CYBERSECURITY TRENDS

ALERT LOGIC®

ALIEN VAULT

bitglass

DELTA RISK
A CHERTOFF GROUP COMPANY

ERPScan

GO ANYWHERE®

(ISC)²

LYNX TECHNOLOGY PARTNERS

Raytheon
Foreground Security

sqrrl

TOPSPIN SECURITY

Veriato

ZIMPERIUM.

OVERVIEW

The cybersecurity landscape is changing rapidly, making current and actionable guidance on the latest trends more important than ever.

This report has been produced by the 350,000 member Information Security Community on LinkedIn in partnership with Crowd Research Partners to explore the current cybersecurity trends, organizations' investment priorities, and solution choices for cloud security, threat management, data protection, application security, security training and certifications, managed security services, and more.

This report reveals the latest data points and trends in cybersecurity, shares how your peers are approaching security, and provides valuable benchmark data that will help gauge how your own organization stacks up compared with others.

Many thanks to our sponsors for supporting this exciting research project:

Alert Logic | AlienVault | Bitglass | Delta Risk | ERPScan | Linoma | (ISC)² | Lynx Technology Partners | Raytheon | Sqrrl | TopSpin | Veriato | Zimperium

Thank you,

Holger Schulze

Holger Schulze
Founder
Information Security
Community on LinkedIn

hhschulze@gmail.com

LinkedIn Group Partner
Information Security

CYBERSECURITY TRENDS REPORT

TABLE OF CONTENTS

KEY SURVEY FINDINGS

1. With 54% of cybersecurity professionals anticipating successful cyberattacks on their organization in the next 12 months, it is no surprise that 52% are boosting their security budget by an average of 21%. The focus areas where companies will increase security spend include cloud infrastructure (33%) and cloud applications (28%). Training/education (23%) and mobile devices (23%) tie for the third spot.

2. The three biggest obstacles to stronger cybersecurity are lack of skilled employees (45%), lack of budget (45%), and a lack of security awareness among employees (40%). To overcome these challenges and create a better security posture, 54% of organizations want to train and certify their current IT staff. Leveraging third-partner security solutions (47%), partnering with a managed service provider (41%), and hiring additional security staff (32%) are popular strategies companies use to address security issues.

3. To better manage cyber threats and reduce the risk of a security breach, companies prioritize three key capabilities including improved threat detection (62%) followed by better analytical capabilities (43%) and threat blocking (39%). Fifty-eight percent of organizations estimate they reduced the number of security breaches by at least 25% using better threat intelligence and monitoring solutions.

4. While cloud computing has become a mainstream delivery choice for applications, services and infrastructure, concerns about cloud security remain high. The top three cloud security concerns respondents need to address include protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (47%).

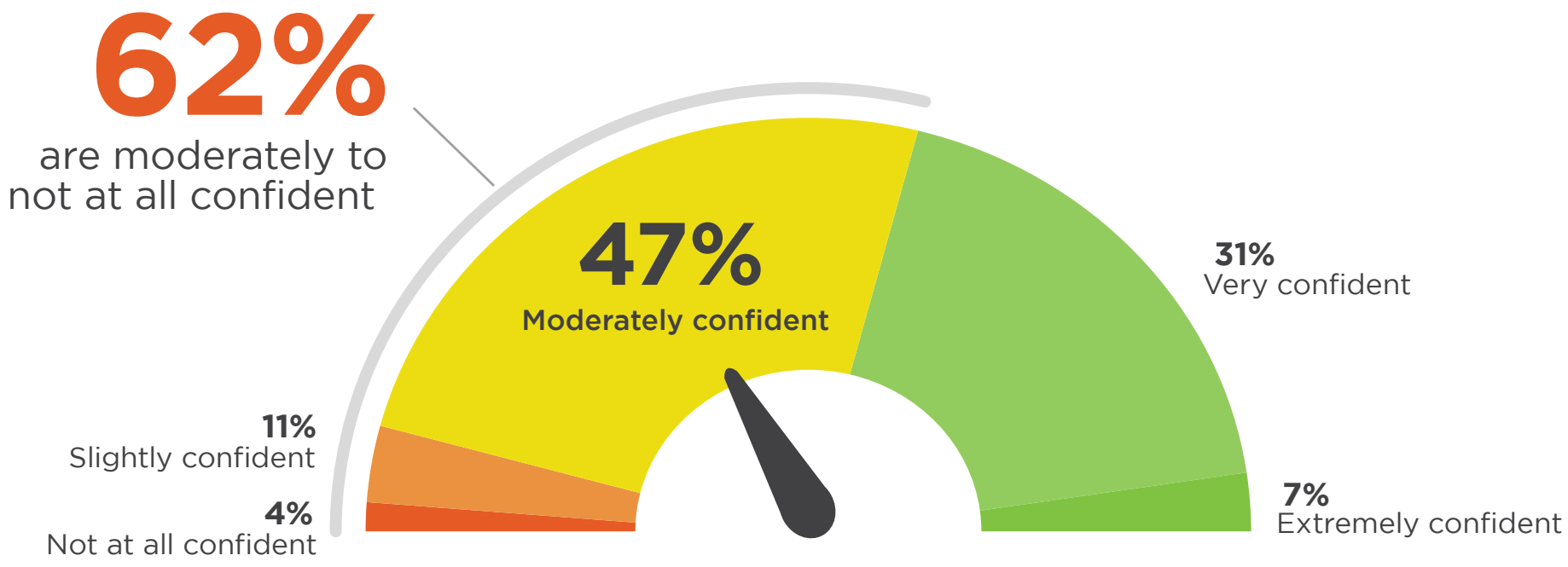
5. As mobility and BYOD initiatives grow in the workplace, so do security concerns. Of biggest concern related to BYOD is data leakage or loss (69%), download of unsafe applications or content (64%), and the introduction of malware into the organization's IT environment (63%).

GENERAL SECURITY TRENDS

CONFIDENCE IN SECURITY

Over half of cybersecurity professionals (62%) are moderately confident to not at all confident in their organization's overall security posture - presenting a significant opportunity for security staff and vendors to improve overall confidence in their organizations' security capabilities. Only 38% of respondents expressed a high degree of confidence in their organization's security posture. Forty-seven percent are moderately confident and 15% are only slightly or not at all confident - presenting a significant opportunity for security staff and vendors to improve overall confidence in their organizations' security posture.

Q: How confident are you in your organization's overall security posture?



SECURITY STRENGTH

Today's distributed, multi-tier IT environments can be quite complex and challenging to secure. Organizations have the highest confidence in the security strength of their data centers (73%), network perimeter (70%), and end-points (60%). In contrast, respondents have the lowest confidence in social media and mobile security.

Q: How would you rate your organization's overall security strength (ability to resist cyber threats) in each of the following areas?

Datacenter
(physical & virtual servers)

73%

Network perimeter/DMZ
(web servers)

70%

Endpoints
(Desktops PCs & Laptops/notebooks)

60%

Business Applications (ERP,HR,CRM,SCM, BI) 55% | Cloud infrastructure (IaaS, PaaS) 53% | Cloud Applications (SaaS) 53% | Web Applications (custom built) 50% | Mobile devices (smartphones, tablets) 39% | Social media Applications (Facebook, Twitter) 37%

CYBERATTACK INCIDENTS

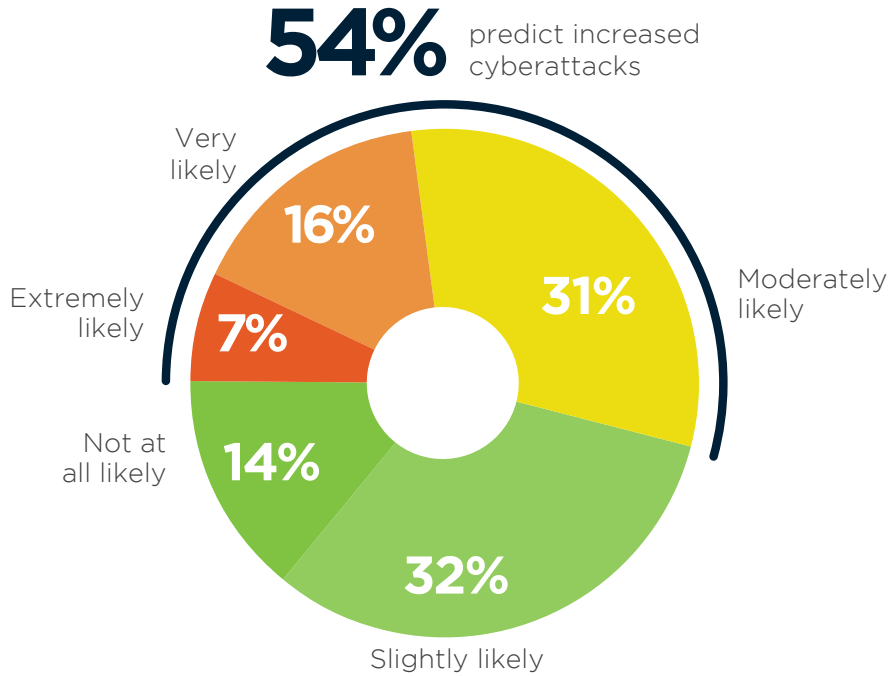
Cybersecurity professionals observed a wide range of cybersecurity incidents over the past 12 months, ranging from zero to hundreds of attacks per organization. On average, cyber experts became aware of 8 cyberattacks in their company in the previous 12 months.

Q: How many times do you estimate that your organization has been compromised by a successful cyberattack within the past 12 months?

8 Cyber Attacks
within the last 12 months

Looking ahead, we asked cybersecurity professionals about their expectations regarding future cyberattacks impacting their organization. Almost a quarter of professionals (23%) assess the probability of future attacks as very or extremely likely. Thirty-one percent say a successful attack is moderately likely. Surprisingly, 46% are confident that their organization is only slightly or not at all at risk of successful cyberattacks in the next 12 months.

Q: What is the likelihood that your organization will become compromised by a successful cyberattack in the next 12 months?



BIGGEST SECURITY THREATS

When it comes to specific threat vectors, cybersecurity professionals are most concerned about phishing attacks, malicious insiders, and malware.

Q: Please rate your overall concern for each of the following cyberthreats targeting your organization.

Phishing Attacks

CONCERN

37%

Malicious & Careless Insiders

CONCERN

33%

Malware

CONCERN

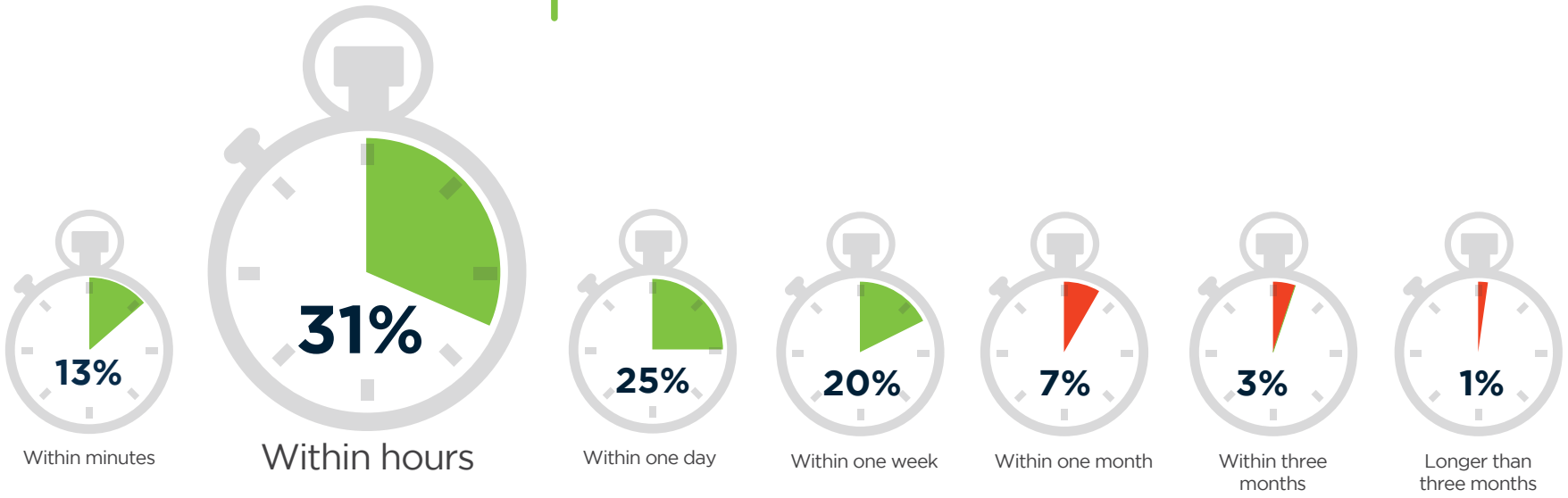
32%

ATTACK RECOVERY TIME

One of the biggest security challenges is the detection of sophisticated attacks. While the time it takes to detect an attack varies from company to company, on average it takes over 200 days to detect a breach. Once detected, 44% of cybersecurity professionals claim they typically recover from attacks within minutes or hours, 25% within one day, dependinig on the severity of the attack.

Q: How long did it take your organization to recover from a cyberattack (on average, once observed)?

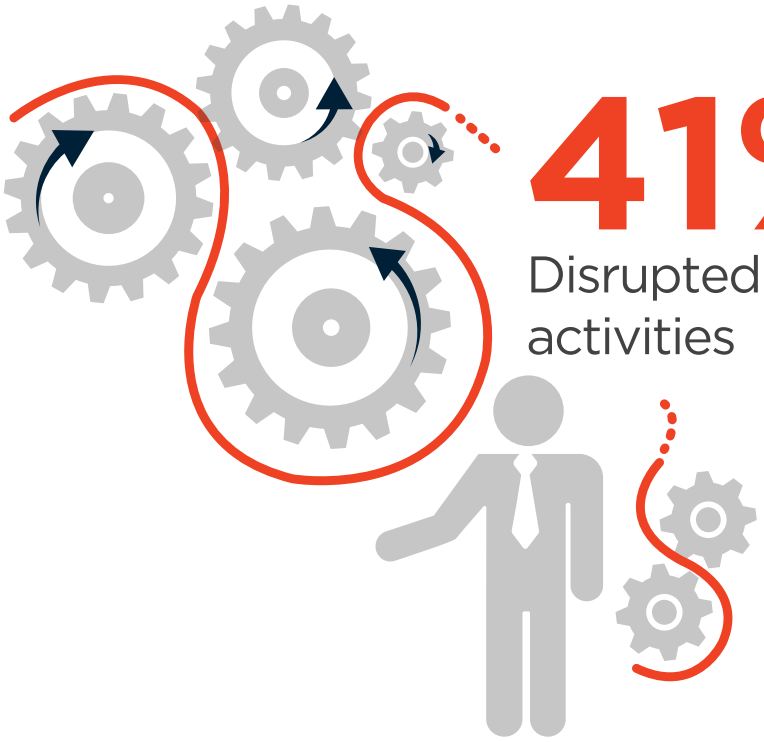
44% recover from attacks within minutes or hours.



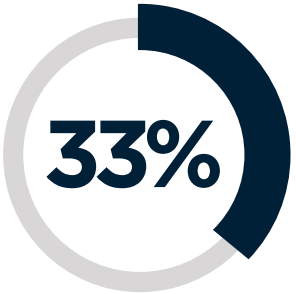
IMPACT OF SECURITY INCIDENTS

Among the organizations who experienced security incidents, the biggest negative impact comes from disrupted business activities (41%), followed by reduced employee productivity (33%) and the impact on IT staff having to triage and remediate the security incident (29%).

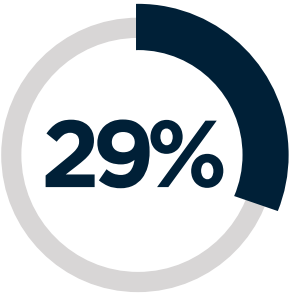
Q: What negative impact have security incidents had on your company in the past 12 months?



41%
Disrupted business activities



Reduced employee productivity



Deployment of IT resources to triage and remediate issue

Increased helpdesk time to repair damage 25% | Reduced revenue/lost business 9% | Corporate data loss or theft 8% | Loss/compromise of intellectual property 7% | Lawsuit/legal issues 4% | Regulatory fines 3%

OBSTACLES TO STRONGER CYBERSECURITY

The three biggest obstacles to stronger cybersecurity are all about skills and resources: lack of skilled employees (45%), followed by lack of budget (45%) and lack of security awareness among employees (40%).

Q: Which of the following barriers inhibit your organization from defending against cyberthreats?

