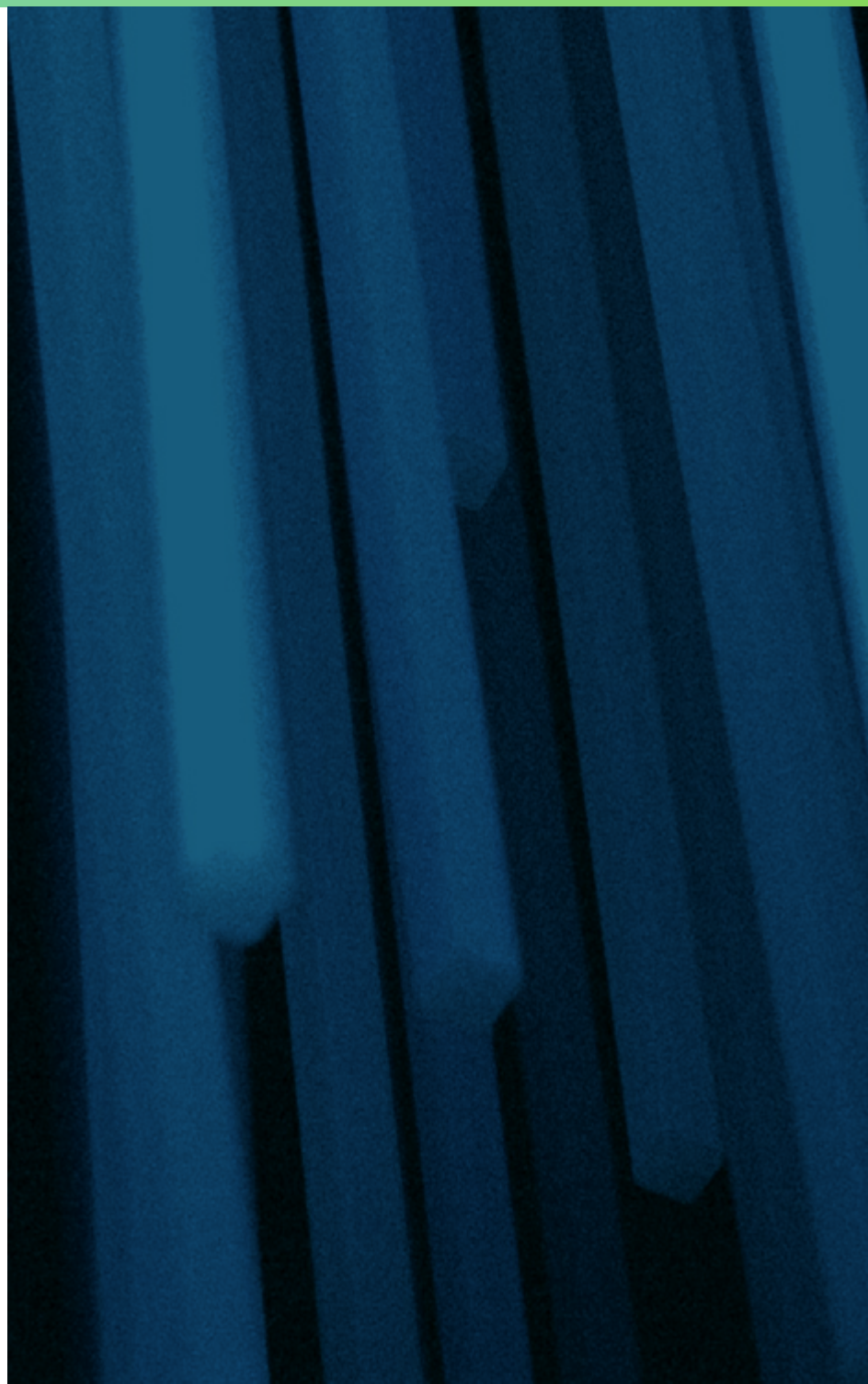
Uncovering the

Latest IT Trends, Threats & ROI Solutions Deliver

Central by LogMeIn

Table of Contents



Introduction

The IT landscape has evolved drastically over the last few years, and one of the biggest challenges is staying ahead of ever-changing security threats. IT teams are constantly being asked to do more with less, so implementing solutions that embrace automation, enhance security and provide a single pane of glass view are absolute necessities. **Remote Monitoring and Management (RMM)**, defined as the process of supervising and controlling IT systems (laptops, desktops, servers), enable automation, security, and control, and have thus become a crucial component in every IT professional's toolkit.

Both Internal IT teams and Managed Service Providers (MSPs) rely on RMM solutions to centrally discover, provision, deploy, update and troubleshoot endpoint devices; however, quantifying the true value RMM software delivers is challenging.

LogMeIn Central commissioned the market research firm Lab 42 Research LLC to uncover the latest IT trends and security concerns, and quantify the value, importance and ROI that a Remote Monitoring and Management solution delivers to small and medium-sized businesses.

We surveyed 500 IT professionals at organizations ranging from 1 – 3,000 employees, across a variety of industries in North America and Europe. Survey respondents held a range of IT roles, with 7% at the C-level, 70% at the director or management level and 23% at the administrator level.

