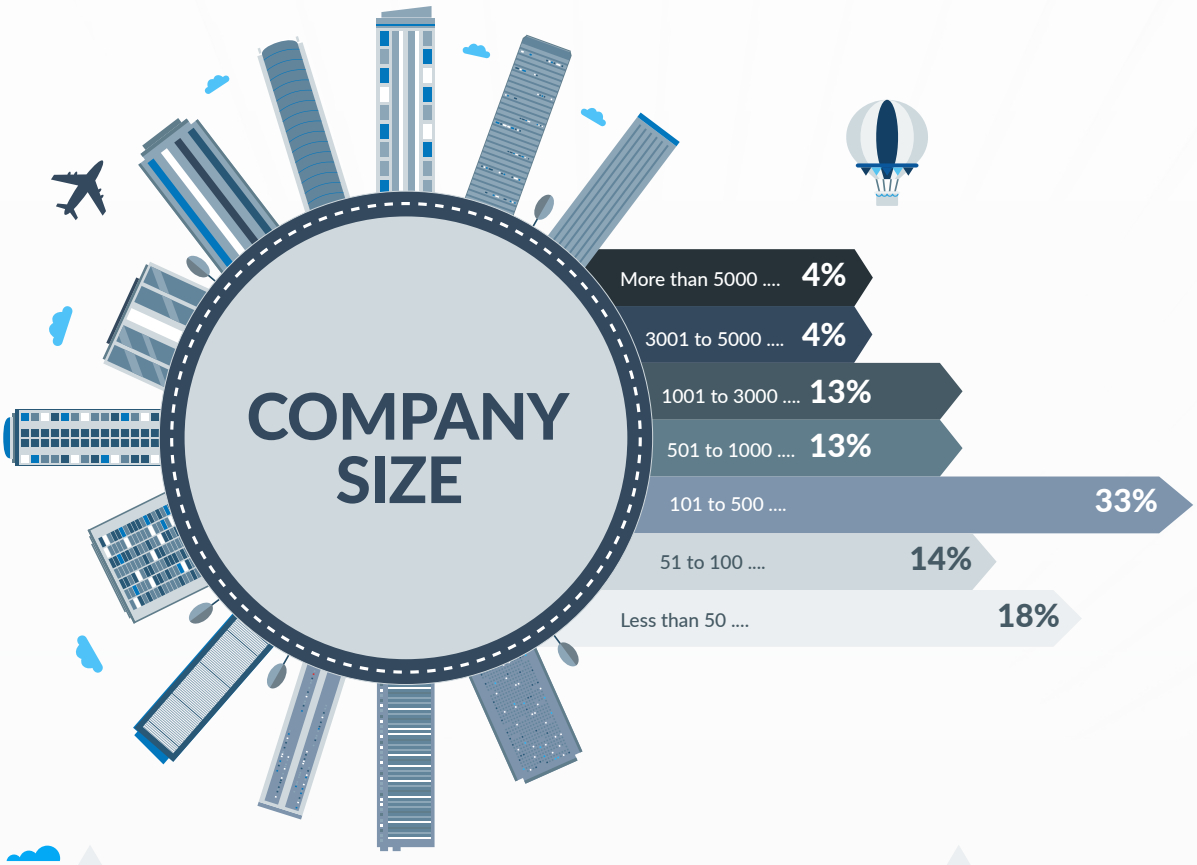
INDUSTRY



A wide swath

of company sizes were represented:

- **32%** of respondents have fewer than 100 employees in their organization
- **33%** of respondents came from companies with between 101 and 500 employees
- **35%** have more than 500 employees in their organization

