UNCOVERING THE HARSH REALITIES OF ENDPOINT MANAGEMENT

Bridging the gaps in multi-device security

Central by LogMeIn

TABLE OF CONTENTS

INTRODUCTION

One of the largest security trends that has grown in prominence throughout 2018 is endpoint management. Endpoint management tools simplify the IT management process by allowing a company to centrally manage, update and troubleshoot all its devices including desktops, laptops, routers, mobile phones, and more.

To better understand the current market trends, business threats, and how companies currently try to mitigate those threats, we conducted a research study among 1,000 IT professionals. These IT professionals represented both small and mid-size companies throughout North America and Europe.

The results of our research reveal that the clear majority of IT professionals consider endpoint management a priority for their teams, driven by the proliferation of a wide variety of endpoints in their organization. These professionals are aware of the very public and very costly security breaches this past year (Equifax, WannaCry, the US government NSA hacking to name a few) caused by unpatched systems and understand that failing to prepare for these risks can have a significant impact on the company's bottom line and reputation.

However, addressing and countering cyber threats is not the only reason why the IT community is making adoption of endpoint management a priority. Workplace trends are also demanding it:

1. BYOD (bring your own device) and remote workforce policies, including laptops and mobile devices, are increasingly becoming more commonplace across small and large companies, and adoption rates are not likely to slow down in the coming year.
2. Along with the plethora of devices also comes the multitude of apps and disparate software on those devices that need to be centrally managed and secured of any potential risks.
3. Organizations continue to move their business processes to the cloud, which puts sensitive data at risk of being accessed, viewed or mishandled.

Evolving workplace trends may be more convenient for the end user but carry with them increased risks of security breaches. Add to that the daily cyber threats companies face, and it is evident why IT professionals around the world are looking for holistic, comprehensive methods to centrally manage all endpoints.

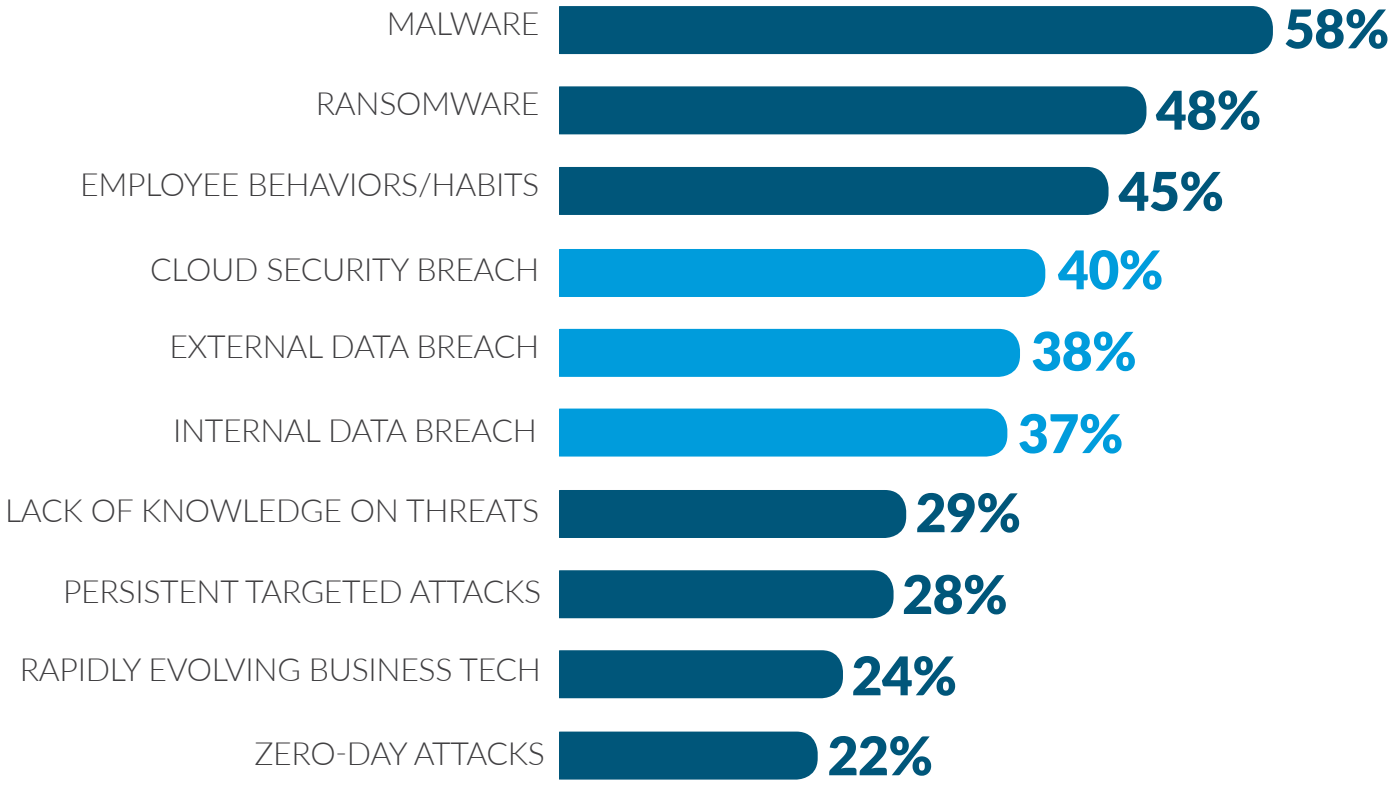
IT professionals consider endpoint management a priority and evolving workplace trends demand it, but **ONLY HALF ARE PROACTIVELY ADDRESSING SECURITY CONCERNS** before a breach occurs