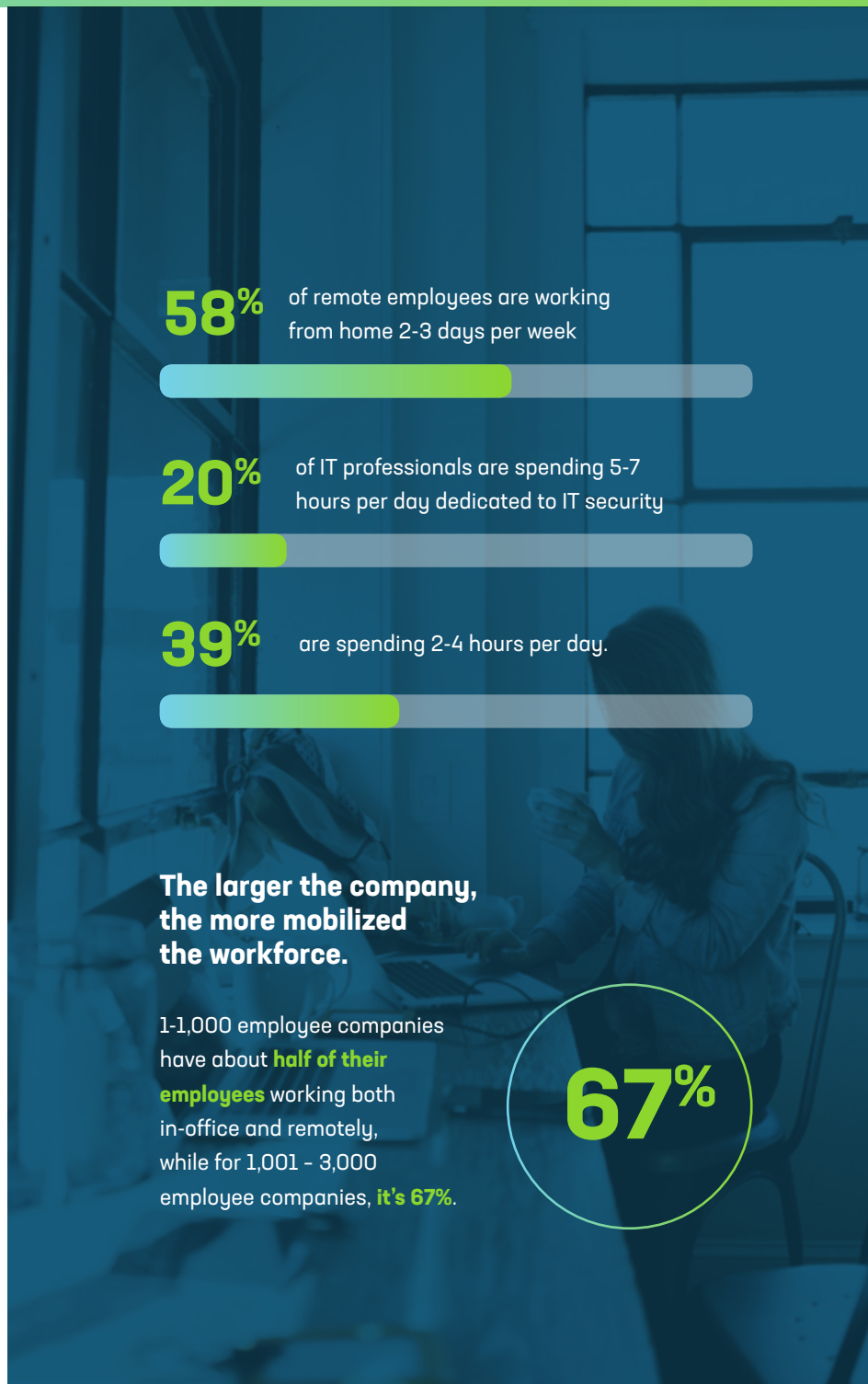
> **In this report, we reveal the latest IT trends and best practices to keep companies secure, and we uncover the ROI of implementing a Remote Monitoring and Management solution for small and medium-sized businesses.**

7 Key IT Trends

1 | The Modern Workplace is Here. Modern IT is Not.

More than half **(58%)** of organizations have a mix of in-office and remote employees working at their companies, demonstrating the prevalent shift toward a remote workforce. While working from anywhere is becoming the new norm, IT professionals struggle with ensuring all company devices stay compliant and protected.

Many IT professionals are dedicating anywhere between **2 to 4 hours** a day to IT security, including monitoring, patching and managing antivirus. Since IT professionals are spending a significant portion of their day addressing security concerns in this changing landscape, implementing solutions that provide them with the ability to take back their time and automate some of these security tasks is an absolute necessity.



30%

of IT professionals did not know how many endpoint devices their company had

15%

of IT professionals did not know how many endpoint devices their company had.

IT professionals unaware of the number of endpoint devices under their management has gone down by **HALF** from 2018 to 2019!

2 | IT Professionals Are More in Control of Their Endpoint Infrastructure.