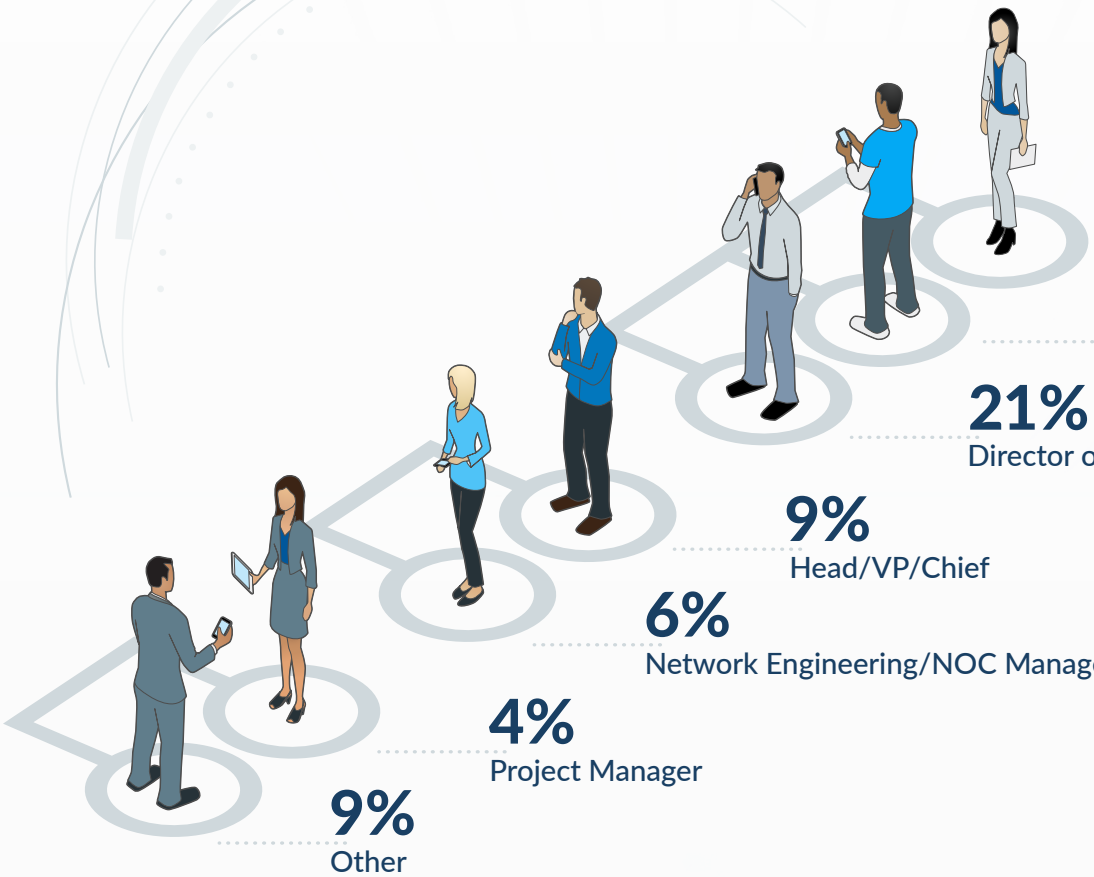


Role

60% of respondents self-identify

as being responsible for all of IT operations.

Job titles reflected this "in the trenches" identification with **62%** identifying as managers or administrators. Tactical IT operations is the daily reality for the majority of our respondents.



28% IT Manager/Supervisor

24% System Administrator

21% Director of IT

9% Head/VP/Chief

6% Network Engineering/NOC Manager

4% Project Manager

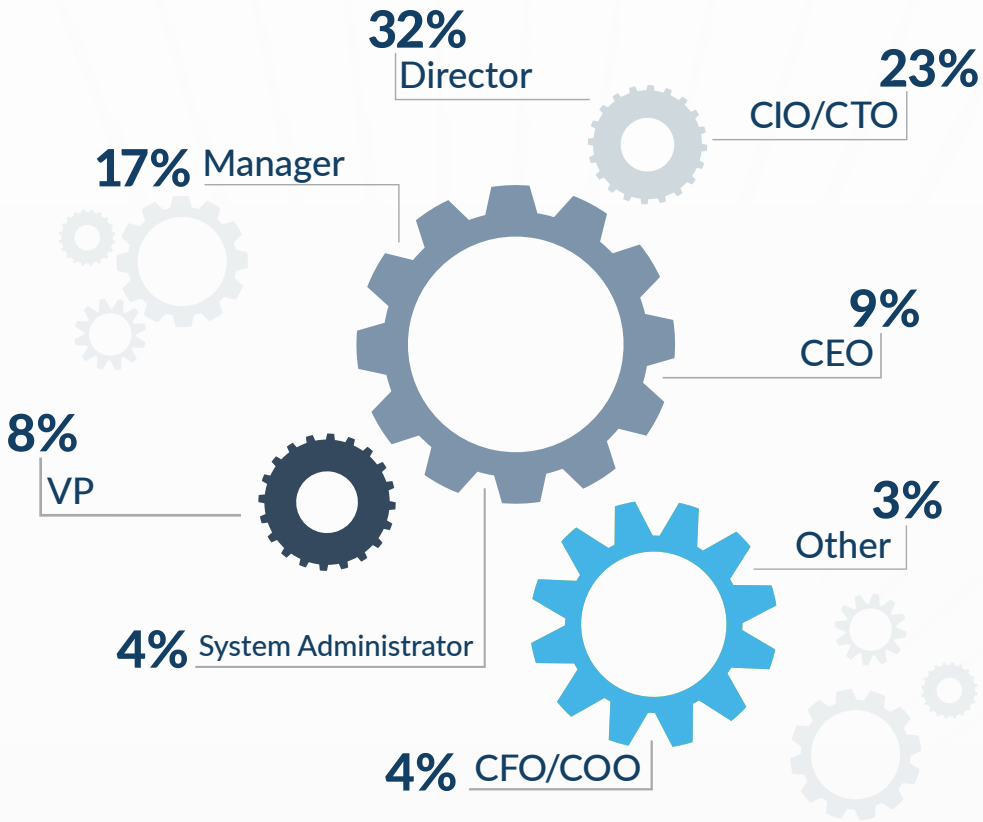
9% Other

The Role of IT in the Midmarket Enterprise

To determine how midsize businesses perceive the value of IT operations, we asked respondents several questions about who makes IT decisions and what impact IT has on the business.