#1
Lack of skilled personnel

45%

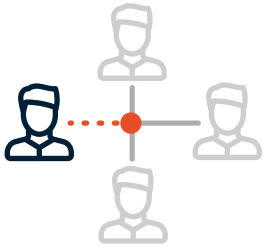
#2
Lack of budget

45%

#3
Low security awareness among employees

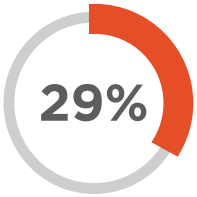
40%

#4
Lack of collaboration between departments

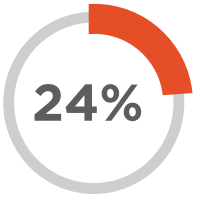


32%

Lack of management support/awareness



Poor integration/ interoperability between security solutions



Too much data to analyze

Lack of contextual information from security tools

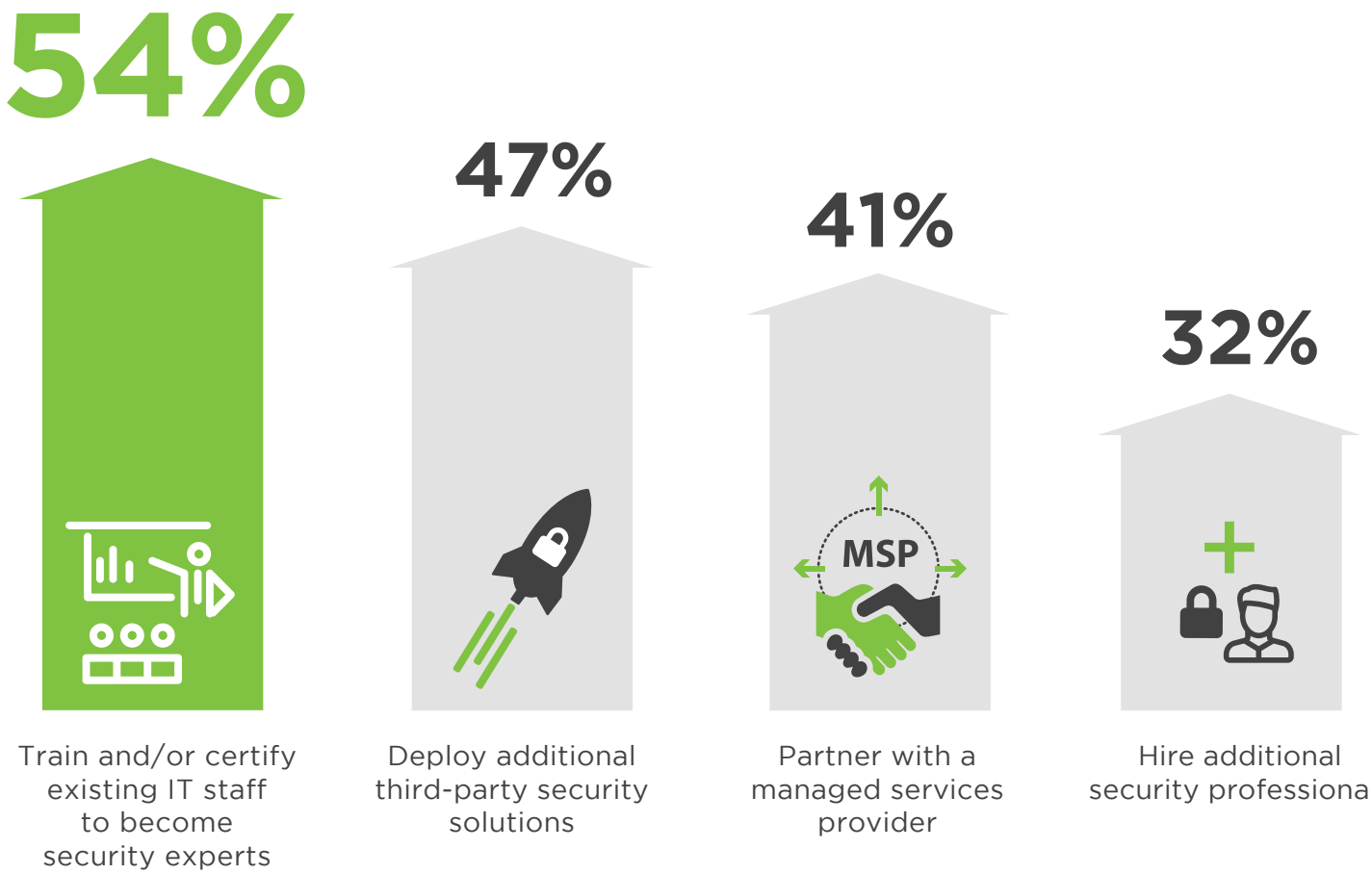
Inability to justify additional investment

Lack of effective solutions available in the market

INVESTMENT PRIORITIES

To address evolving security needs in the coming year, a majority of organizations plan to train and certify existing IT staff to become security experts (54%). Forty-seven percent plan to procure and deploy additional security technology solutions, and 41% plan to initiate or expand partnerships with managed services providers.

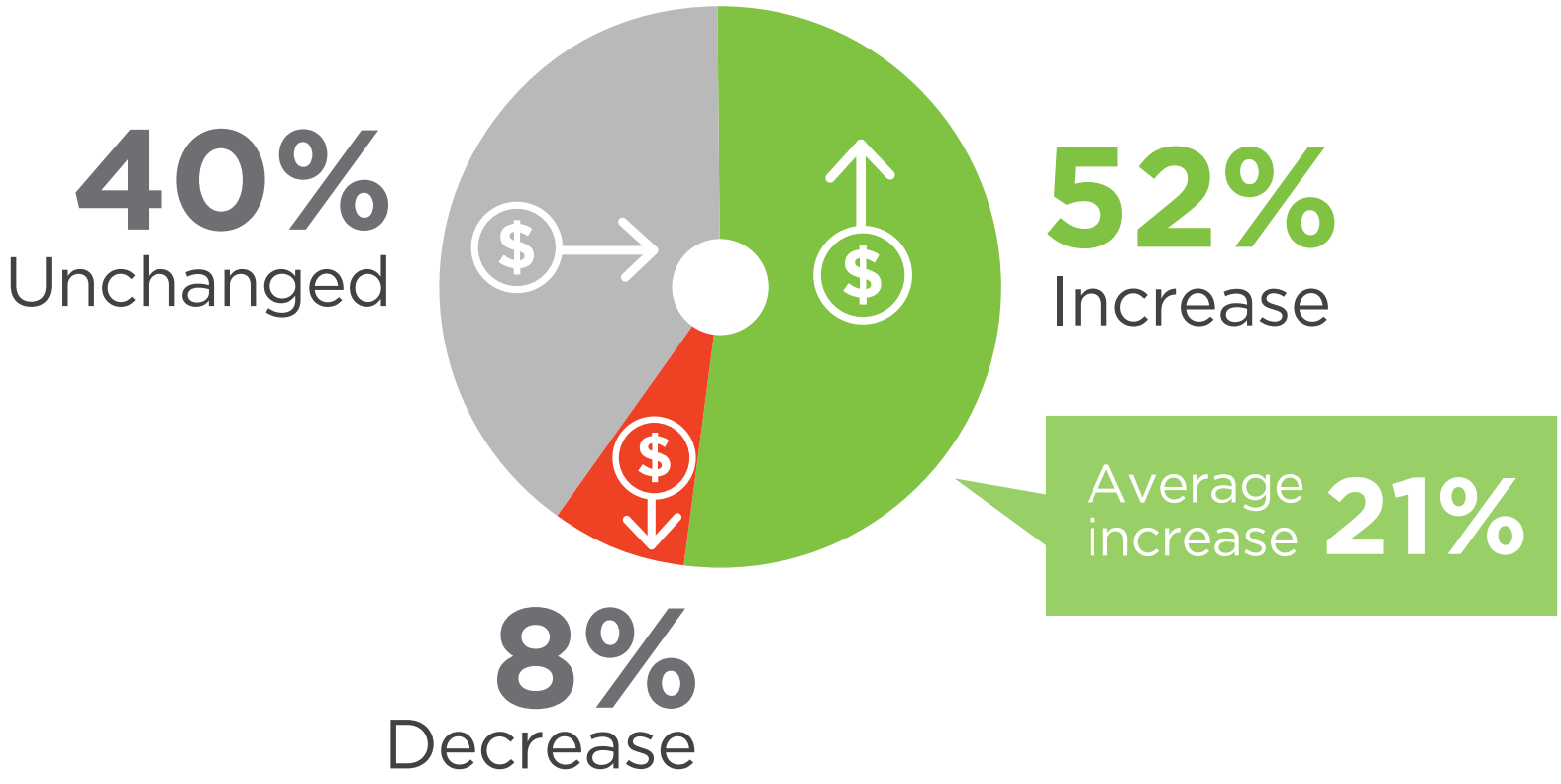
Q: How do you plan to handle your evolving security needs in the next 12 months?



SECURITY BUDGET TREND

There is no debate on the importance of having the right security solutions. More than half of organizations are boosting their security budget (52%). The average increase that companies are allocating for security is 21%.

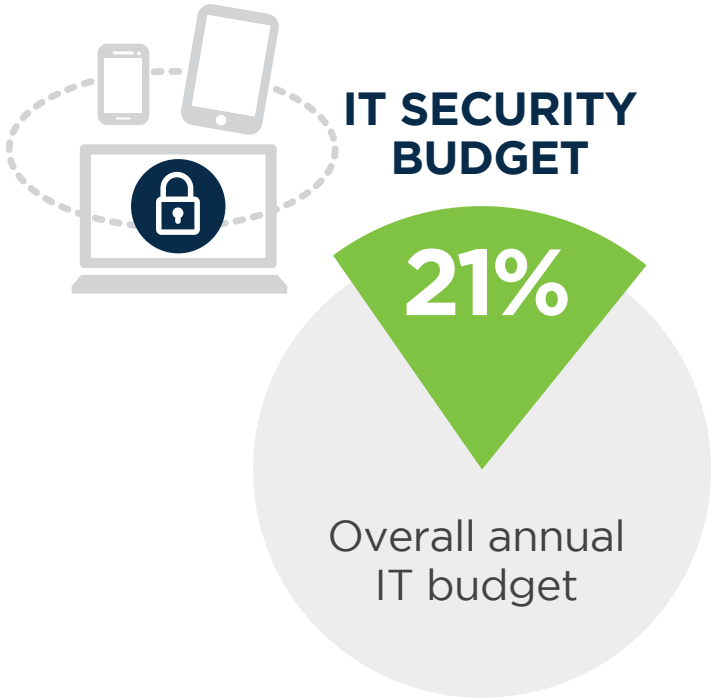
Q: How is your security budget changing in the next 12 months?



SECURITY BUDGET PRIORITIES

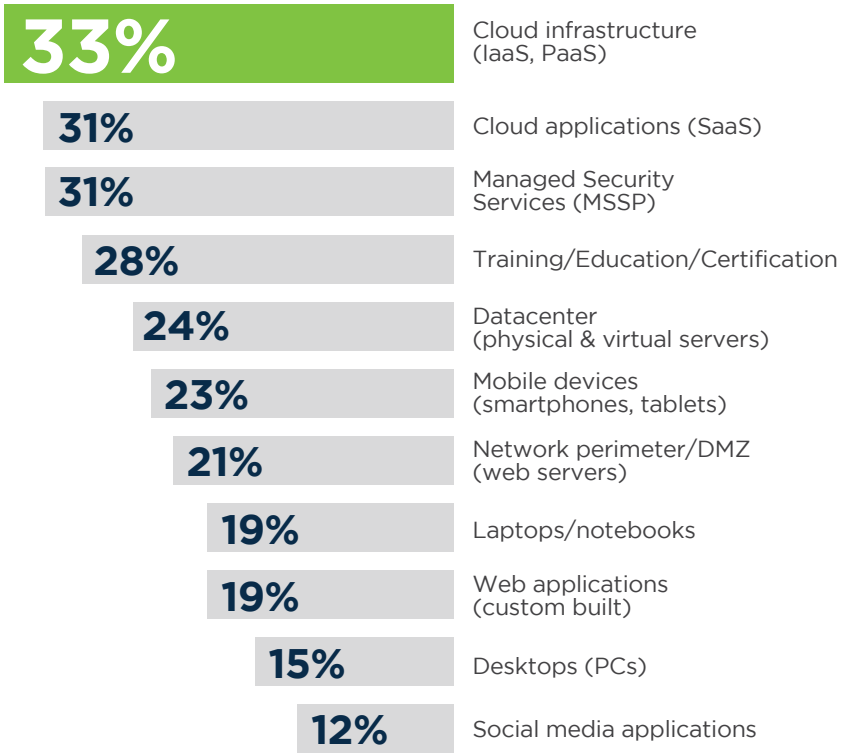
On average, security budgets are 21% of the overall IT budget (excluding headcount). While companies are continually tweaking their budgets, respondents will most likely allocate a higher share of their current security spending on cloud infrastructure, cloud applications, and managed security services.

Q: What IT areas will see an increase in security spend, over the next 12 months? (share of respondents who increase security for each IT tier)



Security is front and center for respondents. Organizations indicate they will boost future spending levels on a variety of priorities including, cloud infrastructure, cloud applications, managed security services, and training and education.

Q: What is your organization's security investment priority in each of the following areas over the next 12 months (increasing spend)?



THREAT MONITORING, INTELLIGENCE & MANAGEMENT

Cybersecurity is about preventing, detecting and remediating external and internal threats facing enterprises and government organizations, ranging from malware and phishing attacks to threats posed by trusted insiders.

A variety of tools have emerged to address these threats—from unified threat management platforms, better threat intelligence solutions for greater visibility across the IT environment, and automatic threat hunting, detection and remediation products to help with emerging and advanced threats.

TOP CHALLENGES FOR SOCS

The top two challenges facing SOCs are the detection of advanced threats (hidden, unknown, and emerging) and the lack of expert security staff to mitigate such threats. More than half of the SOCs face these two top challenges. All the challenges mentioned in the survey were ranked by at least 30% of the participants, suggesting that SOCs are dealing with a broad array of issues on a day-to-day basis.

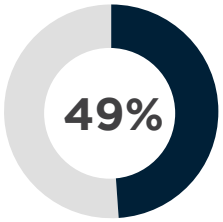
Q: Which of the following do you consider to be top challenges facing your SOC?

70%

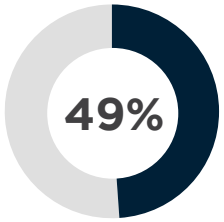
Detection of advanced threats (hidden, unknown, and emerging)

59%

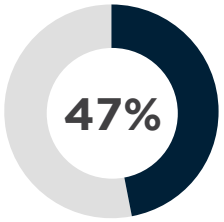
The lack of expert security staff to assist with threat mitigation



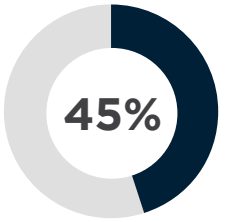
Detection of rogue insiders/ insider attacks



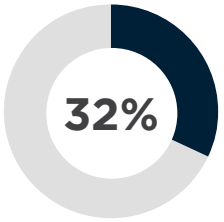
Slow response time to find or detect advanced threats



Too much time wasted on false positive alerts



Lack of confidence in automation tools catching all threats



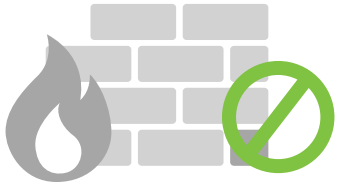
Lack of proper reporting tools

Working with outdated SIEM tools and SOC infrastructure 30% | Too much data to collect, aggregate, report and analyze 30% | Other 7%

DATA CAPTURED FOR FORENSIC REVIEW

When asked about the type of data their SOC log for forensics review, three in four respondents said they log and review firewall/IPS denied traffic. Other commonly collected logs are firewall/IPS allowed traffic, DNS traffic, and Web and email traffic. The importance respondents see in keeping different types of logs for forensic review is evident by the fact that each data option was logged by at least 30% of the respondents.

Q: What kind(s) of data does your SOC log for forensic review later?