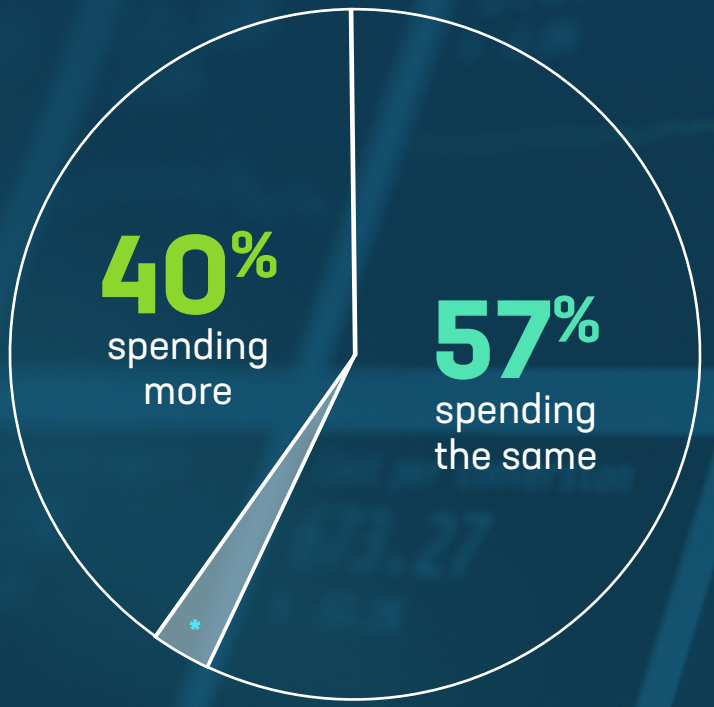
As the workforce continues to mobilize, the endpoint landscape continues to evolve rapidly. **BYOD** (bring your own device) trends mean IT teams have to rethink how they manage and secure their endpoints and company networks. Even though the endpoint landscape is becoming more complex, IT professionals are keeping up well and becoming more in control of their endpoint infrastructure with only 15% not knowing how many endpoint devices are under their management in 2019, compared to **30%** in 2018.

3 | As Risks Evolve, so Should Investment.

Managing budgets is a constant challenge for companies of all sizes, and there's never enough to go around. From expansion to retention, to security to cultural development, organizations are faced with tough decisions in determining their priorities for the year and ensuring those priorities get the appropriate budget needed to fulfill their businesses' strategic direction.

Over the past few years, security and an emphasis on IT have been evolving focal points for budget needs. **40%** of IT professionals anticipate their 2020 IT budget to be more compared to 2019, and **over half (57%)** expect their **budget to stay the same**.

2020 IT Budget compared to 2019



* **3%** spending less

Top 5 Uses of IT Budget

- **Firewalls**
- **IT-Training & Development**
- **Anti-virus on endpoints** (desktops, laptops, etc.)
- **Anti-malware on endpoints** (desktops, laptops, etc.)
- **Employee training**

IT professionals are prioritizing budget on preventative security measures and on education. Both **IT and employee training** top the list of budget priorities in 2019, demonstrating the strong shift from a reactive to proactive approach when it comes to company security.

When it comes to budget, there are both time and cost implications. Of IT professionals that are dedicating more budget in 2020, the biggest time investments include **IT and employee training**, while the biggest cost investments include **anti-malware on endpoints, firewalls and anti-virus on endpoints**.

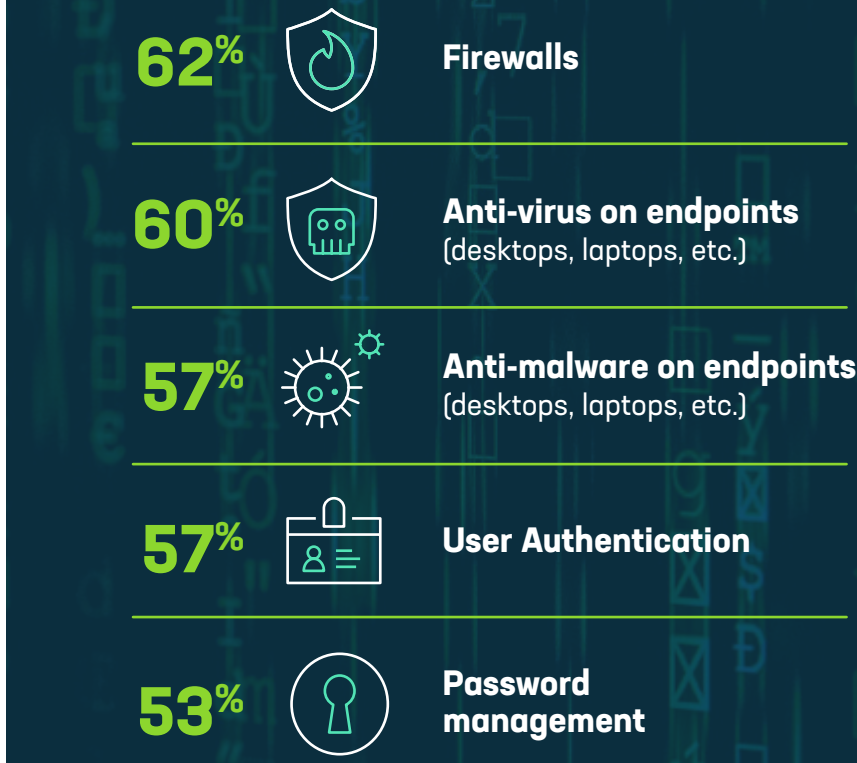
Although remote monitoring and management is an essential piece of the IT toolkit, the large majority of IT professionals **(80%)** are allocating 25% or less of their budget to RMM. IT professionals feel that RMM solutions should not break the bank, so it's important that the solutions they deploy leave additional budget for further security measures and training.