MARKET TRENDS:
SECURITY THREATS ARE REAL AND INCREASINGLY PERVASIVE

IT professionals had several security concerns going into 2018, and they were well justified in their worries: According to McAfee, ransomware grew 56%[5] and was found in 39% of malware-related cases in 2017[5]. In fact, ransomware is no longer targeting just desktops, but also other endpoints like servers and networks.[5]

Our study indicates that IT professionals have their work cut out for them: On average, they are facing at least 4 security concerns, from both internal and external sources. Malware rises to the top of their security concerns, followed by ransomware and employee behaviors/habits. These are quickly followed by the trifecta of breaches — cloud security breaches, external data breaches and internal data breaches. These are real concerns and only add to the need to have comprehensive endpoint management in place across your organization. Being able to quarantine these IT security threats is the first step in ensuring your entire network does not become compromised.

IT TEAMS ARE FACED WITH MULTIPLE SECURITY RISKS, WITH MALWARE AND RANSOMWARE ON TOP OF THEIR LIST OF CONCERNS



BUSINESS TRENDS:
AS WORKPLACE TRENDS CHANGE, SO SHOULD OUR APPROACH TO SECURITY

BYOD RESULTS IN PROLIFERATION OF ENDPOINTS. AS A CONSEQUENCE, IT TEAMS HAVE TO EVOLVE THE WAY THEY TACKLE SECURITY, OR RISK BEING OPEN TO POTENTIAL CYBER THREATS

Not long ago, IT professionals had a finite number of endpoints to manage and secure - and these endpoints were under their direct control. They could protect their company from cyber threats and risks by securing the perimeter and their known on-premise systems. However, in the past several years, BYOD and the remote workforce are changing the way people work, causing IT teams to rethink how they manage and secure endpoints and their company's network.

As companies look to provide more flexibility to their employees, and also benefit financially from higher productivity and lower costs, BYOD and remote workforce policies will continue to take root. In fact, a survey of BYOD trends by MarketsandMarkets found that North American adoption rates were at 36% at the start of 2017, and were projected to increase to nearly 50% throughout 2018[1].