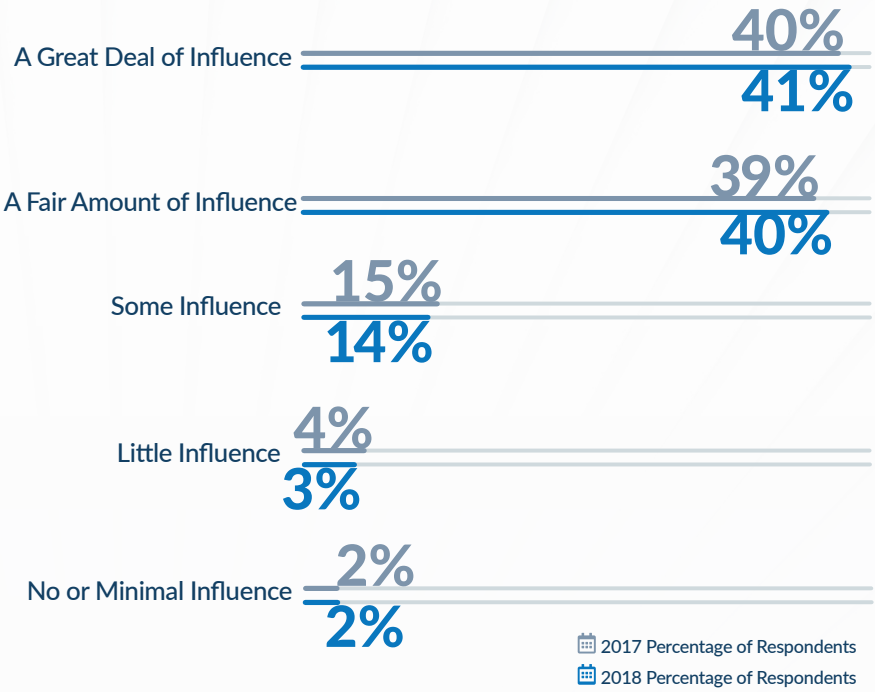
Who is the IT decider?

- In 32% of midsize enterprises, a director holds the deck for IT as the key decision maker when it comes to major IT decisions.
- In 36% of midsize enterprises, a C-level executive (typically the CIO or CTO) has the stamp.



IT Influence

Technology isn't limited to the IT department. Increasingly, technology is a critical component of business success, both from an operational and a revenue perspective. Midsize enterprises are no exception, and it is no surprise that the degree of influence that the head of the IT department has on C-level decision making is increasing.



And IT influence is expected to remain strong in 2019:

63% of respondents expect IT influence to be the same as it is today.

21% of respondents anticipate IT will be the primary decision maker and resource for all IT decisions and support.

IT Management Maturity

In the past, IT's value has been squarely focused on maturity, or "doing more with less." Our 2018 findings indicate a sea change, however. IT is seen as strategic, but with no appreciable change in maturity levels.

IT management maturity measures how well the IT management function supports the IT needs of a business — from systems and service readiness, to technology choices (e.g., cloud services), to responsiveness and through to strategic alignment and business enablement. This groundbreaking model was developed specifically for midsize enterprises based on insights and feedback from midsize Kaseya customers. Previously, all established IT maturity models were relevant only for much larger enterprises.

The model consists of five levels. While IT maturity remains important, we believe it is no longer a harbinger of success. Our trend data indicates that over the past three years, on average IT organizations have self-identified as:

Reactive
34%
Responding to individual user challenges and requests

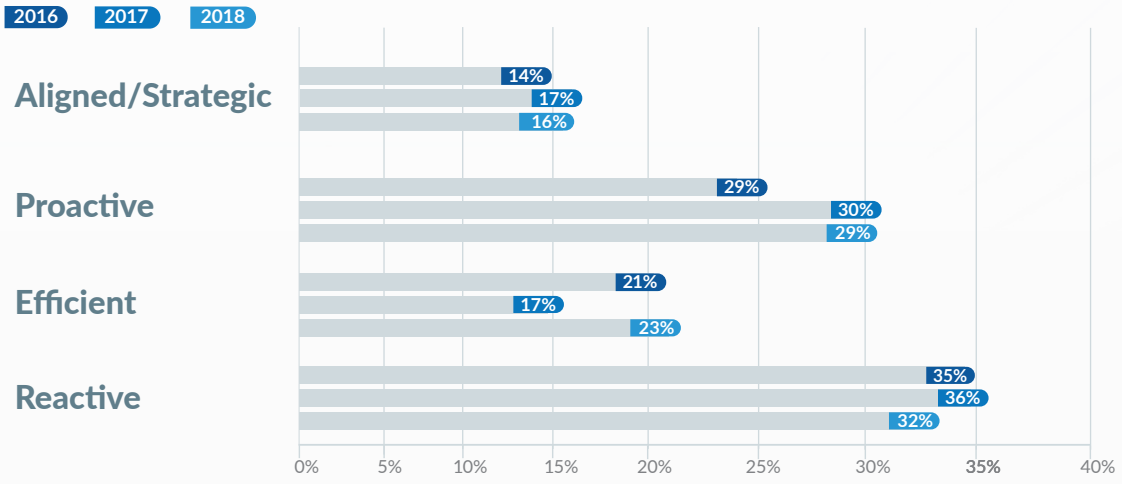
Efficient
20%
Having a systematic approach to solving known issues and dealing with daily tasks

Proactive
29%
Taking a proactive approach to IT management, automating repetitive tasks and many remedial actions

Aligned
6%
Tracking and managing against service-level agreements (SLAs) or availability/performance expectations

Strategic
10%
Achieving IT operational excellence and taking a strategic role in driving business innovation

There has been little variance in year-over-year identification as the following chart shows.



Yet IT organizations are playing an increasingly strategic role in organizations, leading us to believe that overall IT maturity is less critical to success than in past years. At the same time, as IT becomes an increasingly vital component of the customer experience and thus business success, lines of business are increasingly involved in IT decision making.

More than ever, how IT approaches operational functions, particularly around backup, data protection, and security, will determine its role within the organization.

IT Operations

A new champion concept has emerged. Operational maturity is still important, but IT is clearly focused on security, backup, and data protection.

To determine how IT approaches operational functions, we asked a number of questions around practices in backup and disaster recovery, security, compliance, endpoint management, and SaaS adoption.

As IT's importance grows, how it approaches these areas will become even more critical to the success of midsize enterprises.

2018 Technology Priorities

When asked about top priorities for 2018, it is not surprising that improving security takes precedence with the majority of respondents.

More 54% of respondents cite improving security a top priority for 2018, far higher than any other priority, and nearly twice that of reducing costs and compliance, the second and third.

2019 Technology Concerns

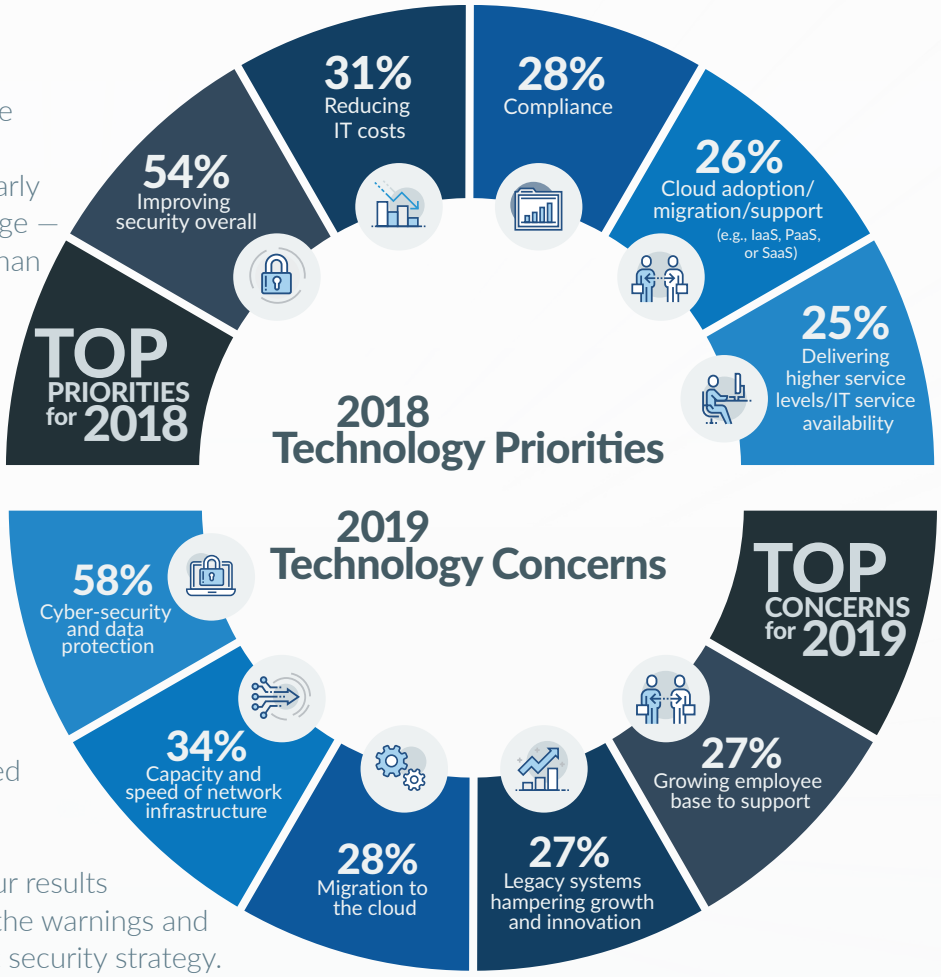
The focus on security is not likely to abate anytime soon. In terms of anticipated concerns for 2019, security was cited nearly twice as often as the next closest challenge — capacity and infrastructure — and more than twice that of No. 3 — cloud migration.