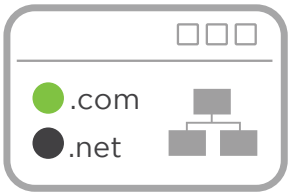


70%

Firewall/IPS denied traffic

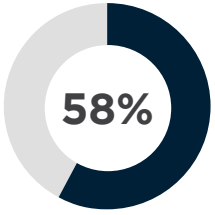
65%

Web and email filter traffic

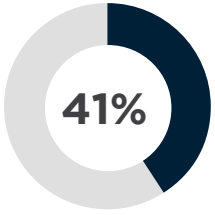


60%

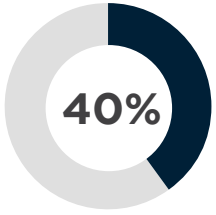
DNS traffic



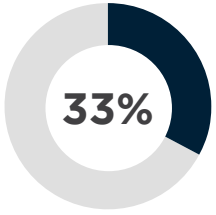
Firewall/IPS allowed traffic



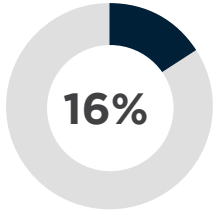
Server traffic



Packet sniff/ tcpdump



Windows domain logs



Unsure

ATTACK DISCOVERY

Attackers dwell on a network for an average of 40 days before they're discovered, according to the survey. Some respondents said attackers were discovered much faster while others said the attack could go undetected for as long as three months or even longer. Nearly all respondents agree that attackers dwell on a network for some period of time before they're discovered by the SOC.

Q: On average, how long do attackers who breach your security defenses dwell in your network before they are discovered by your SOC?

Average time attackers dwell on networks until discovered

An average of 40% of security threats to the respondent's SOC are missed, while an average of 60% were identified. With over 4 in 10 security threats being missed by SOCs, there's significant potential for a breach.

Q: Missed and Detected Security Threats?

40%
MISSED
Security Threats

60%
DETECTED
Security Threats

IT SYSTEMS MONITORING

Monitoring of sensitive systems and users for suspicious behavior is a key component of robust security frameworks. The most commonly monitored IT layer is the network (69%) followed by endpoints (PCs 66%/laptops 61%) and servers in the datacenter (62%).

Q: What IT systems do you routinely monitor for security risks?

Network perimeter/DMZ
(web servers)

69%

Desktops
(PCs)

66%

Datacenter
(physical & virtual servers)

62%

Laptops/ notebooks

61%

Web applications (custom built) 39% | Mobile devices (smartphone, tablets) 36% | Business applications (ERP, CRM, BI, HR, SCM) 31% | User behavior 30% | Cloud applications (SasS) 24% | Cloud infrastructure (IaaS, PaaS) 24% | Social media applications (Facebook, Twitter) 18%

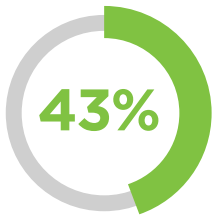
MOST CRITICAL CAPABILITIES

What threat management capabilities are most important to organizations? Threat detection (62%) tops the list, followed by analytical capabilities (43%) and blocking threats (39%).

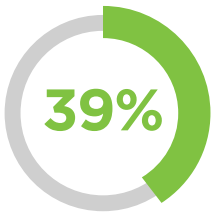
Q: What are the most critical threat management capabilities for your organization?

62%

Improve threat detection

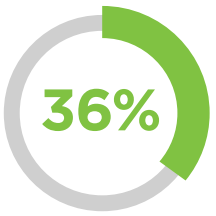


Improve investigating and analyzing threats

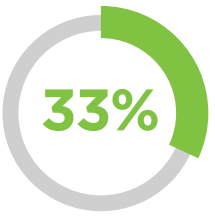


Improve blocking threats

Automate incident response



Proactive threat hunting



Aggregate security alerts

Reduce unwanted/unauthorized traffic 31% | Improve enforcement of usage policies 31% | Not sure/other 17%

BARRIERS TO THREAT MANAGEMENT

In keeping with overall barriers to a more effective security posture, lack of skilled employees also tops the list of barriers to better threat management (33%).

Q: What is the most critical barrier holding your organization back from implementing threat management more effectively?

33%

Lack of trained staff/skills

22%

Lack of management buy-in

12%

Difficulty in implementing new security systems/tools

10%

Too many feeds/inability to prioritize the intelligence being received

9%

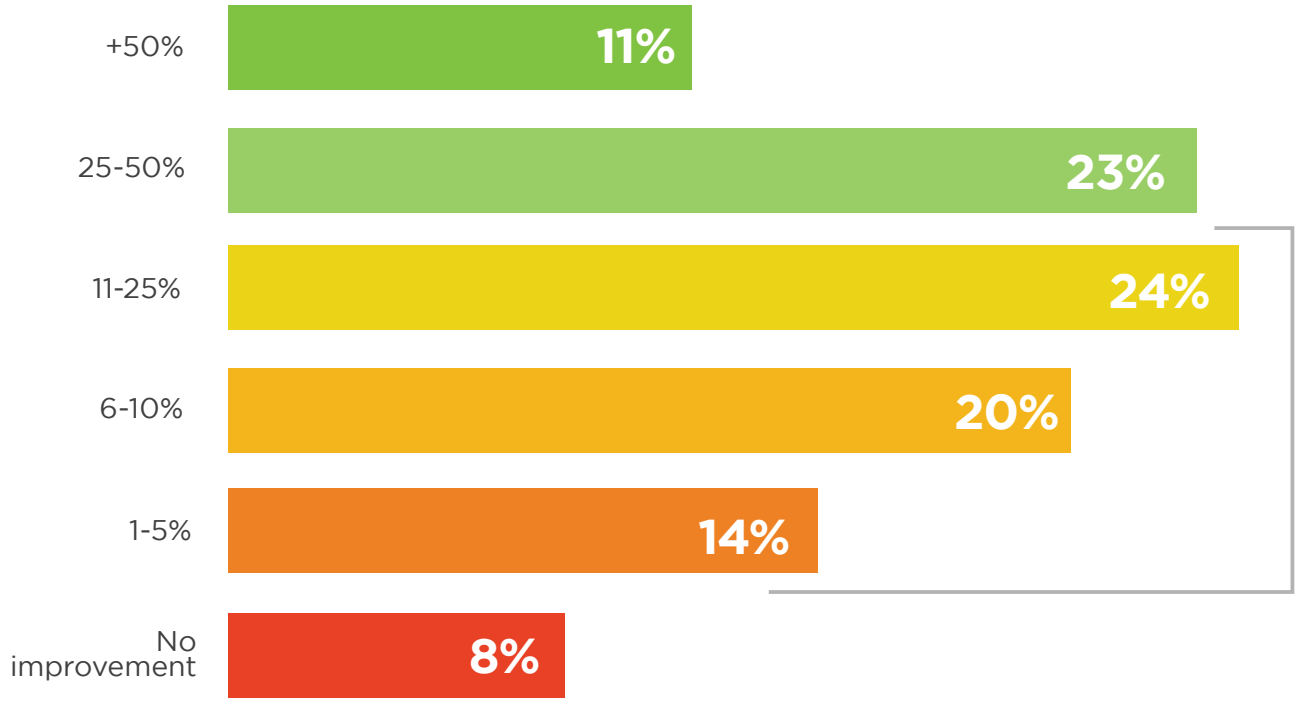
Lack of context/feeds don't provide the information that is needed

Lack of visibility into network traffic and other processes 8% | Lack of confidence in using the information to make decisions 6%

THREAT INTELLIGENCE SOLUTIONS

A majority of organizations (58%) estimate they reduced the number of security breaches by up to 25% by using threat intelligence solutions. Thirty-four percent reduced breaches by more than 25%. Eight percent of organizations saw no improvement.

Q: By what percentage have security breaches been reduced because of using threat intelligence solutions?



58%
reduced security breaches by **at least 25%.**

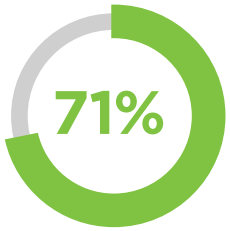
CRITICAL SOC CAPABILITIES

A Security Operations Center (SOC) is defined as an organized and highly skilled team whose mission is to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cyber security incidents with the aid of both technology and well-defined processes and procedures.

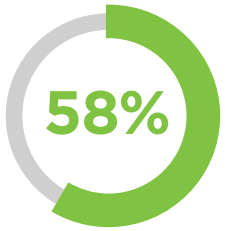
Seventy-six percent of survey respondents agree that the most valuable SOC capabilities center around rapid identification and remediation of attacks.

Q: How valuable are the following capabilities in a SOC?

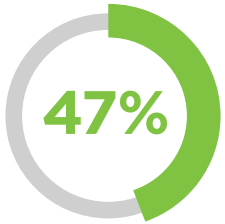
76% Rapid indentification and remediation of attacks



24x threat intelligence, monitoring and analysis



Threat assessment reports to identify vulnerabilities and risks



Security policy and controls management

Compliance-oriented activities

CLOUD SECURITY

IDC predicts worldwide revenues from public cloud services will reach more than $195 billion in 2020, and that in the same year spending on cloud services will nearly equal what is spent on traditional IT.[1]

However, there is one aspect of cloud that consistently worries IT and business professionals alike – how to achieve high levels of security. Our research reveals that the top three cloud security challenges include protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (36%).

Fifty-one percent of organizations cite visibility into cloud infrastructure as the biggest security management headache. Setting consistent security policies comes in second (38%) while compliance concerns are third biggest headache at 37%. It shouldn't be a surprise that the cloud security market is expected to grow at a CAGR of more than 15% and be worth US$8.7 billion by 2019.[2]

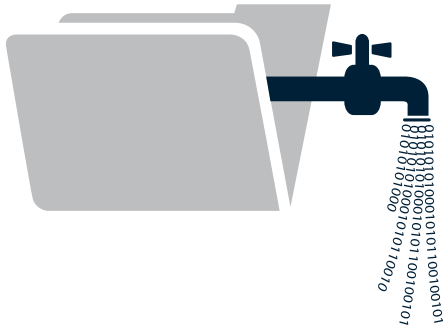
1 | http://www.informationweek.com/cloud/infrastructure-as-a-service/cloud-spending-will-top-$37-billion-in-2016-idc-reports/d/d-id/1326193.

2| Markets and Markets, 2015

CLOUD SECURITY CONCERNS

Cloud providers offer many security measures; however, organizations are ultimately responsible for securing their own data, applications, and services in the cloud. The top three cloud security challenges highlighted by cybersecurity professionals include protecting against data loss (57%), threats to data privacy (49%), and breaches of confidentiality (47%).

Q: What are your biggest cloud security concerns?



57%
Data loss/leakage

Data privacy

49%

Confidentiality

47%

Legal and regulatory compliance

36%

Data sovereignty/ control

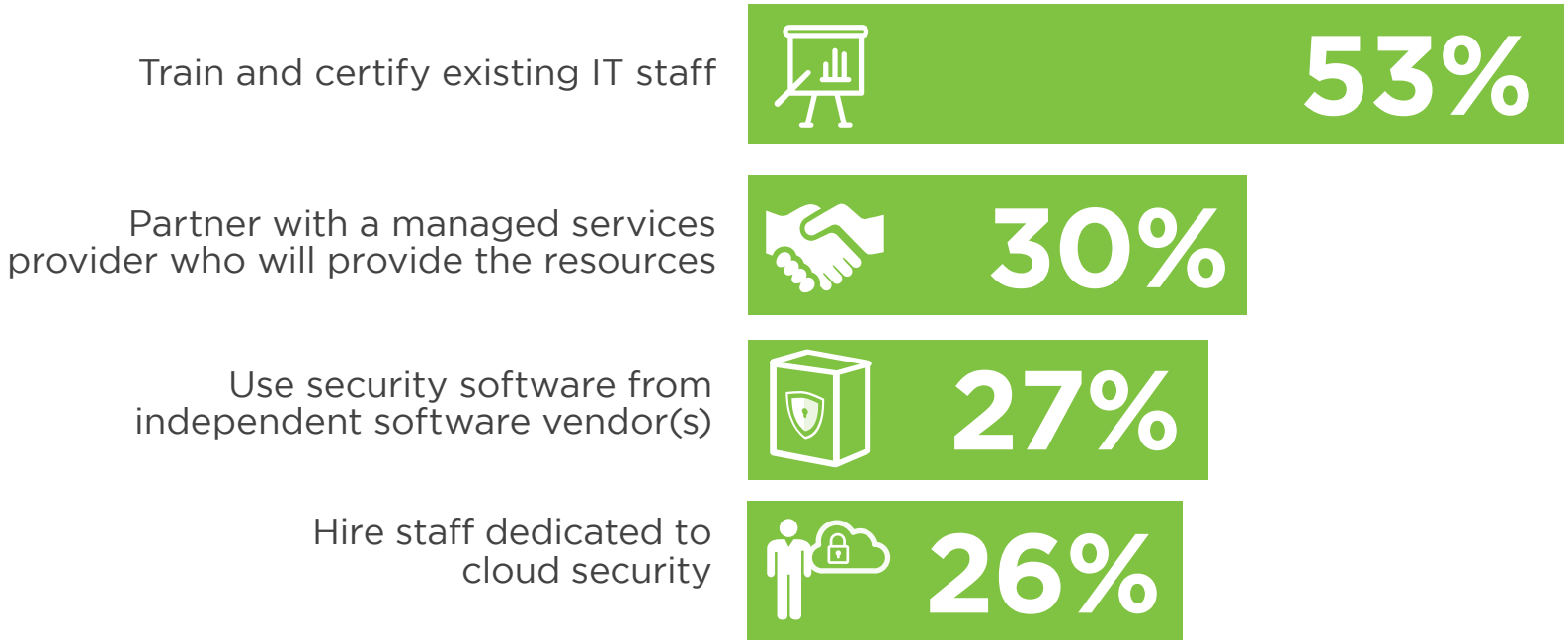
30%

Accidental exposure of credentials 25% | Compliance 24% | Visibility & transparency 22% | Lack of forensic data 20% | Liability 18% | Availability of services, systems and data 17% | Fraud (e.g., theft of SSN records) 17% | Incident & problem management 17% | Disaster recovery 13% | Business continuity 12% | Performance 12% | None 1%

CLOUD SECURITY FOCUS

Moving to the cloud brings new security challenges that require new types of skills. To address these evolving security needs, 53% of organizations want to train and certify their current IT staff - by far the most popular approach. This is followed by partnering with a managed service provider (30%), leveraging software solutions (27%) or hiring dedicated staff (26%).

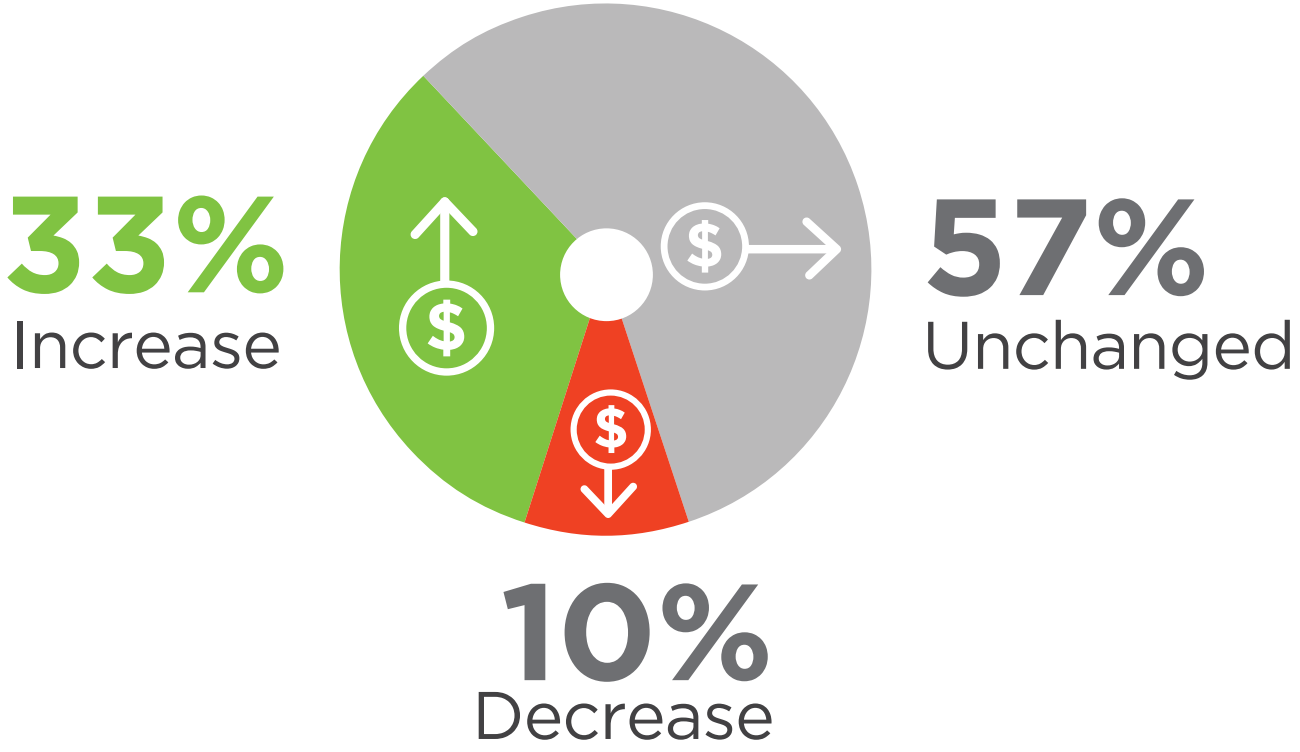
Q: When moving to the cloud, how do you plan to handle your security needs?