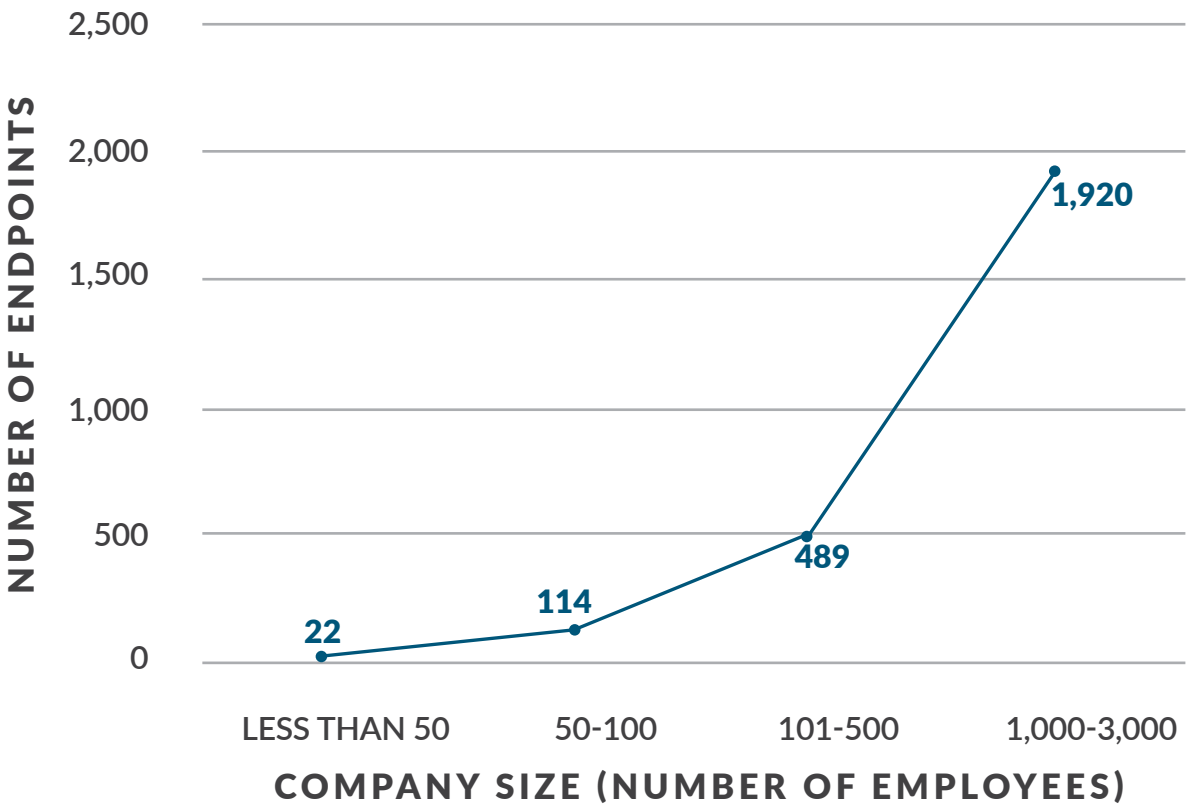
Our research shows that despite concerns about endpoint threats, 30% of IT professionals do not have a firm grasp of how many endpoint devices their company even has.

HOW MANY REMOTE ENDPOINTS DOES YOUR COMPANY HAVE IN TOTAL?

For these companies, finding a way to adapt to the growing BYOD trend with a comprehensive solution that securely manages a wide range of devices will be crucial in effectively preventing cyber-attacks.

Of those IT professionals that could estimate how many endpoints their company has, they report an average of 750 endpoints (servers, employee computers, mobile devices). This substantial number of endpoints adds an extra layer of complexity to the struggle of effectively managing them and simultaneously keeping companies safe from any internal and external security threats.

AVERAGE NUMBER OF ENDPOINTS BY COMPANY SIZE



PROBLEMS WITH CURRENT APPROACH: ORGANIZATIONS NEED TO BE PREPARED TO WIN THE WAR, NOT JUST A BATTLE

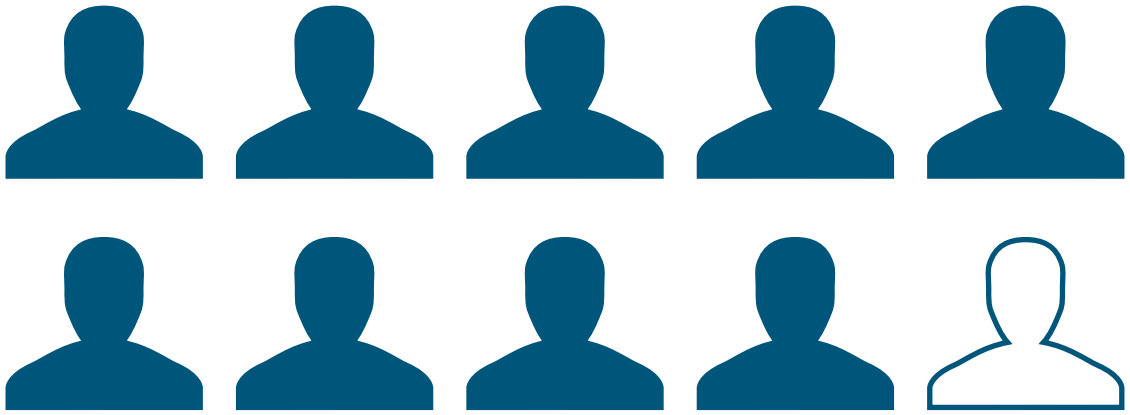
With the plethora of endpoints as well as internal and external security concerns, it is no surprise that nearly 9 out of 10 (88%) IT professionals consider endpoint management a priority for their teams.