Security

Best-of-breed IT organizations in midsize businesses take security and data protection seriously, and as a result they are using layered security and modern vulnerability management.

No matter your size or industry, IT security is mission-critical. A data breach has serious consequences for a midsize enterprise, and if not handled correctly it can decimate the business.

First, the good news: Across the board our results indicate that organizations have heeded the warnings and understand the importance of a stringent security strategy.



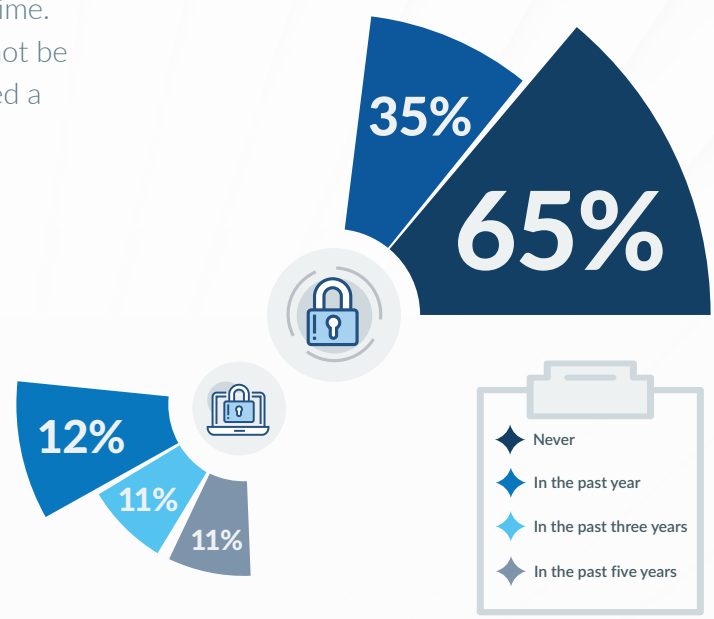
65% of respondents have not experienced a single security breach in the past 5 years.

Among the 35% that have, the responses are evenly split, with 12% having experienced a security breach in the past year.

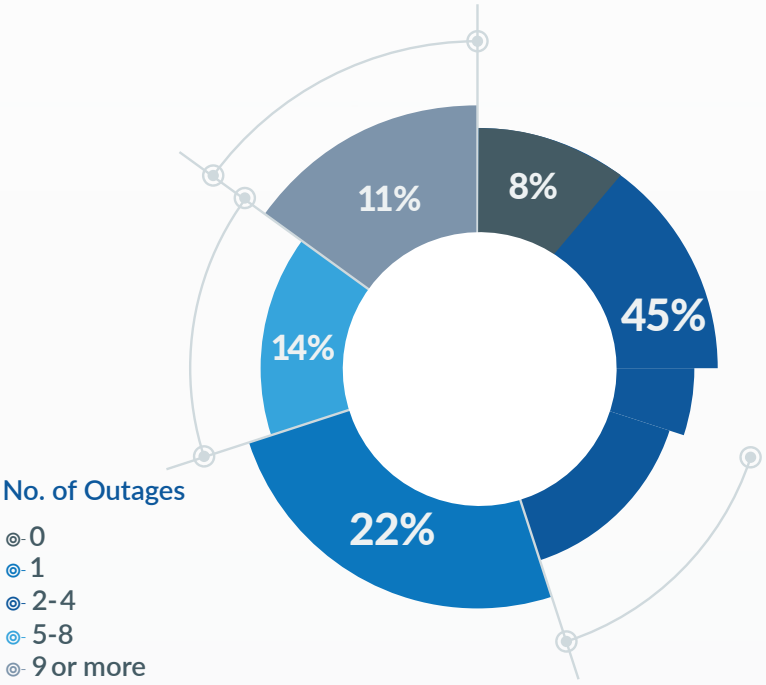
Fewer security breaches mean less unplanned downtime. The relationship between breaches and outages cannot be underestimated. Among respondents who experienced a data breach during the past year:

45% had 2 to 4 outages

70% of those who had more than 1 outage experienced a data breach.