4 | Most Important Security Measures Tackling Biggest Concerns Head On.

When looking at overall security, the majority of IT professionals feel that the following investments are most important to the company's overall safety and security. While firewalls, anti-virus and anti-malware are in-line with budgetary priorities, user-authentication and password management are considered extremely important, but they don't make the cut for getting as much time and budget as they should.

Only a **third** of IT professionals are prioritizing **patch management**, increasing their risk of breaches and cyberattacks exponentially!

Most important security measures to protect companies from cyber-threats



What keeps IT professionals up at night?

Biggest IT security concerns in the next year include:

MSPs are significantly more concerned with **internal data breaches** and **rapidly evolving technology practices**, whereas **internal IT teams** are more concerned with **employee behavior/habits**.

5 | When it Comes to Security, Education is King.

With the threat landscape evolving, IT professionals must adapt their approach or get caught in the crossfire. **Over the past 5 years**, the approach to handling these security concerns has changed, and **education** is the most important enhancement at companies of all sizes.

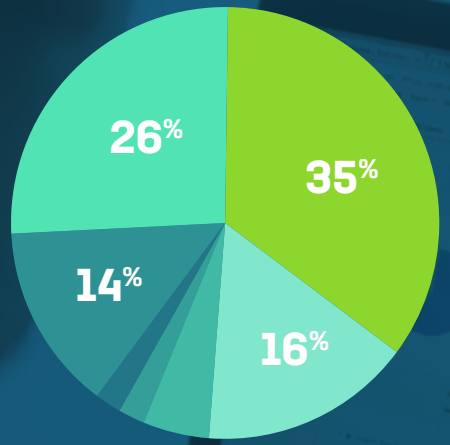
Although security breaches are on the rise, IT professionals feel confident in the safeguards they have in place to protect their companies and end users.

6 | Cost is Insurmountable, and Companies Don't Recover.

Looking at the top-3 biggest IT security concerns, the cost of each occurring ranges, but the majority of companies would be hit with costs ranging from **$10k to $100k**, with about 10% of organizations paying **$500k to $5 million+**.

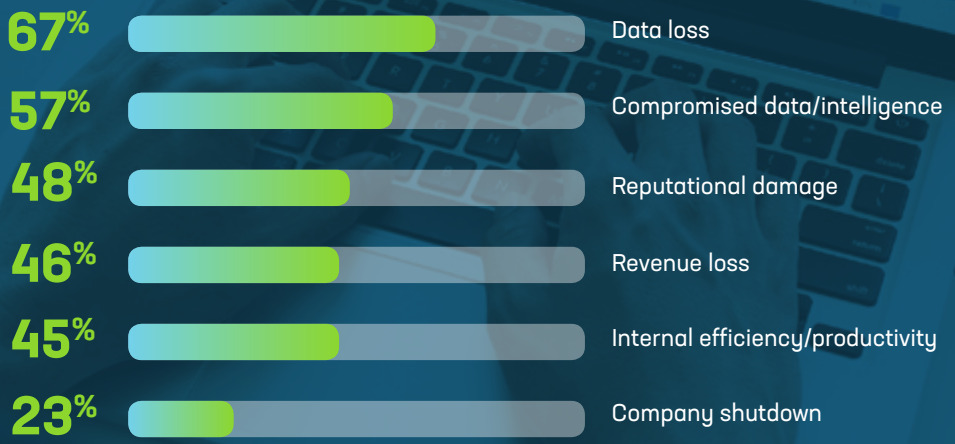
Financial loss is just one small piece of the total cost of an IT security concern becoming a reality. Data loss, compromised data/intelligence and reputational damage are some of the biggest concerns for the majority of IT professionals, and **nearly a quarter** (23%) would experience a company shutdown!