In fact, anti-malware on end-points is the second most common security measure IT professionals implement to address security concerns.

Other common security measures used to combat security concerns include firewalls, user authentication and encryption.

As a result of these security measures, most IT professionals (82%) feel prepared to deal with security concerns, but only 26% feel very confident that these security measures are effective for their end users.

ENDPOINT MANAGEMENT IS ALREADY A PRIORITY BUT MORE SHOULD BE DONE TO KEEP YOUR ORGANIZATION SAFE FOR THE LONG TERM.



NEARLY

9 out of 10

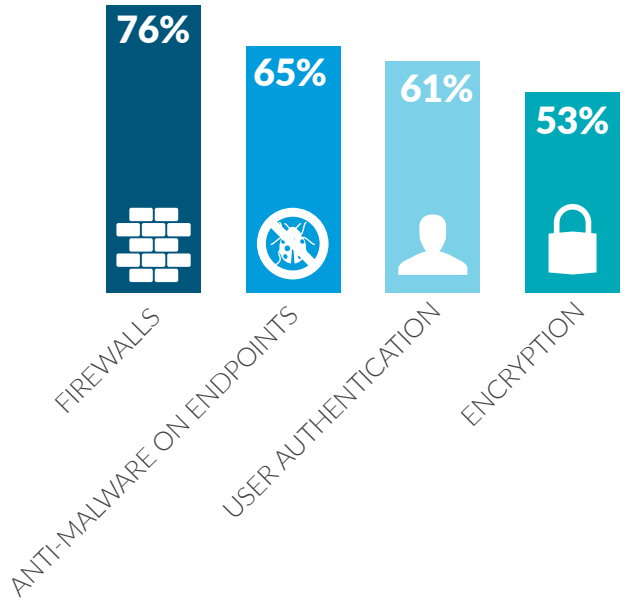
IT professionals consider endpoint management a priority

THIS DATA PROVES THERE'S SO MUCH PROGRESS TO BE MADE WHEN IT COMES TO ADDRESSING ENDPOINT SECURITY LONG TERM IN A HOLISTIC AND COMPREHENSIVE WAY:

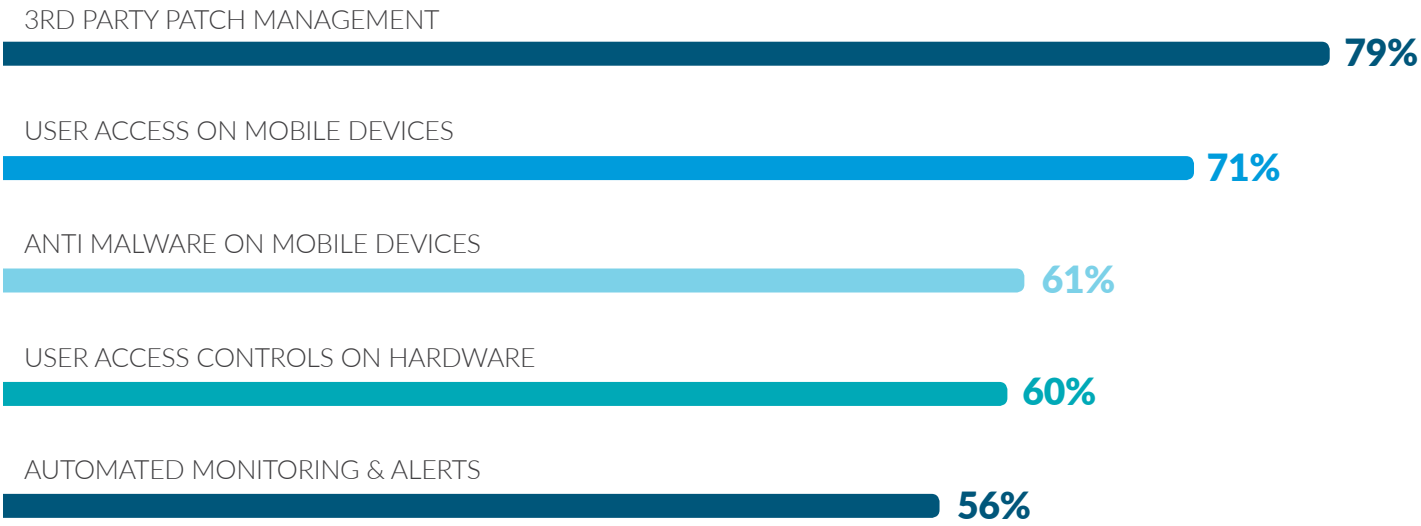
1. Though 71% of IT professionals claim they are actively addressing security on hardware, only 56% are actively addressing security on software, and only 48% are actively addressing security on mobile devices. This lack of coverage leaves significant holes in their security strategy. As an increasing number of employees are using their personal smartphones or tablets for work purposes (download work documents, edit, send emails etc.), ensuring that these devices are as secure as PCs and other endpoints is becoming increasingly important.

2. Additionally, many important security measures are currently not being used by a large percentage of IT teams, such as 3rd party patch management and user access controls on mobile devices, leaving their companies open to cyber-attacks.

MEASURES SET UP TO ADDRESS SECURITY CONCERNS



PERCENT OF IT PROFESSIONALS NOT USING THE FOLLOWING MEASURES



QUANTITATIVE IMPACT:
BY FAILING TO PREPARE, YOU ARE PREPARING TO FAIL

Despite all the recent news highlighting hacks and concerns around security, only just over half of IT professionals (52%) spend any time proactively addressing security concerns before an attack or breach occurs.

The risks that these security threats present to the companies are not just operational, but can also have a real impact on their bottom line, a long-term strain on the company reputation and even cause a company shutdown.

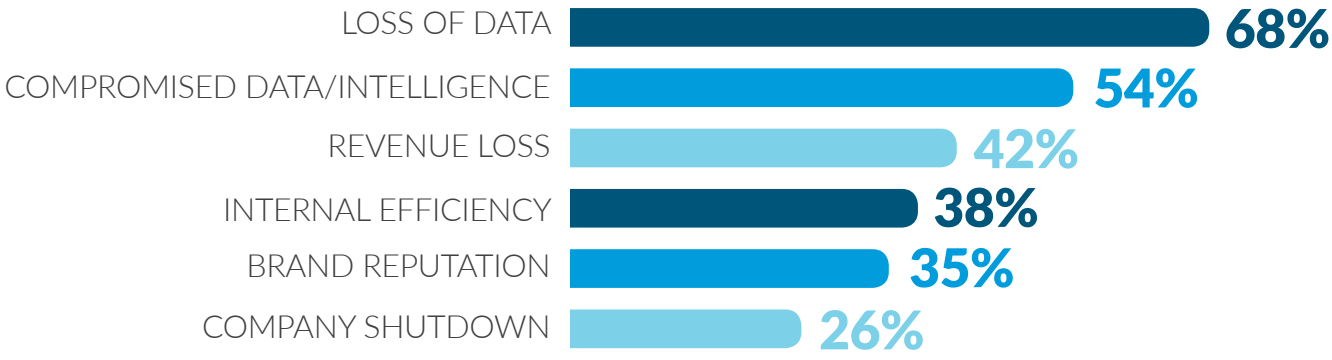
THE NUMBERS ARE STAGGERING

According to some estimates, WannaCry alone caused total damages world wide ranging from hundreds of millions to billions of dollars. The ExPetr ransomware attack, caused FedEx/TNT around $300 million in lost earnings[5].

In addition, according to a global survey conducted by Osterman Research on behalf of Malwarebytes, about 16% of organizations impacted by a ransomware attack experienced at least 25 hours of downtime, with some organizations reporting that it caused systems to be down for more than 100 hours!