CLOUD SECURITY BUDGET

A third of organizations predict cloud security budgets to increase over the next 12 months. With 33%, cloud security is receiving the largest share of predicted budget increase across all IT security areas.

Q: What is your organization's budget outlook for cloud security?



CLOUD SECURITY MANAGEMENT CHALLENGES

Visibility into cloud infrastructure is the biggest security management headache for 37% of respondents, moving up to the top spot from being the second ranking concern in 2016. Compliance comes in second (36%) and setting consistent security policies as the third biggest headache at 33%.

Q: What are your biggest cloud security headaches?

37%

Visibility into infrastructure security

Compliance

36%

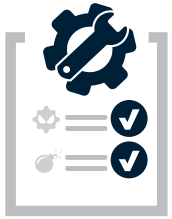
Setting consistent security policies

33%

Reporting security threats

29%

Remediating threats



28%

Lack of integration with on-prem security technologies 27% | Can't identify misconfiguration quickly 24% | No automatic discovery/visibility/control to infrastructure security 24% | Automatically enforcing of security across multiple datacenters 21% | Complex cloud to cloud/cloud to on-prem security rule matching 21% | Security can't keep up with pace of changes to new/existing applications 20% | Lack of feature parity with on-prem security solution 16% | None 7% | No flexibility 7% | Not sure/other 15%

MOST EFFECTIVE CLOUD SECURITY TECHNOLOGIES

Security policies are implemented through processes and technology. The survey reveals cybersecurity professionals prioritize encryption of both data at rest and data in motion as well as access controls as the most effective technologies for protecting sensitive data in the cloud.

Q: What security technologies and controls are the top 5 most effective methods to protect data in the cloud?

Data encryption

72%

41%

Data leakage prevention

Traffic encryption /VPN

60%

38%

Firewalls / NAC

Access control / user authorization

56%

38%

Endpoint security control

Network monitoring, reporting and forensics

53%

38%

Patch management

Intrusion prevention system (IPS)

44%

36%

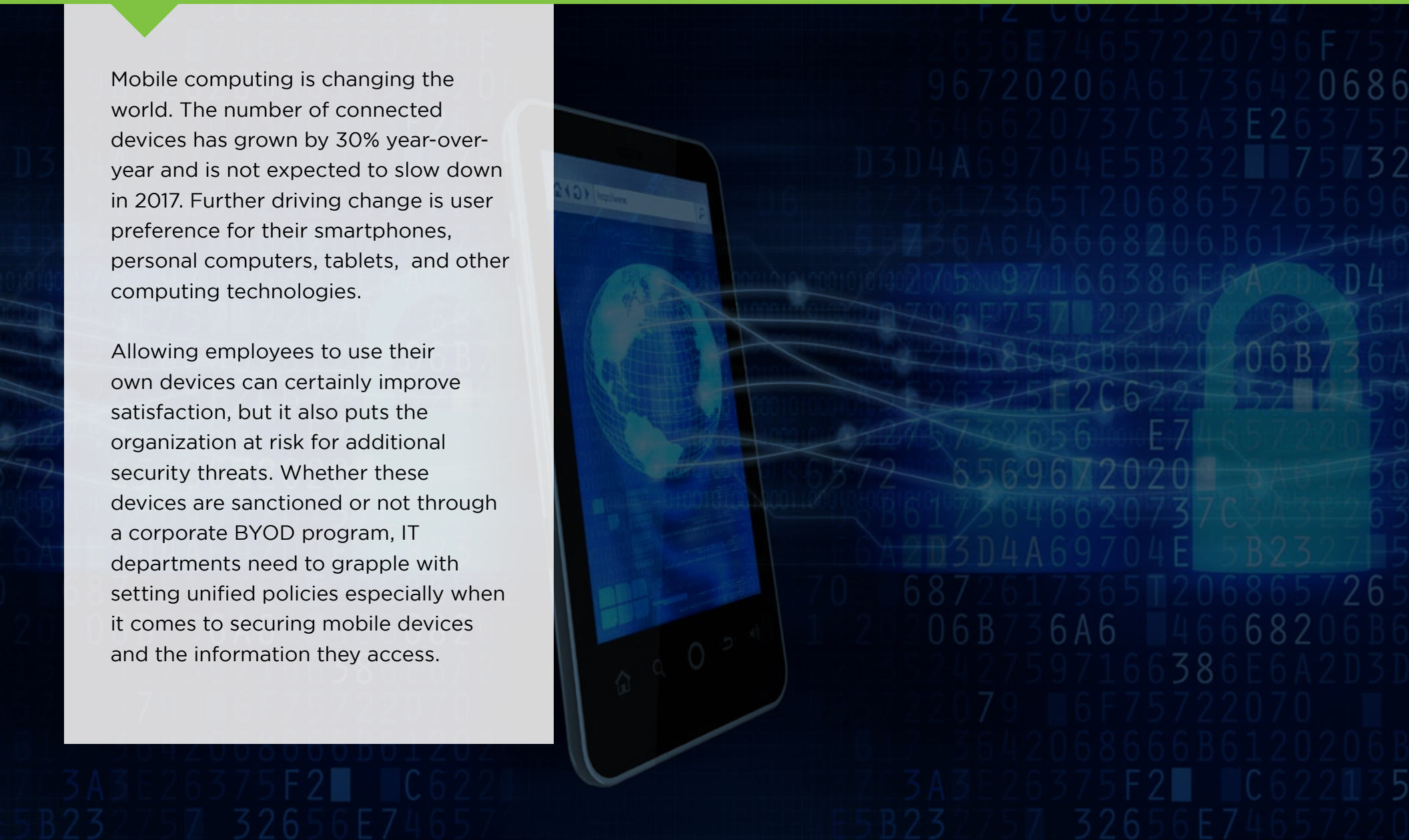
Security information and event management (SIEM)

Anti-virus / anti-malware 26% | Sandboxing 25% | Content filtering 20%

MOBILE SECURITY & BYOD

Mobile computing is changing the world. The number of connected devices has grown by 30% year-over-year and is not expected to slow down in 2017. Further driving change is user preference for their smartphones, personal computers, tablets, and other computing technologies.

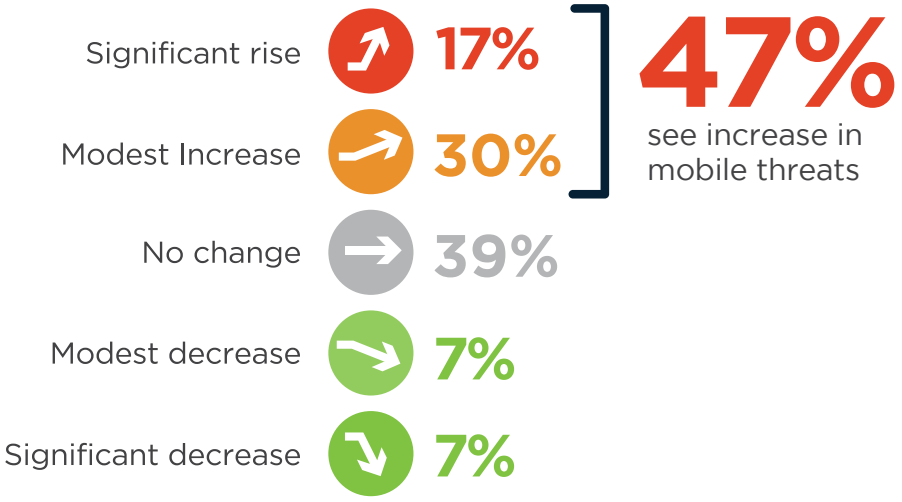
Allowing employees to use their own devices can certainly improve satisfaction, but it also puts the organization at risk for additional security threats. Whether these devices are sanctioned or not through a corporate BYOD program, IT departments need to grapple with setting unified policies especially when it comes to securing mobile devices and the information they access.

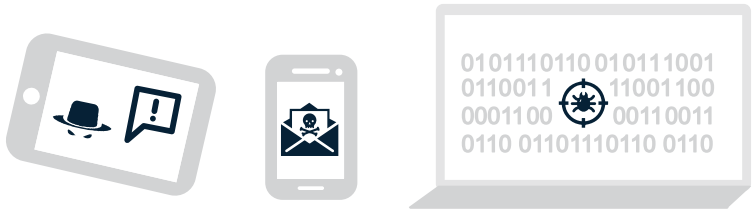


MOBILE SECURITY THREATS

The dramatic growth of mobile devices is driving an increase in cybercrime, from stolen identities to major data breaches. Forty-seven percent of respondents observe either a moderate rise (30%) or significant rise (17%) in mobile device threats. Very few respondents (14%) see modest or significant decreases in mobile threats.

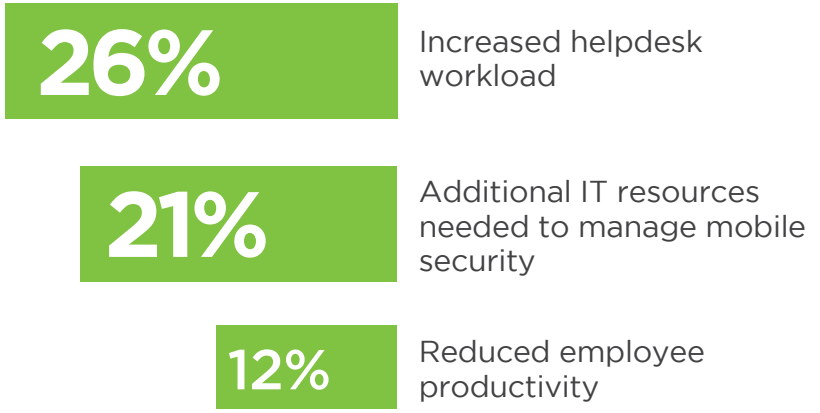
Q: How has the volume of mobile device threats targeting your users' smartphones and tablets changed in the past 12 months?





The impact of mobile threats is being felt in terms of added helpdesk workload and associated cost (26%), need for additional IT resources to manage mobile security (21%), and reduced employee productivity (12%).

Q: What actual negative impact did mobile threats have on your company in the past 12 months?



Unauthorized access to corporate data and systems 12% | Malware infections and related cost 11% | Data loss or leakage occurred 11% | Disrupted business activities 7% | The company had to pay regulatory fines 1% | Not sure/Other 27%

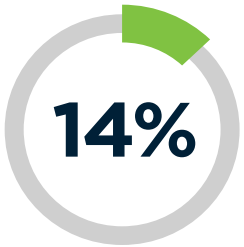
DRIVERS AND BARRIERS OF BYOD ADOPTION

Security is by far the number one barrier to stronger BYOD adoption. For the IT and security teams inside organizations, this points to potential security gaps or weaknesses that may need to be addressed.

Q: What do you believe is the number one inhibitor to BYOD adoption in your organization?

31%
Security Concerns

We don't experience any resistance to BYOD adoption



Employee privacy concerns (e.g., over EMM software)

We offer managed / company owned devices as alternatives 12% | Employees don't want to take on the additional expense 6% | User experience concerns (battery life, don't like app choices, etc.) 5% | Employees don't want or need access through personal devices 4% | Support cost concerns 4% | Management opposition 4%

With over 4 billion mobile subscribers, we live in a world where mobility is ubiquitous and enterprises have begun to benefit from it. The top three drivers of BYOD among employees are improved mobility (65%), reduced cost (55%), and greater employee satistaction (52%).

Q: What are the main benefits of BYOD for your company?

65% Improved employee mobility & productivity

55% Reduced cost

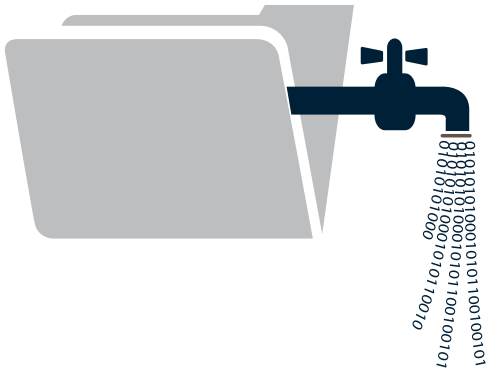
52% Greater employee satisfaction

11% Reduced security risk

BYOD SECURITY CONCERNS

As mobility and BYOD initiatives grow in the workplace, so do security concerns. Of biggest concern related to BYOD is data leakage or loss (69%), download of unsafe applications or content (64%), and the introduction of malware into the organization's IT environment (63%).

Q: What are your main security concerns related to BYOD?



69%
Data leakage /loss

64%
Users download unsafe apps or content

63%
Malware

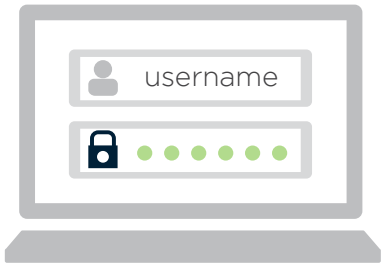
Lost or stolen devices 61% | Unauthorized access to company data and systems 58% | Vulnerability exploits 49% | Inability to control endpoint security 45% | Device management 41% | Network attacks via WiFi 38% | Ensuring security software is uptodate 38% | Compliance with regulations 32%

MOBILE SECURITY TECHNOLOGIES

The significant growth and integration of mobile technologies in both the personal and business spheres is driving IT departments to rethink the security technologies they are using to protect sensitive data and devices. The most commonly used mobile security controls include password protection (77%), remote wipe (72%), device encryption (69%), data removal at device disposal (63%), and mobile device management / MDM (58%). It should be noted that 19% of respondents say they have no mobile security technologies in place.

Q: Which of the following mobile security technologies are in place?

Password protection



77%

Remote wipe

72%

Device encryption

69%

Data removal at employee separation or device disposal

63%

None

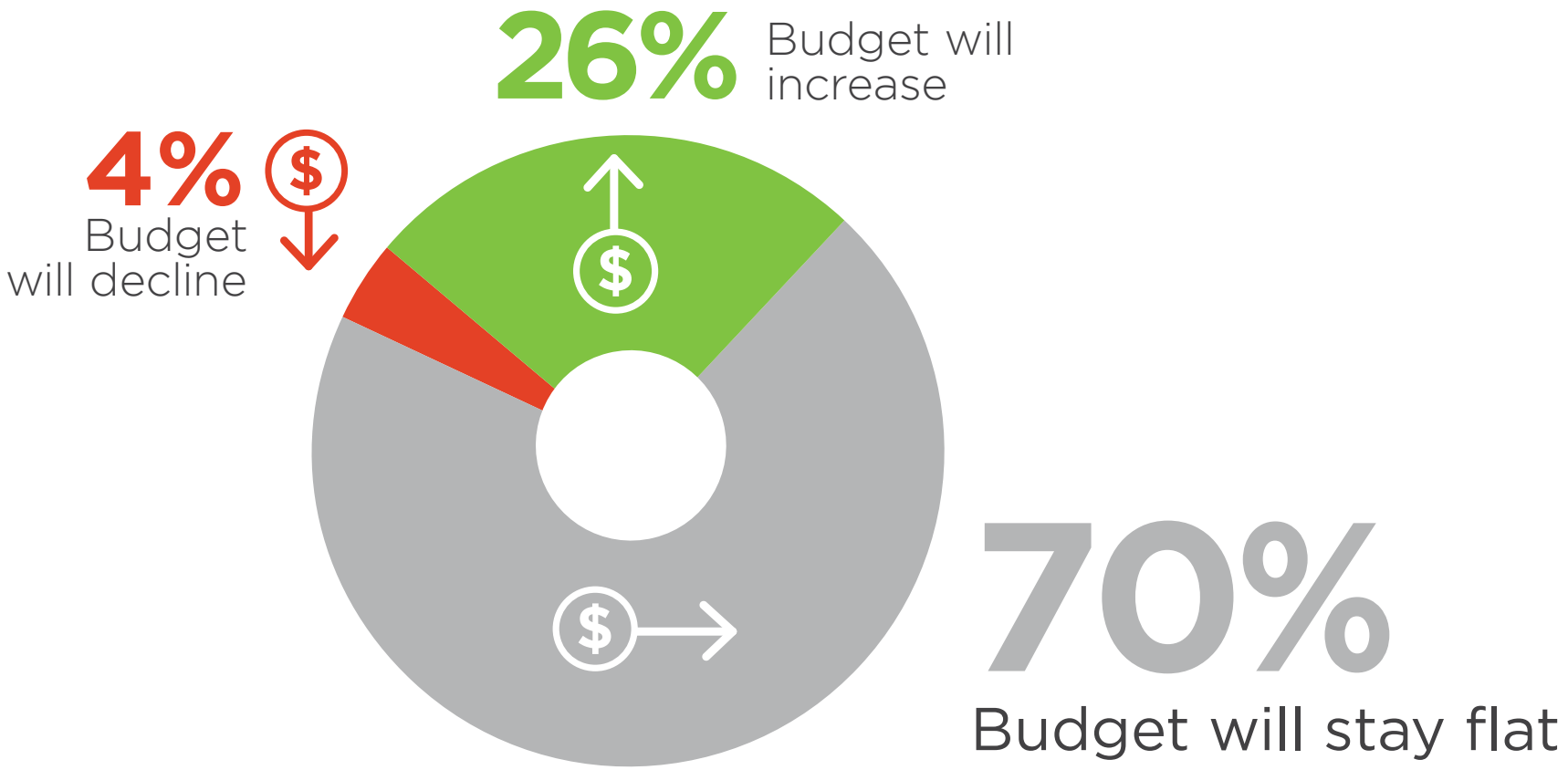
19%

Mobile device management (MDM) 58% | Mobile device file/data encryption 48% | VPN to onpremises security gateway 47% | Endpoint security tools 43% | Device management 41% | Mobile device antivirus/antimalware 39% | Network access control (NAC) 38% | DLP / Access Control 37% | Mobile application management (MAM) 33% | Auditing of mobile devices 30% | Virtual desktop infrastructure (VDI) 30% | VPN to cloudbased security gateway 29% | Containerization/microvirtualization 23% | Automated remediation using other security systems 22% | Mobile Threat Detection & Management (MTM) 22% | Attack and penetration testing of mobile applications 22% | None 19% | Not sure 32%

MOBILE SECURITY BUDGET

While the future of mobile computing is certainly bright, there are many security challenges to address. These concerns are reflected in the budget priorities for 26% of organizations who plan to increase mobile security spend over the next 12 months. Only four percent of respondents are planning on reducing security investments.