Amount companies would pay for a Malware attack:



- **14%** No monetary impact
- **26%** Less than $10,000
- **35%** $10,000 to $100,000
- **16%** $100,000 to $500,000
- **5%** $500,000 to $1 million
- **2%** $1 million to $5 million
- **2%** $5 million+

Biggest risks IT security concerns pose:

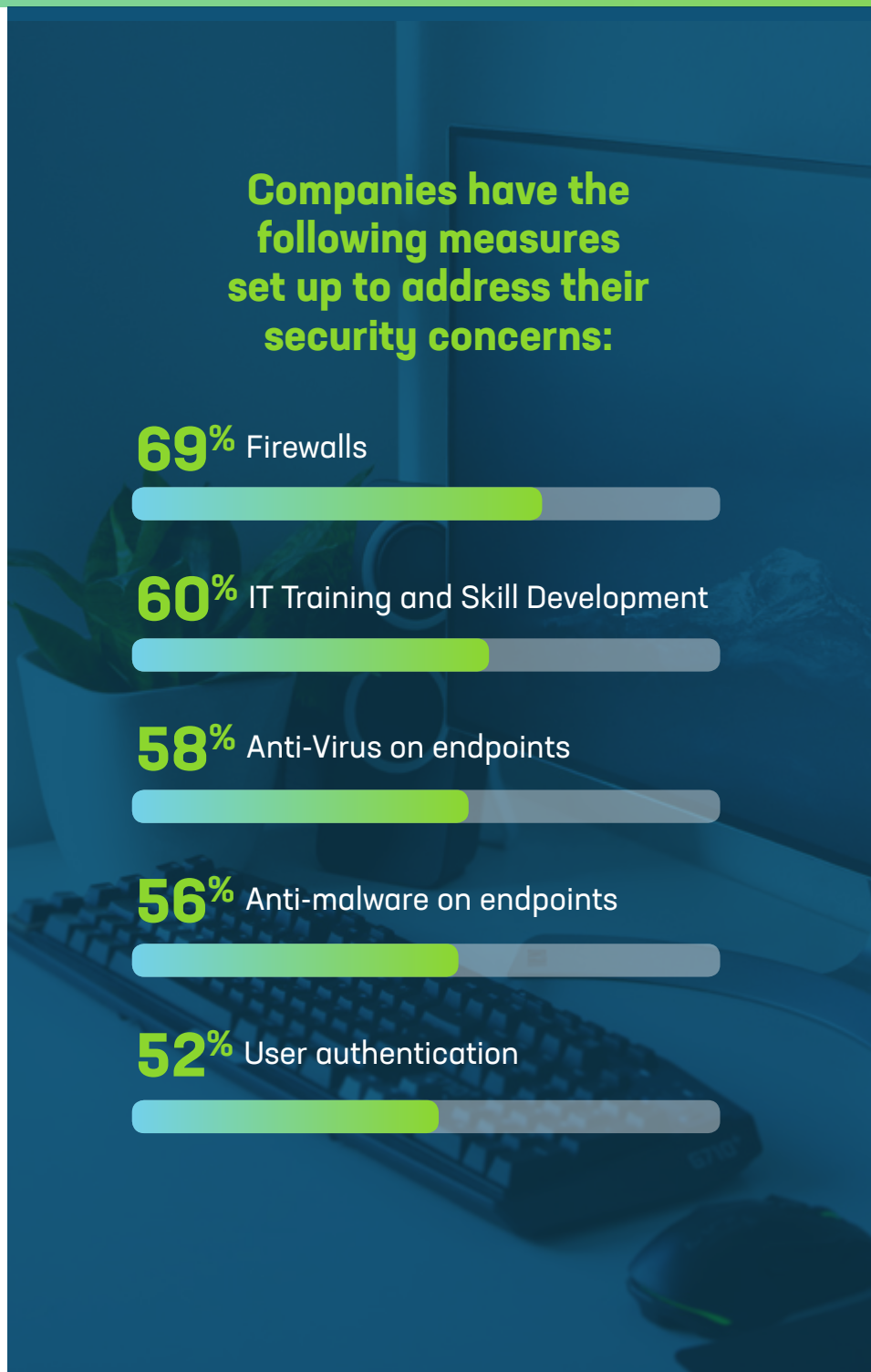


Although most companies simply don't recover from a security breach, the majority of IT professionals **(86%)** feel prepared to deal with these security concerns and tackle them head-on!

7 | Strong Shift from a Reactive to Proactive Approach.

Nearly half **(47%)** are taking a **proactive** approach to tackling security concerns and implementing strategies and policies before a problem/attack/breach occurs, but **32%** are handling the concern **as it happens**, and 15% are addressing it **after** it's occurred! Implementing proactive measures is crucial in ensuring each company and its employees stay protected, and it's the best way to not only prevent a security concern but also prevent the dire consequences that come with a breach.

1 in 5 companies are shifting from a reactive to **proactive IT support** model. It's no longer enough to simply address a problem when it happens, and more and more companies are looking to implement solutions that resolve concerns before they become problems, and even more so, before end users even know something's wrong.