Our study shows that among IT professionals, the highest perceived risks stemming from a security breach are loss of data, compromised data and revenue loss.

RISKS FROM SECURITY CONCERNS



BENEFITS OF INVESTMENT:
AS RISKS EVOLVE, SO SHOULD INVESTMENT

IT SECURITY NEEDS TO MOVE BEYOND CONVENTIONAL METHODS OF PROTECTION TO COVER EMERGING SECURITY THREATS IN A COMPREHENSIVE WAY

Our study indicates that currently anti-malware on endpoints is one of the top 3 security priorities that use most of the IT security budget. Firewalls and IT training round up the top 3 security priorities that receive the most budget.

However, other security areas that can help prevent threats, such as automated monitoring and alerts (26%), anti-malware on mobile devices (17%) and third-party patch management (14%), do not receive as much investment.

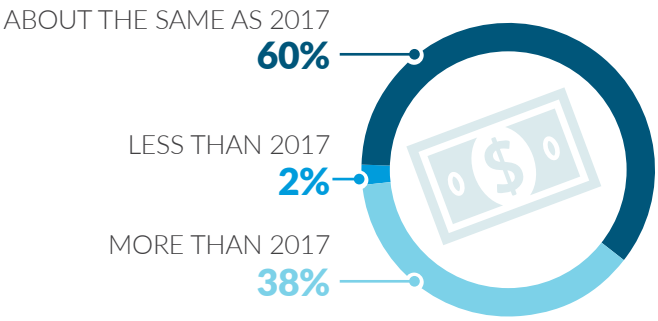
In fact, IT professionals indicate that the areas where they will invest the least money are:

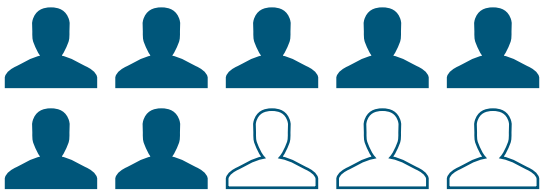
3rd party patch management and user access to mobile devices and hardware.

These measures that receive little investment however, have big benefits if implemented:

- Save time, money and improve productivity by monitoring threats and discerning real threats from false threats
- Improve security by focusing on real security incidents
- Guarantee compliance with best security practices
- Ensure your company's security is up to date with any new features and functions
- Ensure employees' mobile devices do not become a gateway to your company's private data and information

2018 IT BUDGET VS. 2017 IT BUDGET





The **large majority (70%) of IT professionals** dedicate **less than 25%** of their budget to IT security

WHAT CAN YOU DO

As cybersecurity attacks are becoming more prevalent and more sophisticated, and evolving workplace trends result in the proliferation of endpoints, IT teams are preparing by setting up several security measures and making endpoint management a top priority for their teams. However, more things should be done to avoid becoming a victim of cyber-attacks:

BE PROACTIVE

Do not wait until an attack or breach occurs to address security. Preventive security measures like automated monitoring and alerts and updated patches can help shield your organization from many attacks.

PATCH YOUR SYSTEMS

Patch Management is an essential part of securing your IT infrastructure. Whether you set aside a day of the week dedicated to deploying patches to your systems or set up proactive alerts to let you know when they are needed, staying on top of patch management is critical.

IMPLEMENT A MORE HOLISTIC APPROACH TO SECURITY

Attacks do not just focus on PC's anymore. Mobile devices, servers and other endpoints are increasingly vulnerable to cyber-attacks.

EDUCATE YOUR WORKFORCE

Setting up and supporting proper employee behavior and habits when it comes to data security and cybersecurity is a crucial element of a secure IT infrastructure.