Q: How is your mobile security budget going to change over the next 12 months?



APPLICATION SECURITY

Organizations across all sizes and industries are increasingly concerned about the security of their web applications, mobile applications, software packages such as ERP and other software. Application related breaches can lead to lost revenue, significant recovery expense, and loss of reputation. Thus, many organization implement incentives to prevent gaps in the security policy of an application or to avoid vulnerabilities in the underlying system that are could be caused by flaws in the design, development, deployment, upgrade, or maintenance or database of the application.

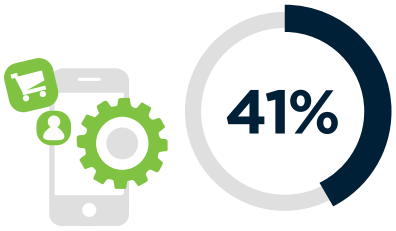
APPLICATIONS AT RISK

According to Verizon's recent security report, attacks on web applications are now the #1 source of data enterprise breaches, up 500% since 2014, causing cybersecurity professionals to be most concerned about customer facing web apps (50%) introducing security risk to the business. This is followed by mobile apps (41%) and desktop apps (34%) and business apps such as ERP platforms (29%).

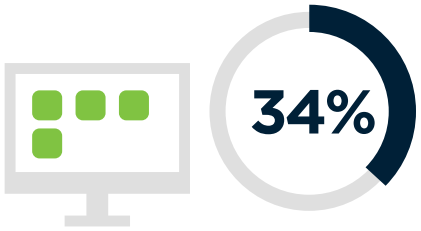
Q: Which types of applications present the highest security risk to your business?

50% Customer-facing web applications

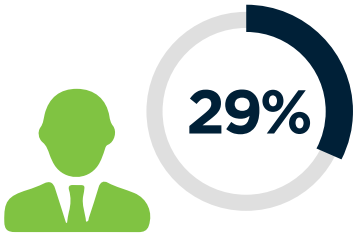
Mobile applications



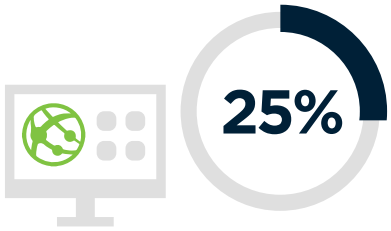
Desktop applications



Business Applications
(ERP, SCM, MES, HR SRM, etc)



Internal-facing web applications



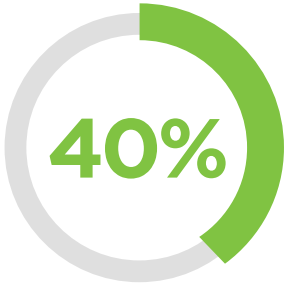
APPLICATION SECURITY CONCERNS

Protection of data (55%) tops the list of application security concerns, followed by detection of threats and breaches (40%) and meeting compliance requirements (33%).

Q: What are your top application security concerns?

#1
Protecting data

#2
Threat detection/ breach detection



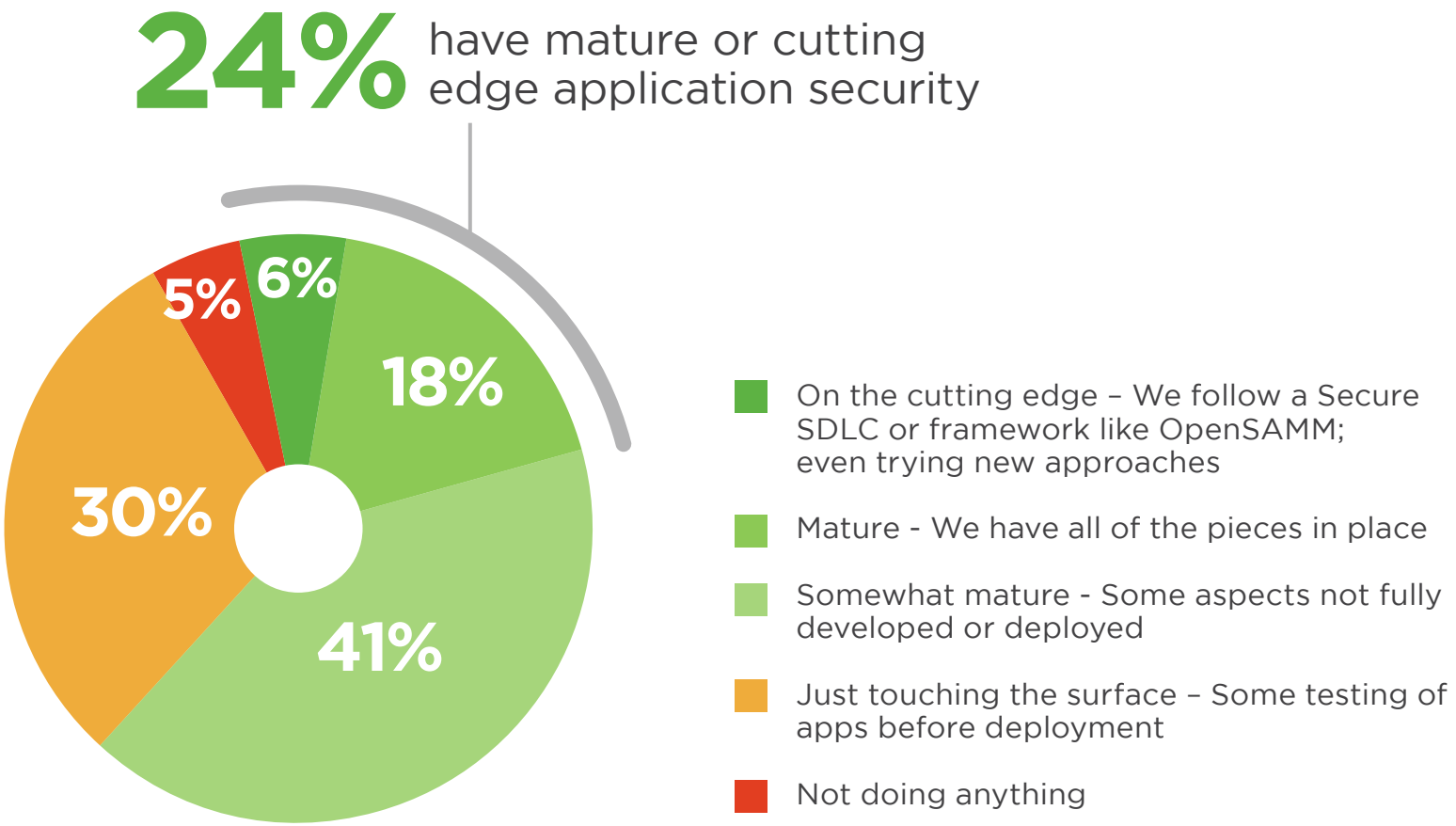
#3
Meeting regulatory/ compliance requirements

Security cloud apps 32% | Malware 32% | Security mobile apps 29% | Securoty business apps (ERP,etc) 26% | Effective threat modeling 26% | Meeting customers' security needs and requirements 24% | Securing open source software 19% | Other 2%

APPLICATION SECURITY MATURITY

Only a small minority of organizations consider themselves at the cutting edge of application security (6%) or mature, with all critical application security controls in place (18%). The plurality of organizations feels only somewhat mature (41%) with key application security controls missing or just touching the surface (30%).

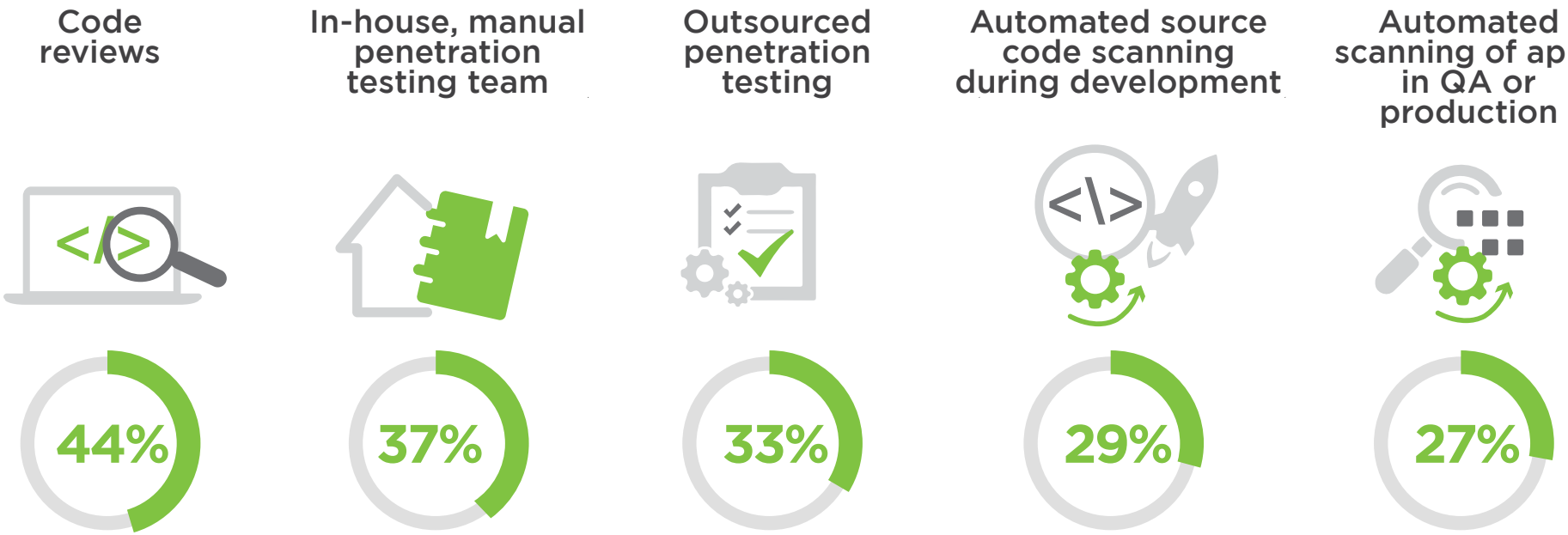
Q: Where do you think your company is in terms of the maturity of your application security strategy?



APPLICATION SECURITY TESTING

Code reviews are the most common security testing control deployed by organizations (44%). This is followed by penetration testing, either conducted in-house (37%) or outsourced (33%). Application scanning during development (29%), QA or production (27%) round out the top five most common security testing controls.

Q: What application security testing do you have in place currently?



Dynamic scanning of production code 24% | We require our software vendors to secure code before it enters our environment 20% | Automated binary code scanning during development 16% | None of the above 8% | Not sure/Other 20%

APPLICATION SECURITY CHALLENGES

A recurring theme in our cybersecurity survey, the lack of security skills (46%) combined with a lack of budget (45%) are the biggest obstacles to implementing a robust application security program.

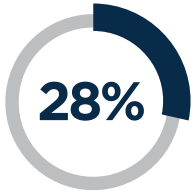
Q: What challenges do you face in implementing an application security program?

46%

Lack of skills

45%

Lack of budget



Lack of support/ management buy-in

No challenges

PROTECTING BUSINESS APPLICATIONS

Pentesting (59%) and security monitoring (58%) are leading the pack as the most popular measures to protect business applications.

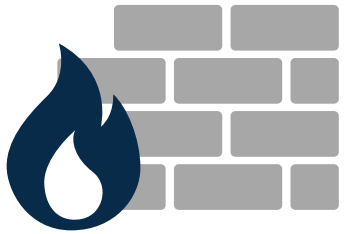
Q: What application security measures are you taking in order to protect your business applications?

59%

Penetrating testing

58%

Security monitoring



47%

Web application firewalls

Static/dynamic testing 44% | Developer education 44% | Bug bounty programs 8 % | Not sure/Other 14%

ERP SECURITY

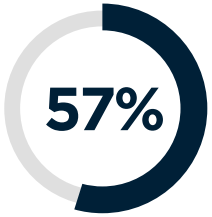
Just a few years ago, ERP security was a synonymous with separation of duties. Nowadays, leading analysts list ERP security as an increasingly important topic to protect the life blood of organizations processes and data managed in complex ERP systems.

ERP security has become a rapidly growing market as organizations start paying attention to this area of cybersecurity. This happened not least because of real cyber attacks against ERP platforms, first of all, the US-CERT alert addressing vulnerabilities in SAP, which hit headlines in 2016.

MOST CRITICAL BUSINESS APPLICATIONS

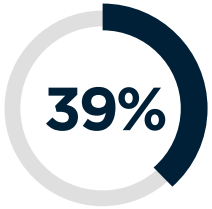
The three most critical business applications are at the core of organizations' business functions - any disruptions can immediately and significantly impact revenue: Enterprise Resource Planning (ERP) is considered the most critical business application by 61% of respondents. This is followed by financial systems (57%) and customer relationship systems (CRM) (55%).

Q: What are the most critical business applications?



Financial System (FI)

Customer Relationship Management (CRM)



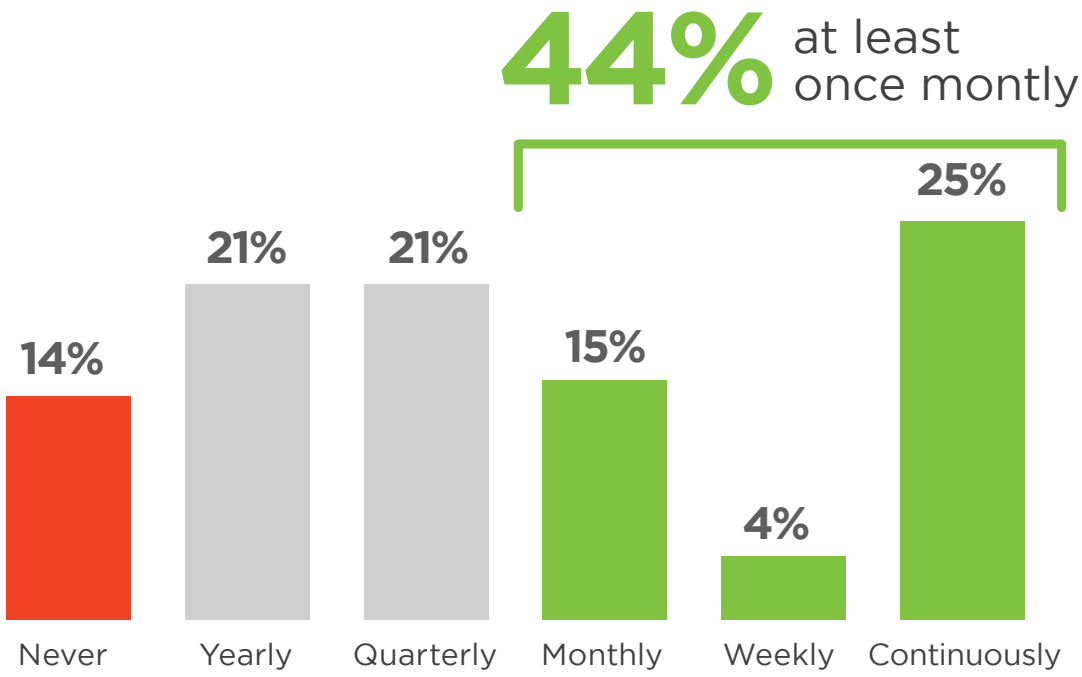
Human Capital Management (HCM/HR)

Business Intelligence (BI/BW) 36% | Supply Chain Management 32% | Product Lifecycle Management (PLM) 30% | Enterprise Asset Management (EAM) 27% | Supplier Relationship Management (SRM) 18% | Manufacturing Execution System (MES) 18%

ERP SYSTEM SECURITY

Forty-four percent of respondents analyze the security of their ERP systems at least monthly, 25% even continuously. An alarming 14% of respondents say they never analyze security of their ERP systems.