Of the measures set up, the top three most effective ones include:

Firewalls

Anti-virus on endpoints

IT-Training & Development

Of all measures put in place, companies feel that they should be doing even MORE in the following areas:

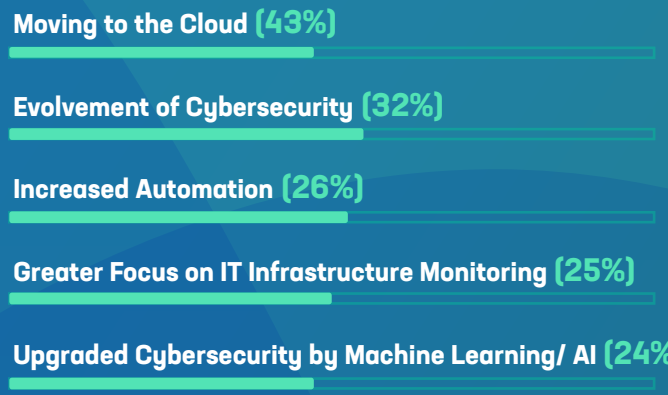
- IT Training and Skill Development
- Employee Training
- Multi-factor Authentication
- Encryption
- Password Management

Keeping up with Evolving IT Trends

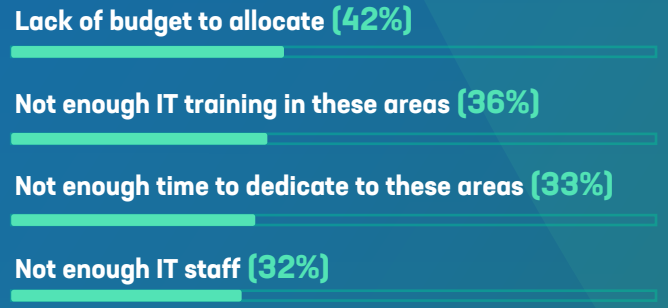
More and more companies are shifting away from on-premise solutions and embracing the cloud, and **1 in 4 companies** are implementing tools that enable their IT teams to take back their time and automate manual tasks.

Keeping up with evolving **IT trends is a challenge**, and the biggest hurdles include lack of budget, training, time and an IT labor shortage. To tackle these shortcomings, IT teams urgently need to ensure they implement solutions that give them a single pane of glass view into their IT infrastructure, allowing them to enable proactive measures to take back their time and focus on high-priority projects.

Biggest IT Trends Driving Change



Biggest Challenges Companies Face in Keeping Up with IT Trends



Value RMM Delivers

Remote Monitoring and Management (RMM) software is an **integral piece of the IT toolkit**, both for Internal IT teams and MSPs.

77% of IT professionals have a Remote Monitoring and Management (RMM) solution deployed. As organizations grow, both in employee size and office locations, RMM becomes even more prevalent and essential to supporting daily operation of the IT team.

Although 1 in 5 organizations **do not** have an RMM solution in place **(21%)**, it's growing in need, as **more than half (51%)** of organizations state it's an extremely important initiative, and **89%** state it's either extremely or somewhat important compared to all initiatives IT teams have coming up in the next year.

For the 21% of organizations who do not currently have an RMM solution, top 5 reasons include:

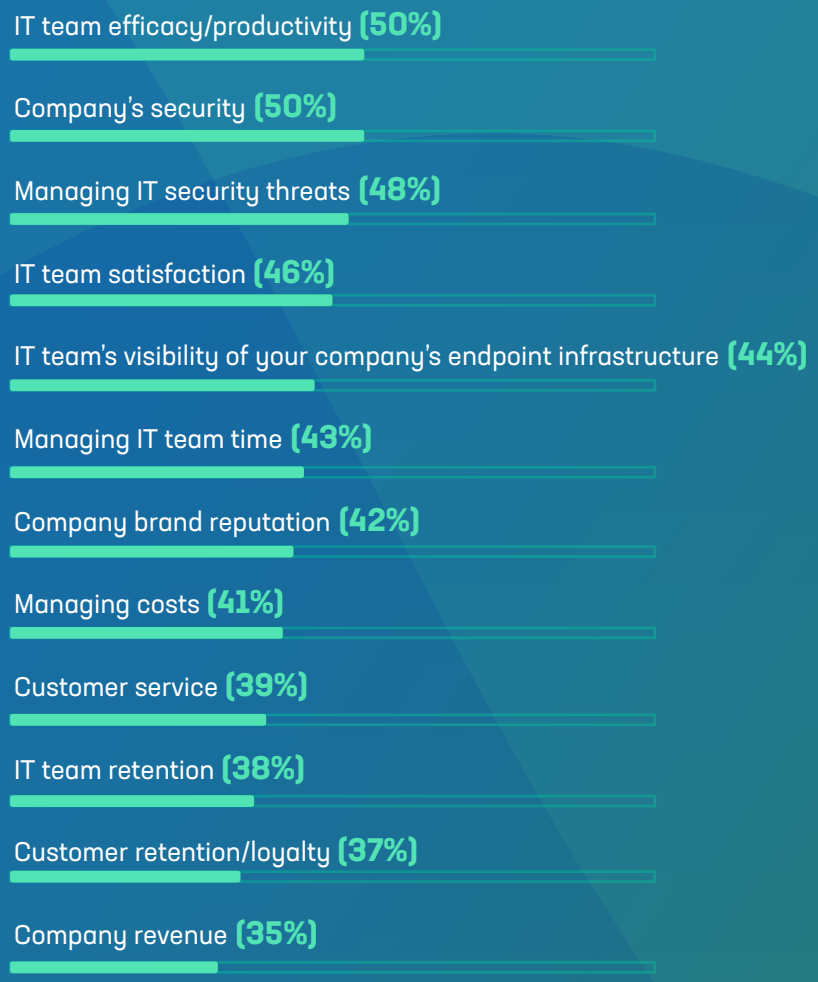
44% of companies feel RMM is very important when it comes to their company's overall safety and security, and nearly all companies (97%) feel it's somewhat important.