Sources

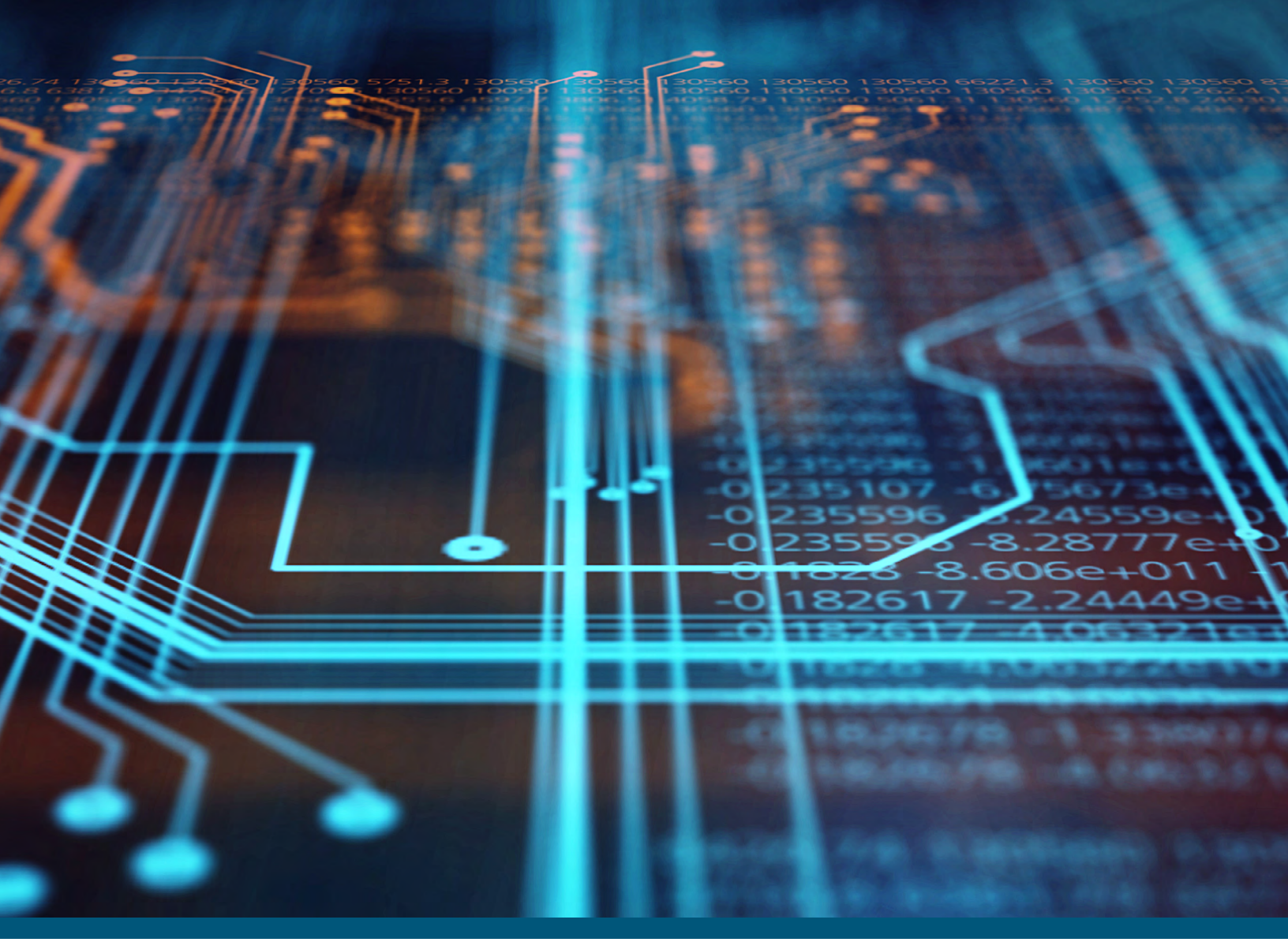
[1] Mobile Business Insights: The latest BYOD trends and predictions, from mobile focus to endpoint management By Jonathan Crowl - August 14, 2017

[2] Entrepreneur: Business Cyber Attacks Top 4,000 Per Day: Your Guide to Ransomware By Jorge Rey November 30, 2016

[3] ZDNet.com Infographic: 2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud By Amy Talbott | October 2, 2017

[4] 2016-2017 Ransomware statistics and facts Published by Sam Cook on January 17, 2018 in Antivirus

[5] 2018 Data breach Verizon report Maria Korolov Contributing Writer, CSO | APR 10, 2018 3:00 AM PT



Central by LogMeIn

SIMPLE, SECURE IT AUTOMATION AND ENDPOINT MANAGEMENT

Part of the LogMeIn Inc. Identity & Access Management portfolio, LogMeIn Central is a pure, cloud-based endpoint 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.

https://www.logmein.com/central