Fewer Breaches = Less Downtime



Ransomware Takes Hold

The not so good news is that cyber-criminals are constantly changing their approach. The latest scrounge: Ransomware, malicious software that blocks access to a system until a ransom is paid.

22% (more than 1 in 5) of respondents were impacted by ransomware this past year.

Among respondents who experienced a security breach in the past year,

44% were hit with ransomware.

Our respondents were not alone, however. **Between 2016 and 2017, over 2.5 million users were affected by ransomware.** This trend shows no sign of abating. The effects of a ransomware attack are particularly onerous and usually result in loss of data, the ensuing liability of that loss, and the extortion of financial resources in an attempt to get the data back.

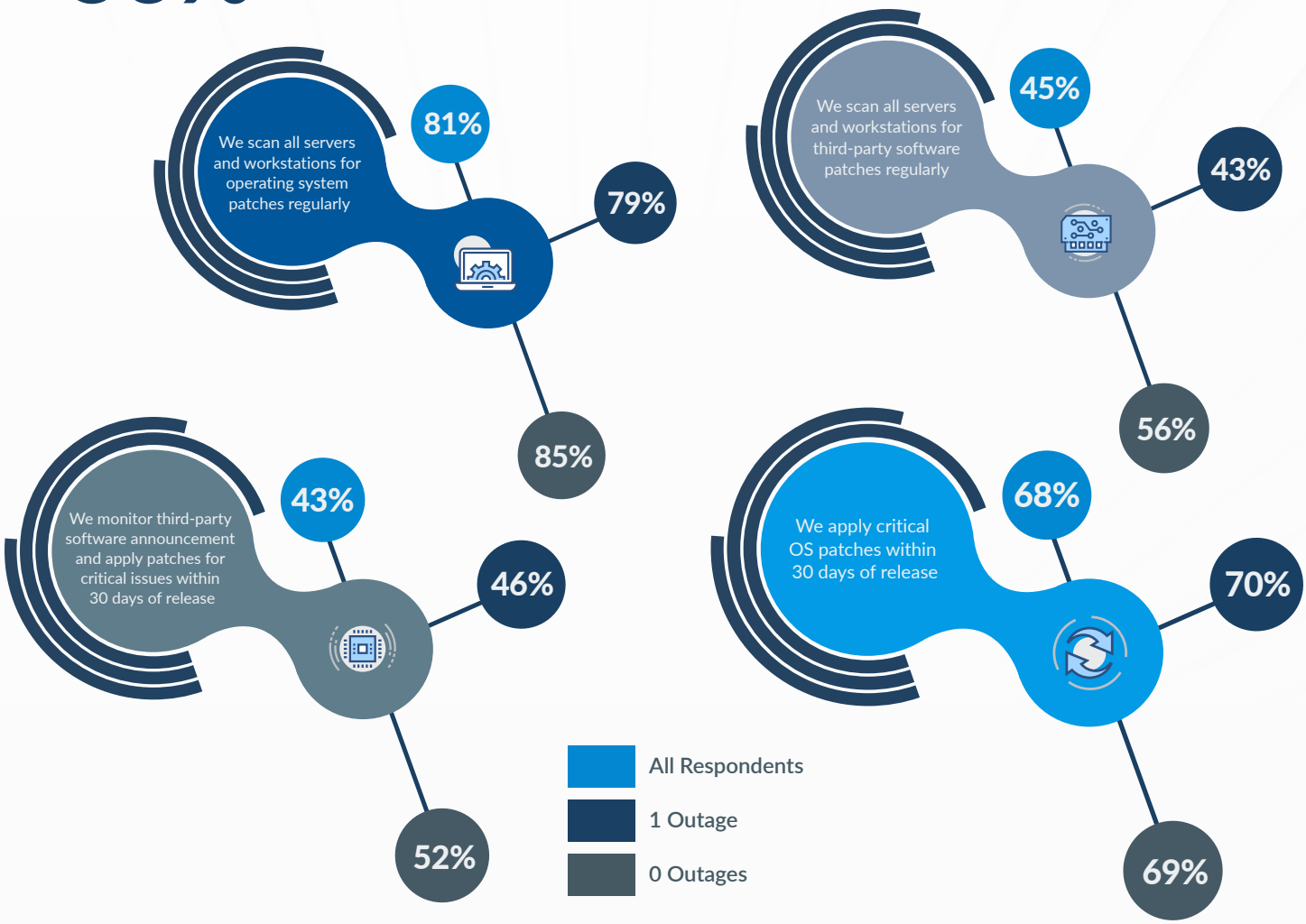
For a midsize business this combination can be truly devastating.