When it comes to **value**, the stats are in, and they're undisputable!

Thinking about all the positive outcomes and benefits RMM has on companies, both in terms of **tangible** benefits like dollars earned or saved, and **intangible** benefits like employee satisfaction and customer retention, **38%** feel RMM delivers a lot of value overall, while **90%** feel RMM delivers significant value.

RMM has the **biggest impact** in increasing IT teams' productivity, improving company security and managing security threats.

The areas where Remote Monitoring and Management software deliver the most value include:



Quantitative Impact and ROI

The value implementing remote monitoring and management software delivers is extremely high, but taking that a step further, quantifying the impact is challenging but crucial to get the full picture.

Breaking down the ROI of RMM: Time Savings

The majority of IT professionals experience spending 30 minutes to 4 hours per day on each of the following tasks **BEFORE** implementing an RMM solution:

TIME SPENT

30 minutes to 4 hours per day (67%) troubleshooting issues on employee devices

30 minutes to 4 hours per day (70%) on manual IT tasks (deploying patches, installing software, distributing files)

30 minutes to 4 hours per day (70%) accessing employee devices

AFTER implementing an RMM solution, the majority of IT professionals have been able to save between 30 minutes and 4 hours per day, enabling them to focus on other high impact initiatives and get back a large portion of their time.

TIME SAVED

30 minutes to 4 hours per day (67%) saved on troubleshooting issues on employee devices

30 minutes to 4 hours per day (67%) saved by automating IT tasks

30 minutes to 4 hours per day (67%) saved remotely accessing employee devices

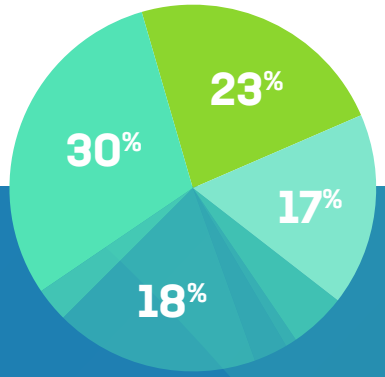
Breaking down the ROI of RMM: On-Site Visit & Support Call Improvements

More than half (53%) of organizations pay their IT technicians that handle calls and on-site visits **$20-$100 per hour**.

Each IT technician does between **6 and 20 on-site visits per week (56%)**.

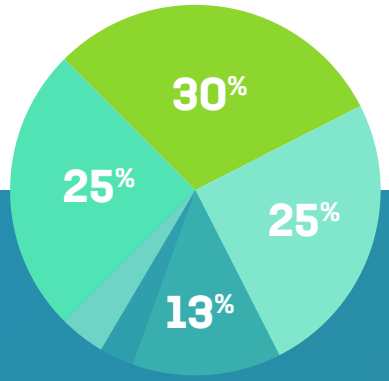
Each on-site visits typically runs between 1-2 hours **(54%)**, and a quarter of IT technicians spend 3-5 hours per visit **(24%)**.

Hourly rate of IT technicians



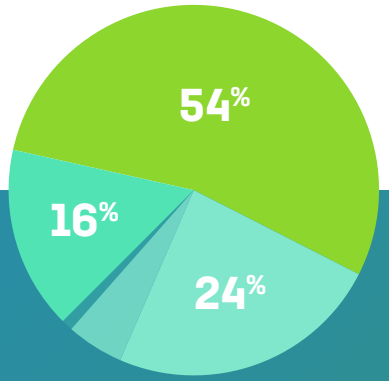
(3%)	Less than $20/hour
(30%)	**$20 to $50/hour**
(23%)	**$51 to $100/hour**
(17%)	**$101 to $150/hour**
(5%)	$151 to $200/ hour
(1%)	More than $200/hour
(3%)	I don't know
(18%)	My company does not employ hourly technicians (only salaried IT staff)

Number of on-site visits per week



(25%)	**Less than 5 visits**
(30%)	**6 to 10 visits**
(25%)	**11 to 20 visits**
(13%)	**21 to 50 visits**
(3%)	50+ visits
(4%)	I don't know

Length of each on-site visit



(16%)	**Less than 1 hour**
(54%)	**1 to 2 hours**
(24%)	**3 to 5 hours**
(5%)	6 to 7 hours
(1%)	More than 7 hours

After implementing RMM, IT technicians have been able to shave off 4 to 10 minutes per call, which translates to thousands of hours saved each year!