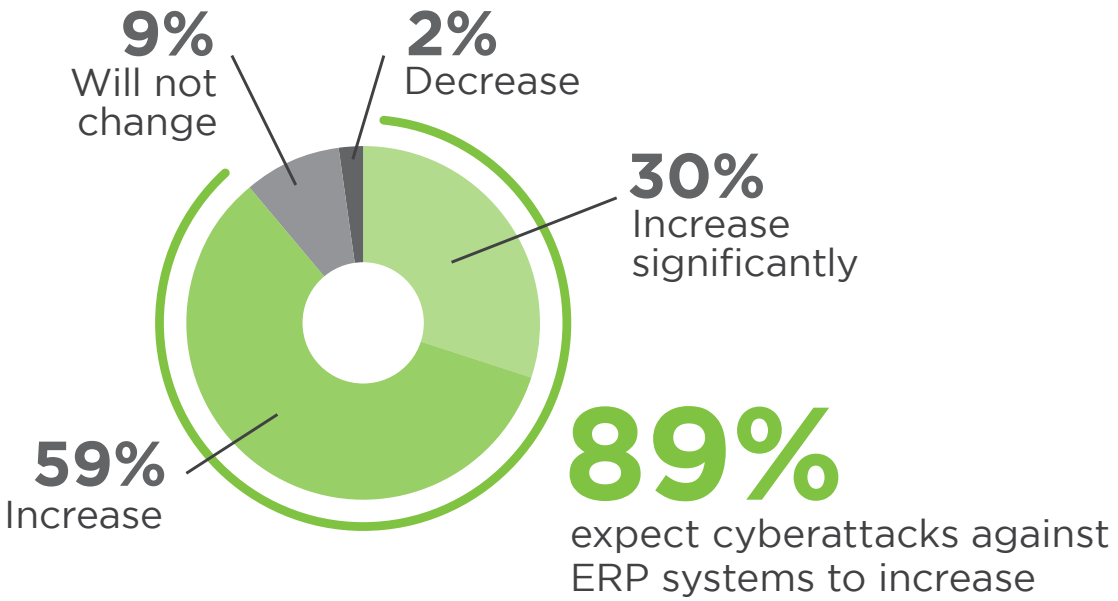
Q: How often do you analyze security of your ERP systems?



CYBERATTACKS AGAINST ERP SYSTEMS

Eighty-nine percent of IT security professionals expect the number of cyberattacks against ERP systems to increase - 30% of them expect a significant increase.

Q: How will the number of cyberattacks against ERP Systems change within the next 2-3 years?

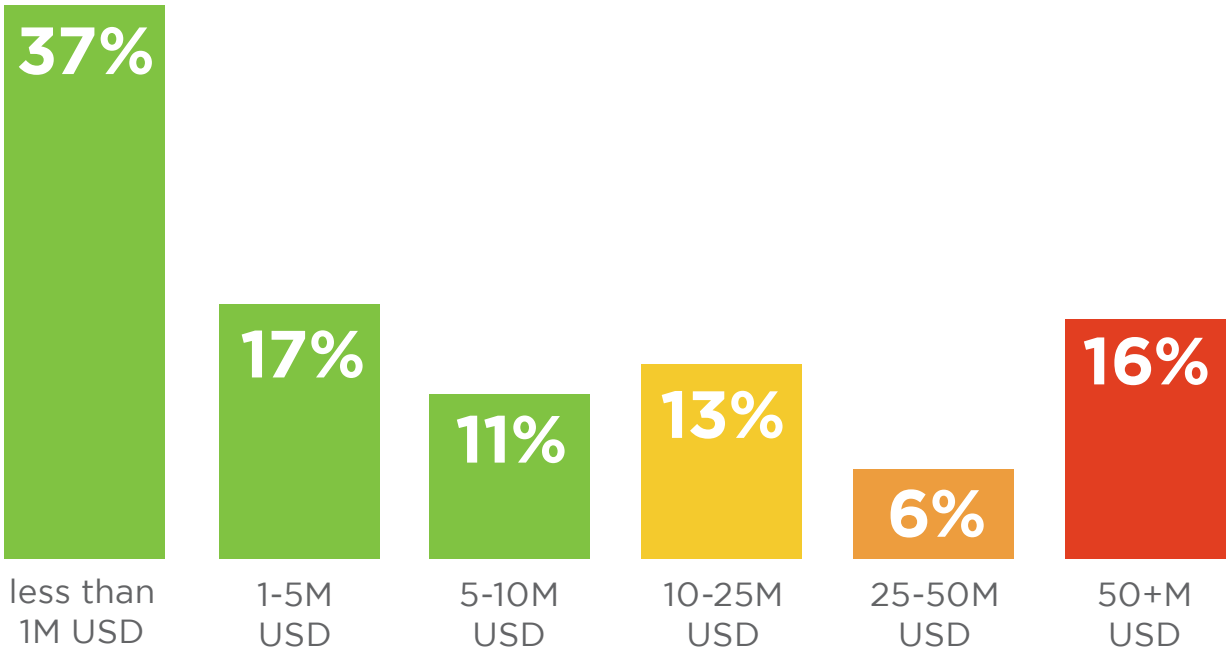


COST OF AN SAP ATTACK

A successful SAP breach can be very costly to an organization. While over a third of respondents estimate a successful SAP attack to cost their organization less than $1 million in damages, another third estimates cost between $1 million and $10 million, and the final third estimates cost of an SAP breach to be well over $10 million.

Q: How much would an attack on SAP cost your organization?

DATA THEFT



DATA & FILE PROTECTION

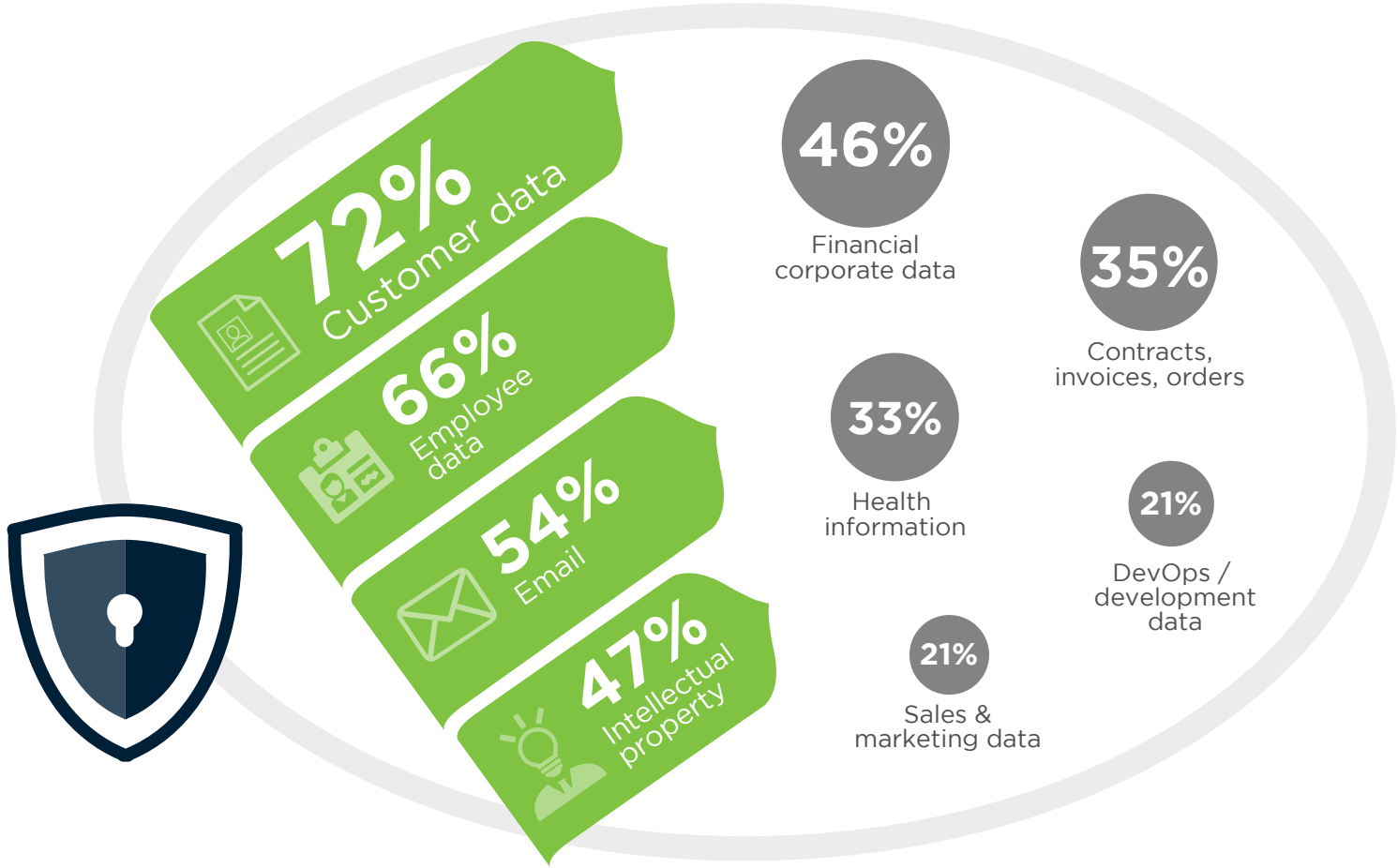
Data is the lifeblood of IT systems, services, and applications. It is also the ultimate target of attacks to steal, sell, manipulate, erase, or corrupt sensitive data and the systems that process it. Data protection needs to encompass a comprehensive strategy for protecting information assets from application/ user errors, malware attacks, machine failure, or facility outages/disruptions along the information lifecycle. This also includes the secure transfer of files, be it for backup or corporate projects. Today, email is still the most common file transfer method for smaller files – yet one of the least secure methods.

Sixty-seven percent of survey respondents ranked data encryption as the most effective means for protecting against cyber security attacks.

MOST SENSITIVE INFORMATION

Securing sensitive information is a key concern for all companies, also driven by regulation that require certain sensitive information be protected. Cybersecurity professionals are most concerned about protecting customer data (72%), employee data (66%), and email (54%). Sales and marketing data is considered least critical to be secured (21%). Robust protection of sensitive data at rest and in motion through encryption and other methods is paramount to organizations security strategy.

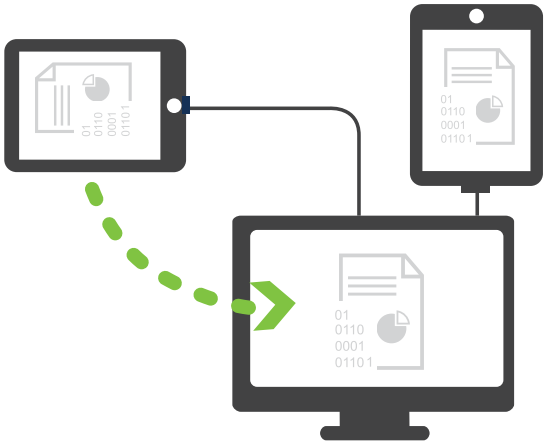
Q: What types of sensitive data are you most concerned about protecting?

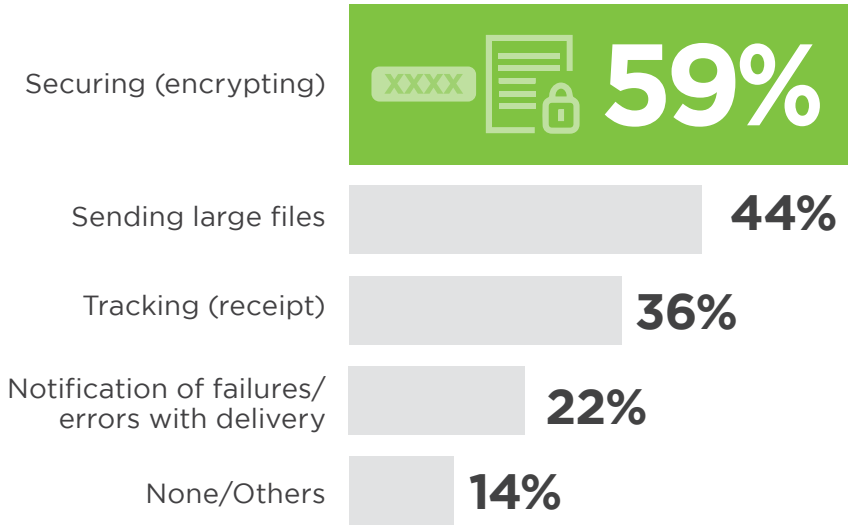


FILE TRANSFER CHALLENGES

Security is the number one concern (59%) when transferring files, followed by sending large files (44%) and tracking file transfer success (36%).

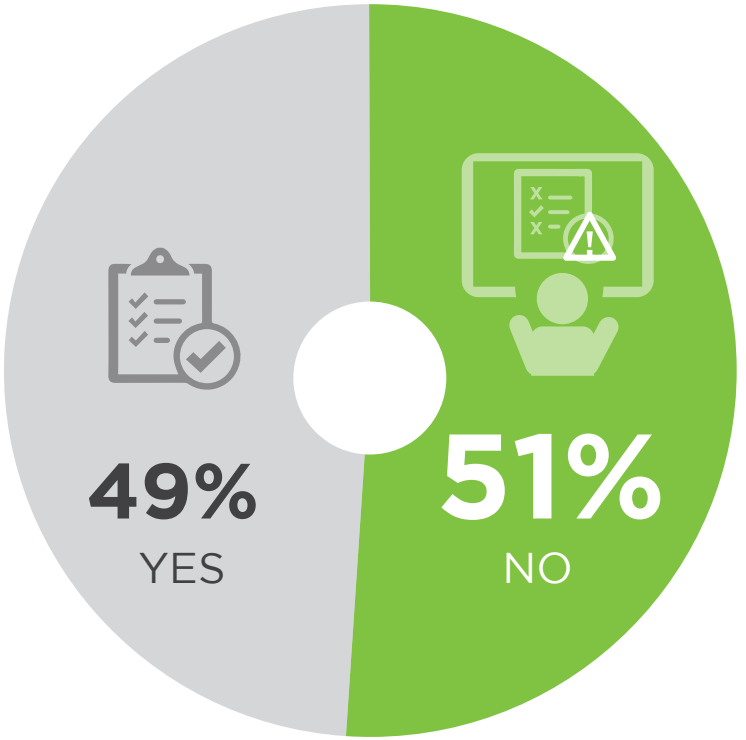
Q: Which challenges do you face when transferring files?





Over half of IT security professionals confirm they lack the tools to prove compliance related to transfer of sensitive files. Secure file transfer solutions should include not only proper file encryption and access controls but also detailed audit logs for maintaining compliance – ideally automated as to reduce the potential for human error.

Q: If your file sharing practices were audited for regulatory compliance, do you have the tools you need to streamline the process?