Vulnerability Management Key to Preventing Outages

The solution is an effective vulnerability management strategy, ideally one that follows a layered approach. The importance of OS patching goes without saying, and indeed, it is ubiquitous across the board. Among respondents with no outages lasting longer than 5 minutes this past year, the primary differentiator is monitoring third-party applications.

52% of respondents monitor third-party software announcements and apply patches for critical issues within 30 days of release compared to 43% of all respondents.

56% of respondents scan all servers and workstations for third-party software patches regularly compared to 45% of all respondents.



Monitoring third-party applications is a key part of a vulnerability management strategy for organizations that want to ensure uptime.

For vulnerability management to truly be successful, however, you cannot put all of your eggs in one basket. You need a layered approach. Companies that did not experience any outages in the past year report having on average almost 3 policies in place, while the average among all respondents is closer to 2.

Outages and the Rise of Backup and Disaster Recovery

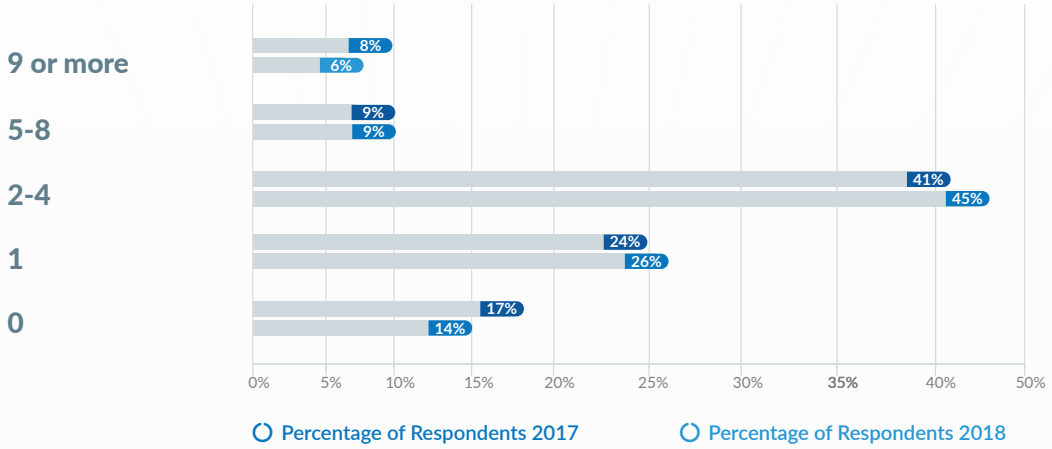
There is a direct correlation between deploying an optimal backup and disaster recovery solution and maximizing uptime.

Uptime is critical. If your systems are down, you risk lost sales and reputational damage. The longer the outage, the larger the revenue hit.

86% of respondents had at least 1 IT network outage lasting longer than 5 minutes in the past year.

74% had more than 1 outage in the past year.

45% of respondents had between 2 and 4 outages lasting longer than 5 minutes in the past year.



Fortunately, it is possible to mitigate the potential impact of downtime with an effective multi-prong backup strategy, and companies are well aware of this.

The top 5 backup and recovery actions among respondents are:

90%
We back up servers

69%
We back up locally and offsite

38%
We have the capability to automatically recover to a separate site (disaster recovery)

38%
We have a formal business continuity and disaster recovery plan approved by management

37%
We back up to an appliance

On average, respondents rely on 4 backup and recovery technologies.

SaaS Adoption

SaaS brings many benefits, but smart enterprises know it also carries its own set of challenges.

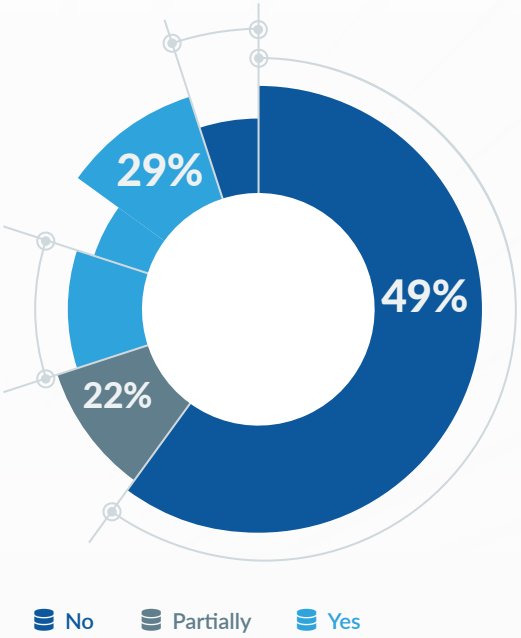
Software as a Service (SaaS) offers myriad advantages, from low maintenance to scalable costs to widespread accessibility of applications. SaaS-based applications are a natural fit for many midsize businesses.