Time saved on each support call after implementing an RMM solution to remotely access work stations:

Breaking down the ROI of RMM: Biggest Improvements and Cost Savings

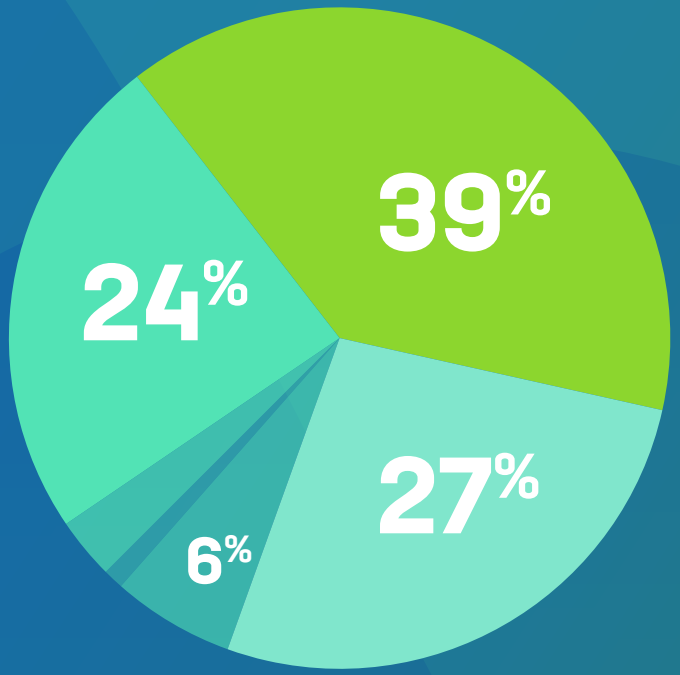
When looking at overall improvement to companies, RMM has had the **biggest impact** in improving IT teams' productivity and optimizing their time so they can focus on **high-impact initiatives**.

Biggest Improvements After Implementing an RMM Solution

Breaking down the ROI of RMM: Biggest Improvements and Cost Savings

Nearly 75% of IT professionals are saving at least **$50,000** a year from implementing a RMM solution for their company!

Cost Savings Companies Experience After Implementing an RMM Solution



24%	Less than $50,000
39%	$50,000 to $99,999
27%	$100,000 to $499,999
6%	$500,000 to $999,999
1%	More than $1 million
3%	No cost savings

Benefits of Investment

Regardless of whether you work in internal IT or you're an MSP, implementing a remote monitoring and management solution has immense benefits and enhances the efficacy and productivity of the IT department.

Benefits of RMM

Taking the average hourly rate and average salary of an IT technician, the results are indisputable! For an IT technician making $20 to $100 per hour, and assuming 48 weeks worked per year:

2 hours per day saved equals 20 days saved per year. For just this reallocation of 2 hours per day, companies benefit between **$9,600 and $48,000** in annual savings per technician.

With 6-10 on-site visits per week, each lasting 1-2 hours, by deploying an RMM solution, companies have been able to decrease onsite visits by 26-50%, or 3 to 20 days saved per year, equaling **$1,500 to $48,000** in annual savings per technician.

With 11-20 IT support calls per week, each lasting 11-29 minutes, by implementing RMM, technicians are able to resolve issues quicker and shorten each call by 6 -10 minutes, saving 2 to 6 days per year, or **$1,056 to $16,000** in annual savings per technician.

All in, most companies are saving between $50,000 to $99,999 annually, improving security, protecting their employees/customers, and enhancing productivity by enabling their IT teams to deploy a remote monitoring and management solution.

What Can You Do

1 | Invest in both IT and employee training

Cyberthreats are evolving, and the number of attacks is rising year over year. The best form of defense is a good offense, so ensure your IT team is prepared to mitigate risks and your employees know how to protect company data. Take this a step further, and make sure everyone at your company is trained on how to handle a malicious attempt and the protocols are always followed.

2 | Implement the right RMM solution for your company

The positive impact of implementing a remote monitoring and management solution is tough to dispute. IT teams improve their productivity levels, and companies benefit from overall time and cost savings. However, there are a lot of solutions out there, so doing your due diligence in evaluating is crucial. Look for solutions that are intuitive and allow you to have your team running within hours, not weeks. Also look for solutions that offer a single pane of glass view and allow you to consolidate vendors by offering patch management, anti-virus, alerting, reporting, automated task management and remote access within one tool.

3 | Prepare for the worst

With more than half of small and medium-sized businesses experiencing a cyberattack, if you're not preparing for the worst, you're preparing to fail. Preparing for the worst means your company not only has the proper training in place, but also the proper protocols to deal with any and all instances, so if something happens, you, your team and your employees know what to do. A swift and proactive response will ideally minimize negative impact of any attack attempt.

SECURE, RELIABLE, INTUITIVE REMOTE MONITORING AND MANAGEMENT

Part of the LogMeIn Inc. Identity & Access Management portfolio, LogMeIn Central is a pure, cloud-based remote monitoring and management solution enabling IT professionals to effectively monitor, manage and secure their endpoint infrastructure. Whether you have remote employees or endpoints scattered across the globe, LogMeIn Central provides IT organizations with the speed, flexibility and insight needed to increase productivity, reduce IT costs and mitigate risk. Rated the #1 remote access tool for small businesses to manage multiple computers, LogMeIn Central equips every endpoint in your network with premium remote access so you can troubleshoot anytime, anywhere.

www.logmein.com/central

09.03.2019/LMI0842