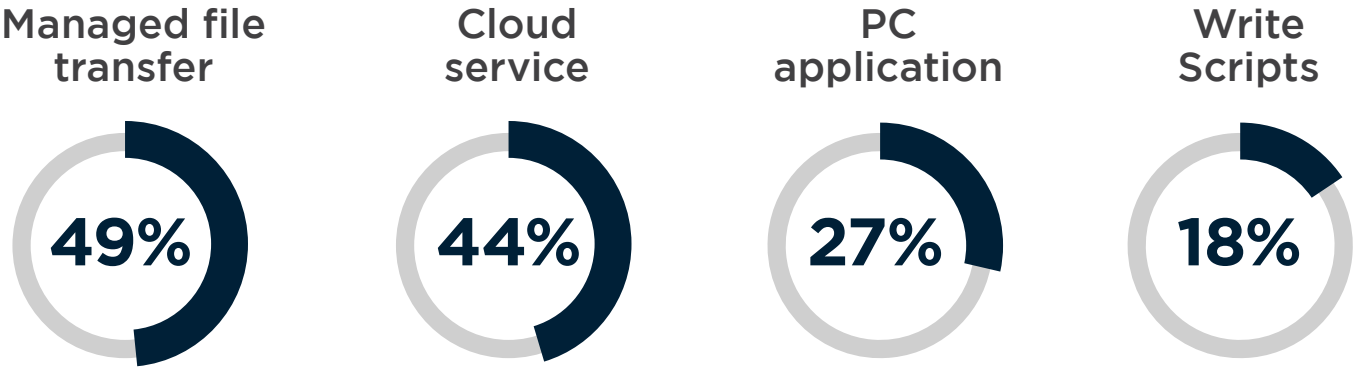


FILE EXCHANGE METHODS

Email is still the most common file transfer method for smaller files (63%). This is a red flag as unsecured email is both prone to security risk and difficult to track for auditing purposes. For larger files, managed file transfer is the next most popular (and more secure) choice (49%), followed by cloud services such as Dropbox, WeTransfer, or YouSendIt (44%).

Q: How do you currently exchange files?

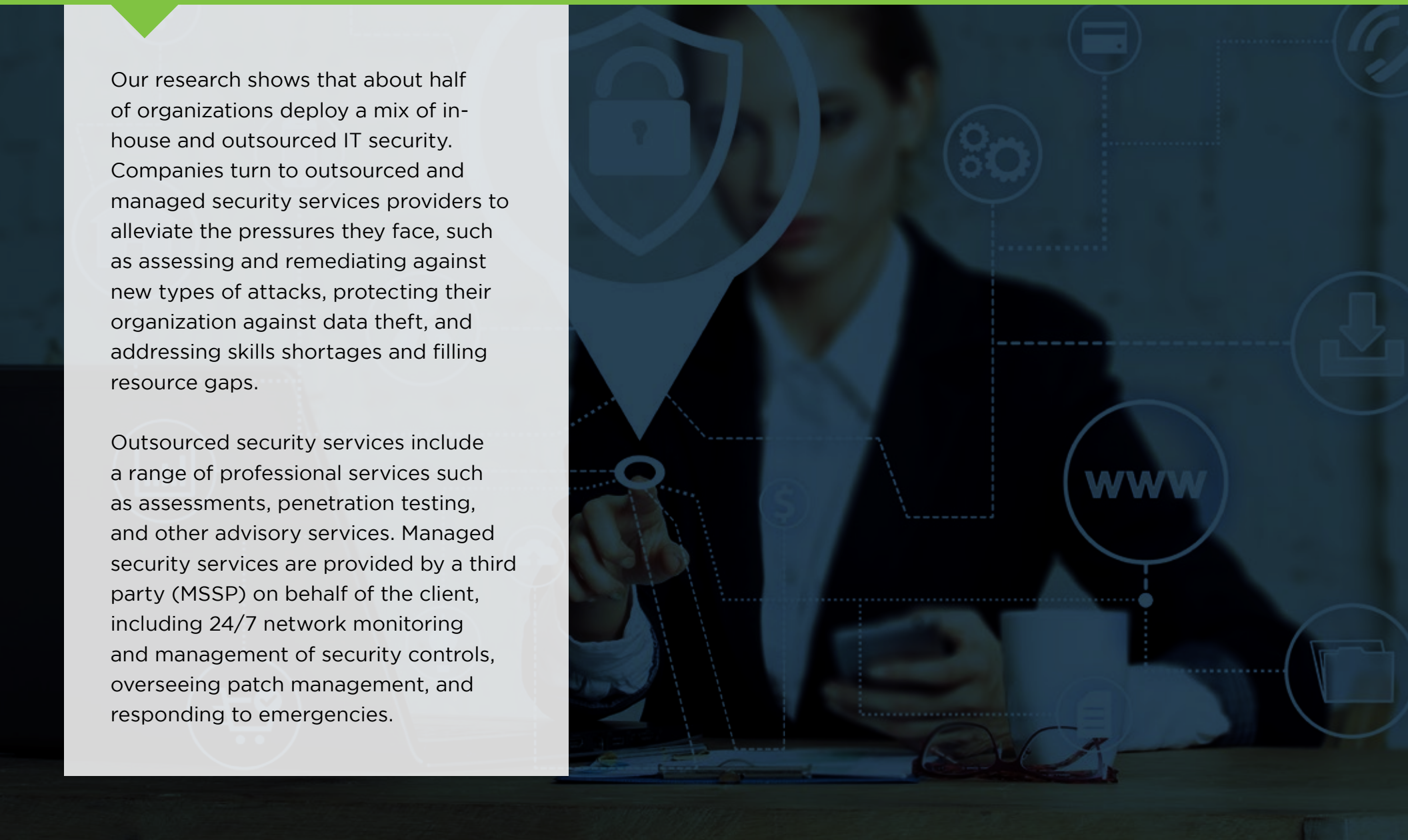
63%
Email



MANAGED & OUTSOURCED SECURITY SERVICES

Our research shows that about half of organizations deploy a mix of in-house and outsourced IT security. Companies turn to outsourced and managed security services providers to alleviate the pressures they face, such as assessing and remediating against new types of attacks, protecting their organization against data theft, and addressing skills shortages and filling resource gaps.

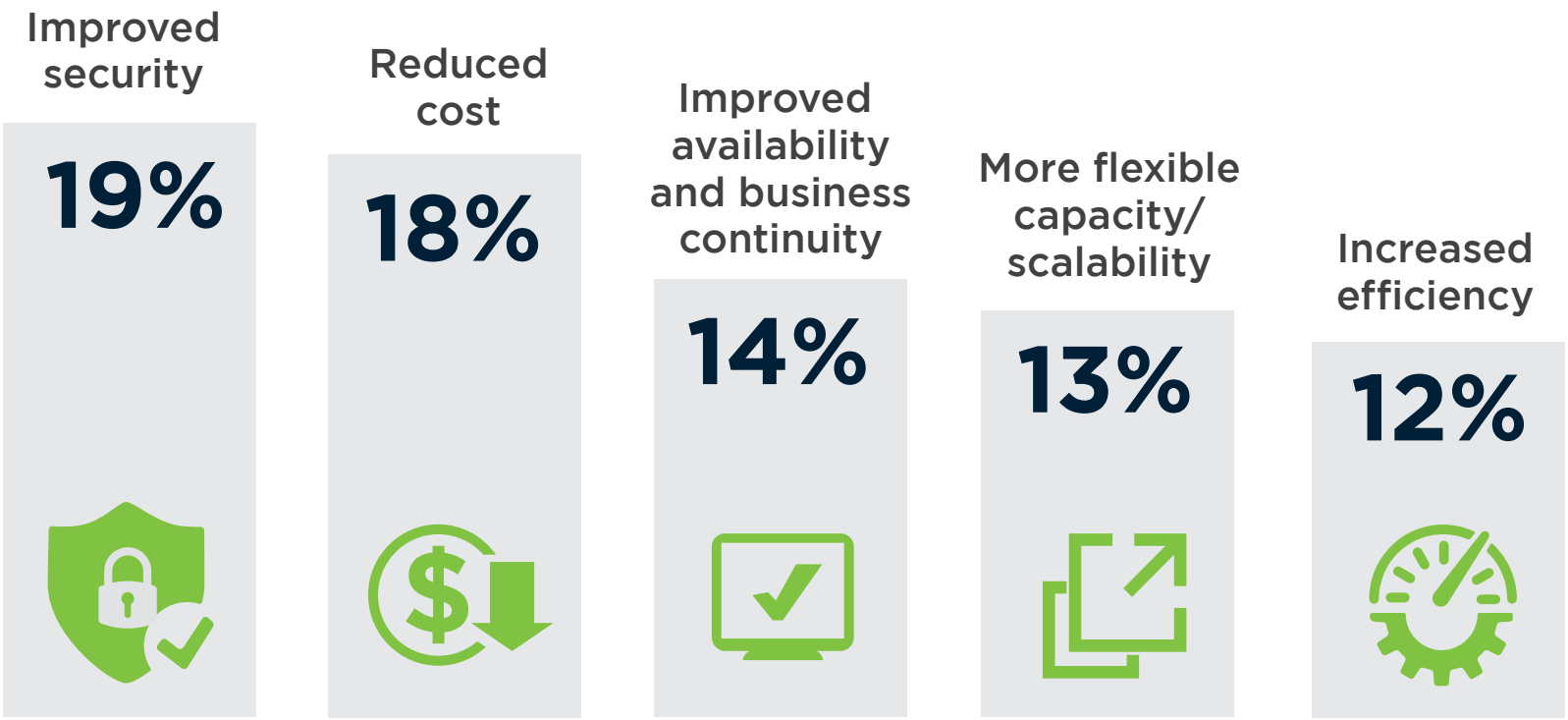
Outsourced security services include a range of professional services such as assessments, penetration testing, and other advisory services. Managed security services are provided by a third party (MSSP) on behalf of the client, including 24/7 network monitoring and management of security controls, overseeing patch management, and responding to emergencies.



BENEFITS OF OUTSOURCING SECURITY

The two most frequently mentioned benefits organizations have realized from managed security services are improved security and reduced cost – two of the main drivers for organizations looking to outsource information security. Improved availability, flexible capacity and scalability, and increased efficiency round out the top 5 benefits. These findings confirm that organizations generally receive the overall benefits promised by managed security providers.

Q: What benefits have you realized from outsourcing security to a third-party service provider?

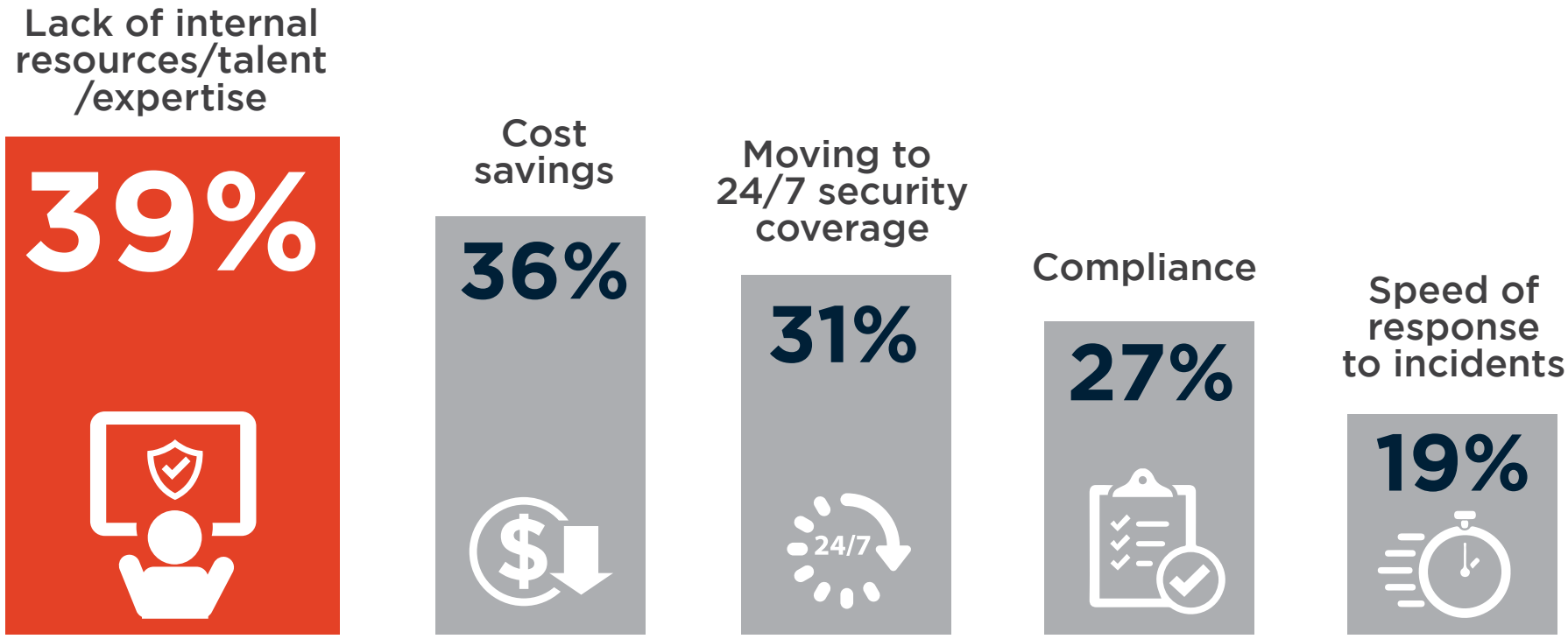


Increased geographic reach 10% | Improved performance 8% | Improved regulatory compliance 8% | Moved expenses from fixed CAPEX (purchase) to variable OPEX (rental/subscription) 6% | Reduced complexity 6% | Accelerated deployment and provisioning 5% | Increased Agility 3% | IAccelerated time to market 3% | Increased employee productivity 1% | Align cost model with usage 1%

WHY MANAGED SECURITY

The predominant driver for organizations to consider managed security services is lack of internal security resources and expertise (39%) to cope with the growing demands of protecting data, systems and applications against increasingly sophisticated threats. This is closely followed by a desire to reduce the cost of security (36%), moving to continuous 24/7 security coverage (31%), improving compliance (27%), and increasing the speed of response to incidents (19%).

Q: If you're not currently using a managed security service provider, what would drive you to do so?



Lack of security domain expertise 17% | Looking to shift cost from capex/headcount to opex 16% | Breach Protection 15% | Lack of industry compliance expertise 11% | Other 9%

MSSP EVALUATION FACTORS

Security expertise (71%) is by far the most critical capability organizations look for in MSSPs, followed by cost (54%) and breadth of capabilities (50%) – all in close alignment with the research findings regarding the key drivers for outsourcing security. Reputation (48%) and flexibility (31%) round out the top five selection criteria.

Q: What factors are most important to you when selecting a managed security services provider (MSSP)?

#1

71%

Security expertise

#2 **54%** Cost

#3 **50%** Breadth of capabilities

#4 **48%** Stability/ reputation

#5 **31%** Flexibility

Industry/ vertical domain expertise 21% | Leadership 17% | Location / Proximity (Ability to interact with a local or regional analyst) 15% | Company size 14% | Customized approach 7% | Other 7%

MOST IMPORTANT MSSP CAPABILITIES

The most requested security capabilities offered by MSSPs are security monitoring (54%), event correlation and alerting (52%), and intrusion detection and prevention (IDS/IPS) (49%).

Q: What are the most important capabilities your MSSP needs to provide?

#1

54%

Security monitoring

#2

52%

Event Correlation and Alerting

#3

49%

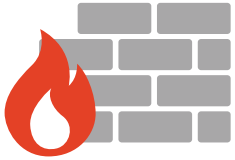
IDS/IPS

#4

47%

SIEM

#5



35%

Firewall

#6

32%

Threat Hunting

Packet Capture 17% | EDR Management 12% | DFIR 12% | Other 12%

OUTSOURCED ADVISORY SERVICES

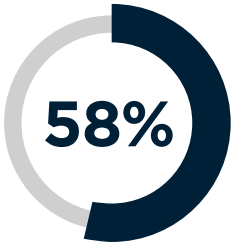
To stay ahead of evolving security threats or recover from successful attacks, organizations often find it valuable to outsource certain services to maintain or regain a strong security posture. The top three advisory services companies outsource include penetration testing (72%), security assessments (58%), and education and training (47%).

Q: What security advisory services would you consider outsourcing to a security service provider?