The most popular among respondents are:

1. Office 365 **72%**
2. Dropbox **29%**
3. Salesforce **17%**
4. G Suite **17%**

While turning to a SaaS-based-application provides the functionality that midsize companies need, organizations own their data and with that comes the responsibility of data protection — unless they opt to outsource that as well. A third-party backup and recovery solution can alleviate this burden.

Slightly more than half of our respondents are turning to a third-party vendor to protect at least some of their data.



Compliance

When it comes to meeting compliance requirements and InfoSec standards, size has little bearing. Enterprises must adhere to the same rules as their larger counterparts.

PCI or HIPAA/HITECH are the most common compliance regulations that respondents follow. This is not surprising given that **78% of respondents are in the United States.**

Regulation

- **PCI** 33%
- **HIPAA/HITECH** 31%
- **ISO 27001** 18%
- **CIS** 17%
- **SOX** 13%

GDPR ranked No. 6, with 11% of respondents adhering to it. As GDPR had yet to go into effect at the time of our survey (April 2018) and many midsize enterprises are under-estimating its potential impact, it is not surprising that the percentage is slightly higher than the percentage of EMEA respondents (7%).

Endpoint Audits

Knowing what is in your infrastructure is essential to being able to manage it.

84% of respondents audit endpoints as part of their asset management processes. Here's what they look for:

- **OS information** 68%
- **Installed software** 64%
- **Computing information** (e.g., CPU, RAM, or disk) 56%
- **Vendor and serial number/ warranty information** 53%
- **Software licensing data** 48%
- **User account information** 46%

Development of Capabilities and Strengths

As IT influence grows, understanding where strengths lie is critical. Knowing where you excel enables you to make an informed decision about what must be improved or outsourced. When asked to rate effectiveness in optimizing IT efficiency, the following technologies and strategies were the most common areas of expertise.

- **Centralized Antivirus/Antimalware Scanning** 77%
- **Data Storage Backup (Daily, Weekly, Monthly)** 75%
- **Server Monitoring** 68%
- **Centralized Patch Management** 62%
- **Remote Device Access/Control** 61%

Given the criticality of security and backup, it is encouraging that over 75% of respondents self-identify with competence in these areas, and, even more importantly, a majority are able to demonstrate that through operational decision making.

Conclusion: All Roads Lead to IT as the Guardian and Protector of the Business or Organization

Technology has made it possible for midsize businesses to compete with larger players. In many ways, size matters less than ever. This has brought numerous opportunities along with a host of challenges.

Chief among those is IT security. When it comes to IT security, midsize businesses are equally at risk as their larger counterparts. However, a Fortune 500 company generally has deeper pockets to absorb a successful ransomware attack.

Prevention is always the best defense, but for a midsize enterprise it is essential to survival. Security is the No. 1 concern among our respondents for a reason!

Hence, a mature and well-planned out security plan is not optional.

At the same time, security is not the only IT issue with which midsize organizations must contend. Cost constraints, scalability, and maintaining an optimal customer experience are still important for success. IT is expected to take an increasingly strategic role.

Operation maturity still matters, but the definition is changing. Security expertise is becoming a cornerstone of it, and it is tantamount to survival. Priorities for IT organizations are rapidly evolving, and IT has two choices: Mature quickly in a variety of specific areas or partner with a third party to get the get access to experience and knowledge that you need.

> For an IT organization to be truly strategic, it must develop specialization in security or obtain the skill set externally through a third party if it cannot do so.

Survey Methodology

Kaseya conducted its annual IT Operations Benchmark Survey using a structured questionnaire in April 2018.

All participants were asked if they were primarily employed in an IT operational role with some responsibility for IT infrastructure or IT services deployment, operation, management, or support. Only responses from those who answered in the affirmative were included in the survey results. Among those, 60% of the final respondents identified their primary responsibility as “all of IT.” In total, valid responses were received from 1,287 IT professionals. The main focus of the survey was IT operations (individuals and groups) at midsize organizations, which we define as organizations with up to 5,000 employees. Only companies in this range are included in the survey results.

ABOUT KASEYA

Kaseya is the leading provider of complete IT infrastructure management solutions for managed service providers (MSPs) and internal IT organizations. Through its open platform and customer-centric approach, Kaseya delivers best in breed technologies that allow organizations to efficiently manage, secure, and backup IT. The Kaseya IT Complete platform is the industry's most comprehensive, integrated solution suite purposely engineered to help IT both run and grow the business. It empowers businesses to command all of IT centrally, easily manage remote and distributed environments, simplify backup and disaster recovery, and automate across IT management functions. Kaseya solutions manage over 10 million endpoints worldwide. Headquartered in Dublin, Ireland, Kaseya is privately held with a presence in over 20 countries. To learn more, visit www.kaseya.com.