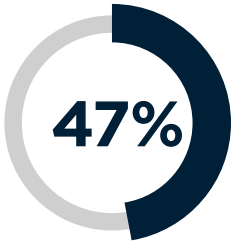
72%

Penetration testing

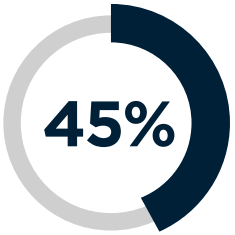
Security assessment



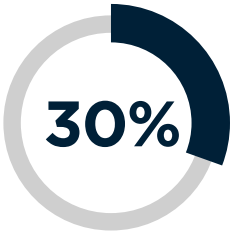
Education/ Training programs



Cyber Exercises/ Red Team Operations



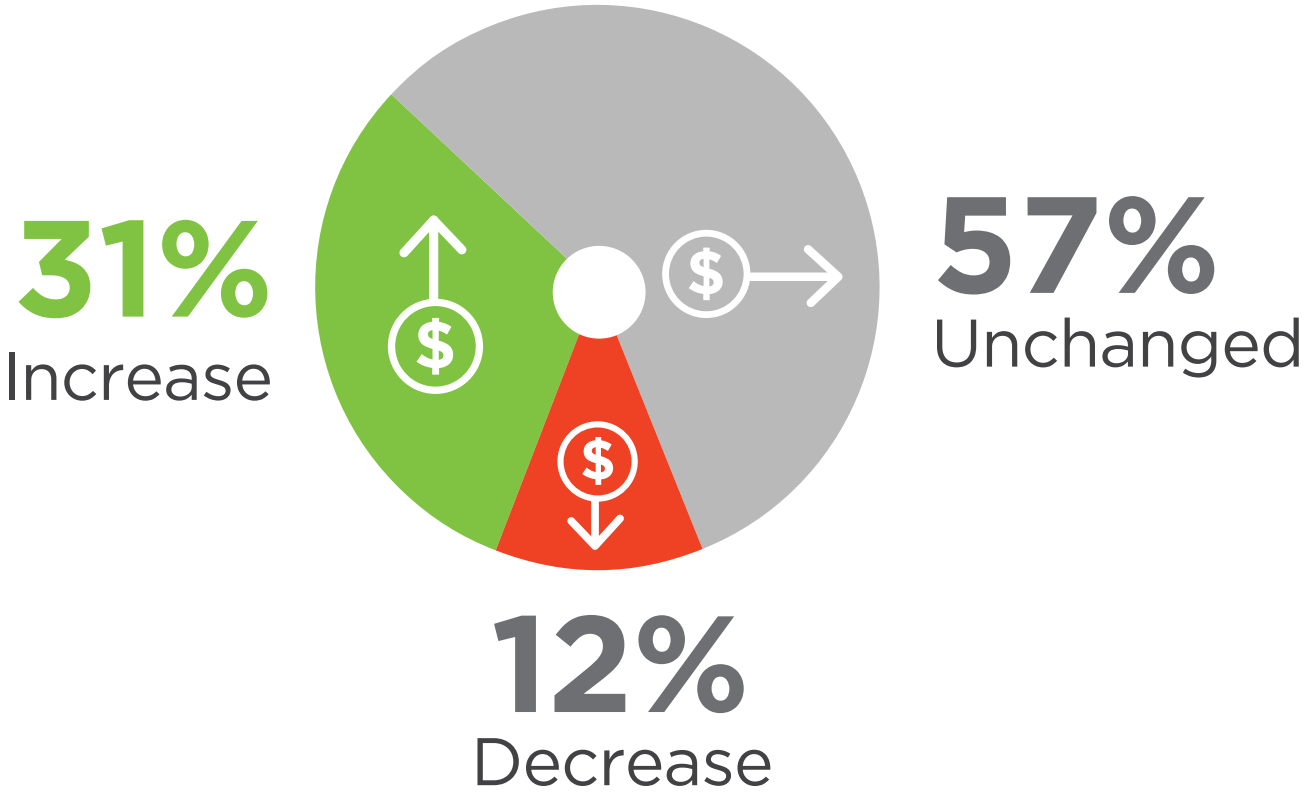
Compliance



MANAGED SECURITY BUDGET TREND

About a third of organizations predict a budget increase for managed security services over the next 12 months. With 31%, this area is receiving one of the largest shares of predicted budget increase across all IT security areas.

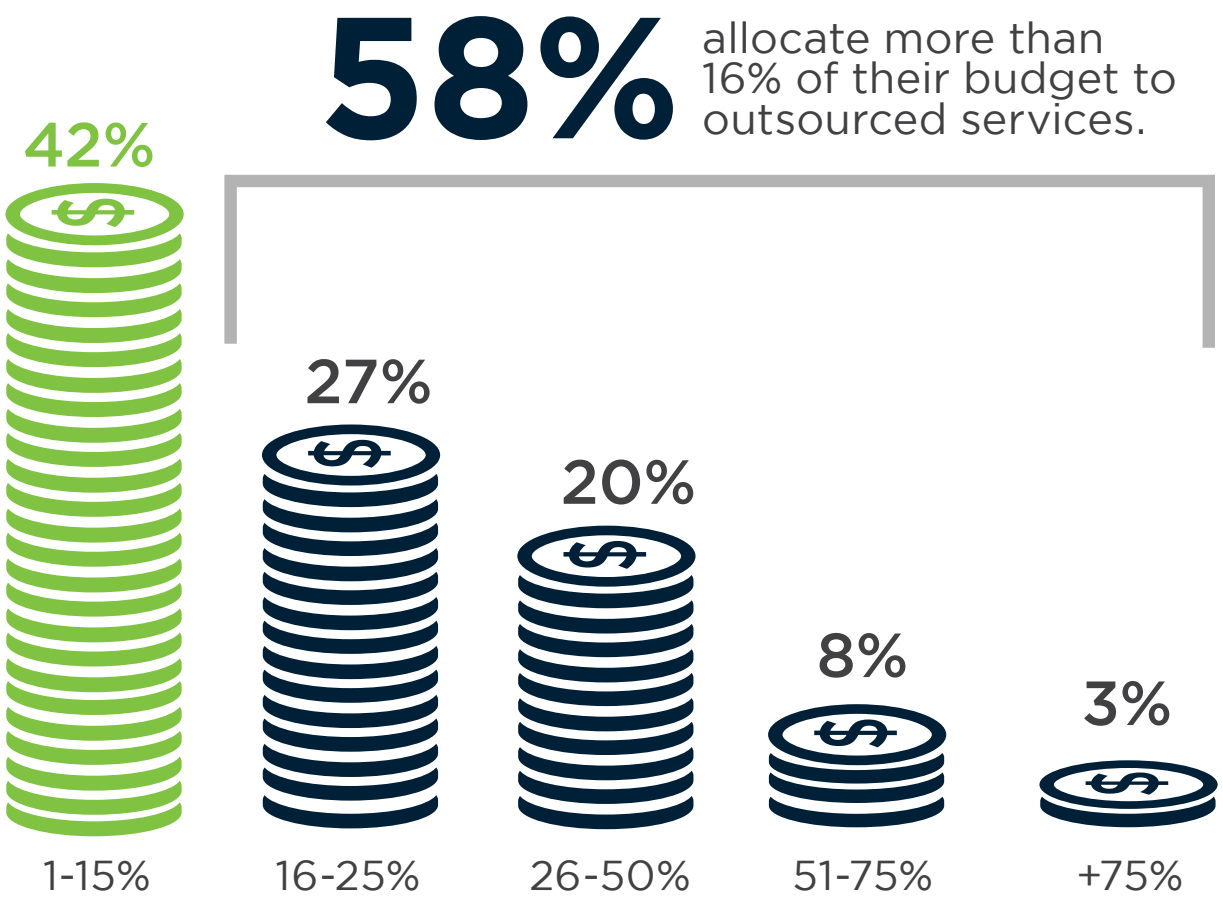
Q: What is your organization's budget outlook for managed security services?



MANAGED SECURITY BUDGET

Companies find value in outsourcing components of their security solution. Of organizations who use a mix of in-house and outsourced security, 58% allocate more than 16% of their budget to outsourced services - 31% of companies even allocate more than a quarter of budget to managed services.

Q: If you are using a mix of inhouse and managed security service providers, what percentage of your security budget is allocated for managed security services?



SECURITY TRAINING & CERTIFICATION

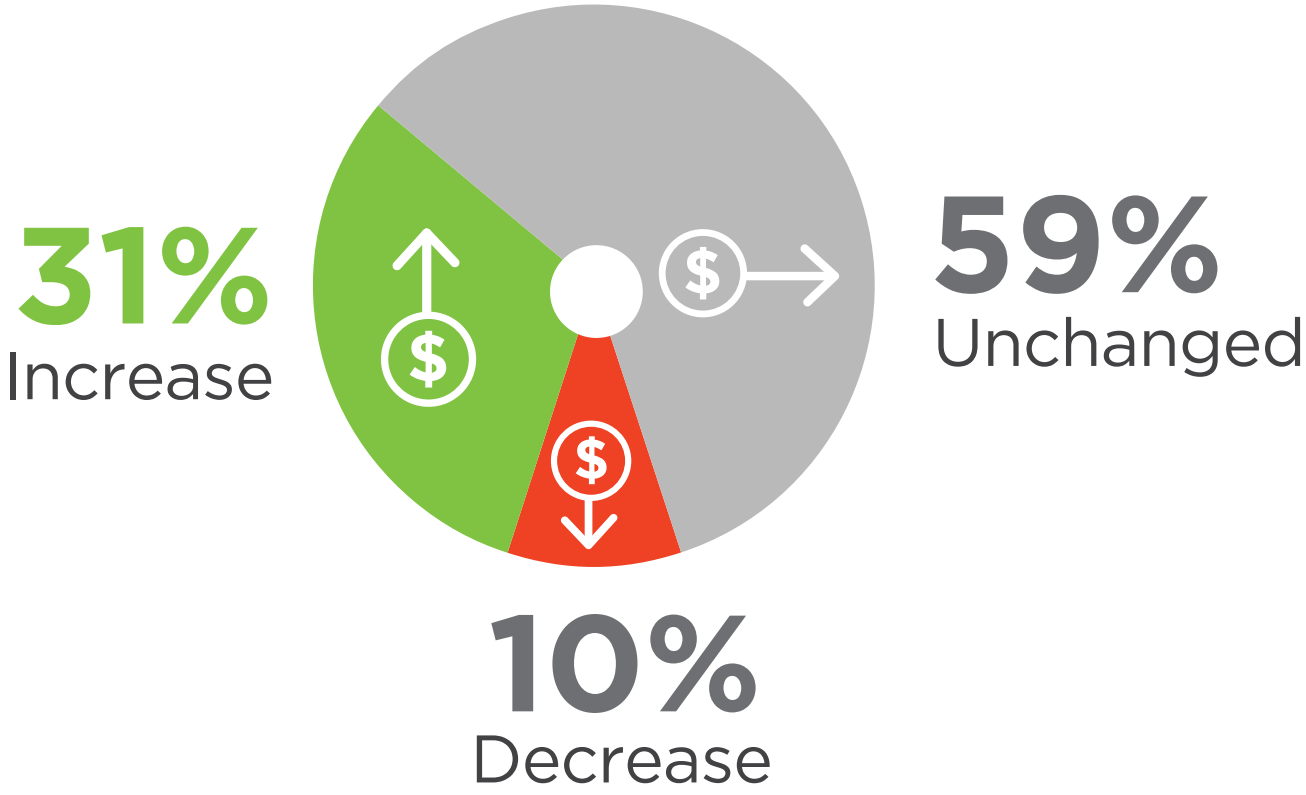
Security training and certifications are critical in ensuring employees and IT professionals are equipped with the latest skills and knowledge to provide compliance with regulations and help safeguard organizations' information and technology assets against cyber threats. Our survey reveals that 6 out of 10 employees would benefit from additional security training and certifications for their jobs.

Per IDC, the security training and certification market will reach over two-billion dollars by 2020. Fueled by accelerated use of cloud computing, mobility, and IoT technologies coupled with "always- on" organizations, these programs are rapidly evolving to keep up with the pace of changing technologies and cyber threats.

TRAINING & CERTIFICATION BUDGET

About a third of organizations predict a budget increase for security training, education, and certifications over the next 12 months. With 31%, this area is receiving one of the largest shares of predicted budget increase across all IT security areas.

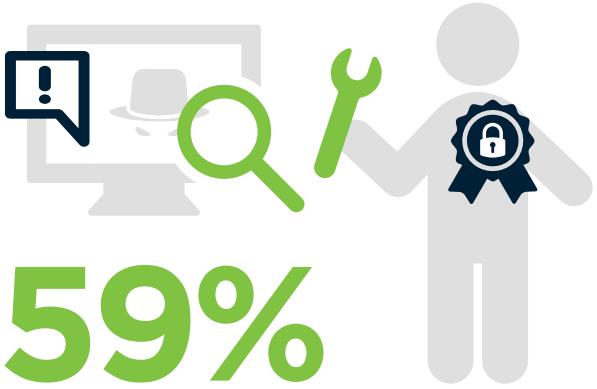
What is your organization's budget outlook for security training, education, and certifications?



MOST CRITICAL SECURITY SKILLS

When it comes to cybersecurity skills, organizations are prioritizing incident detection and response skills. Incident response skills are named as the most important security skill (59%), followed by detection of abnormal system behaviors (56%), and knowledge of critical business processes (55%).

Q: What are the most important security skills required in your organization?

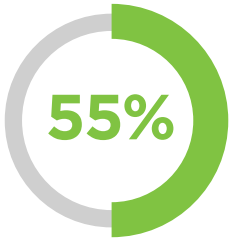


59%

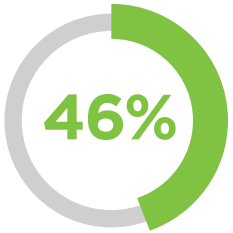
Incident response skills

Detection of abnormal system behaviors

Knowledge of critical business processes



Intelligence analysis skills

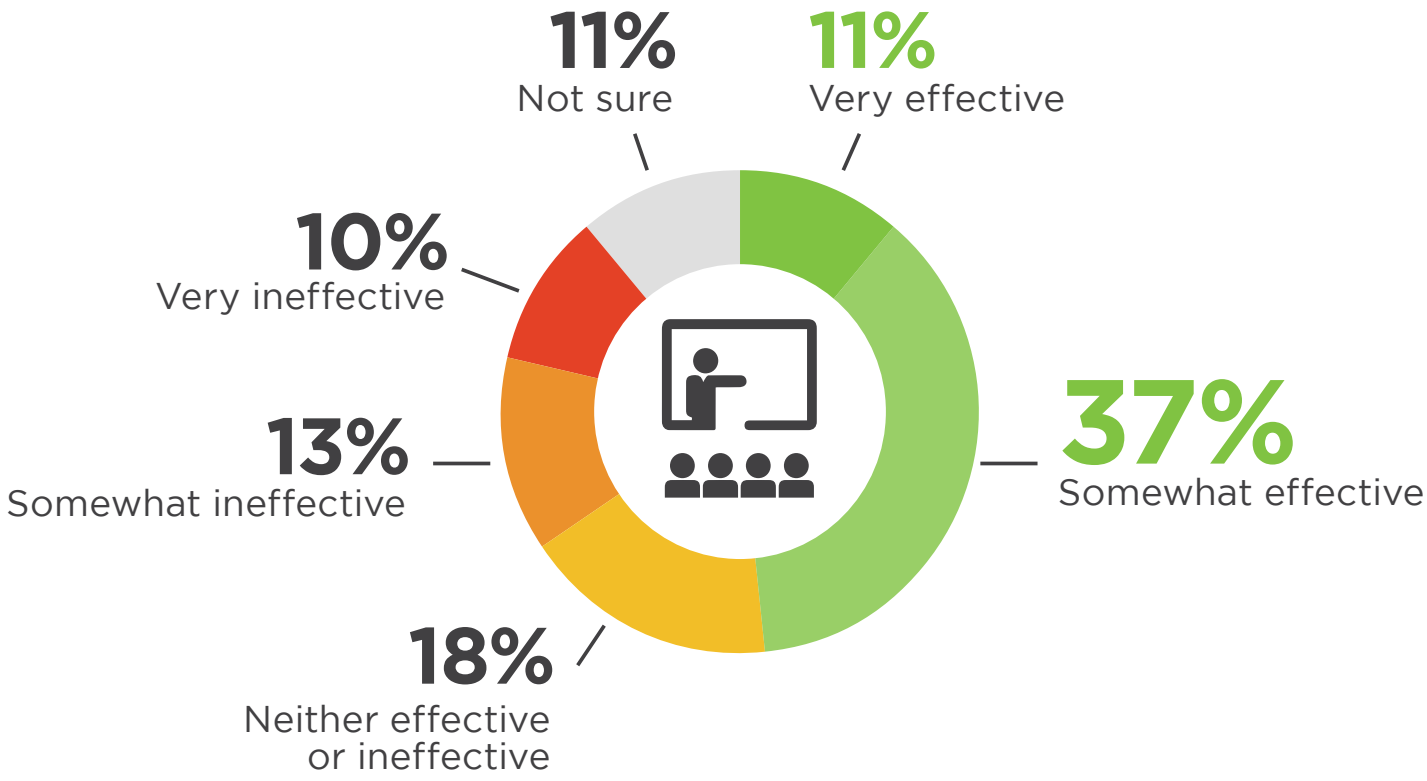


Malware analysis skills 39% | Familiarity with commercial tools and feeds 34% | Reporting/writing skills 34% | Presentation/oral communications skills 31% | Knowledge of adversaries and campaigns 22% | Ability to write correlation rules to link security events 21%

SECURITY PROGRAM EFFECTIVENESS

Security is not a destination, it is a process, and measuring security effectiveness is organization dependent. However, there are some best practices that companies can follow including measuring the success of an organization's security training programs. Cybersecurity professionals see room for improvement with their security training programs. Only 11% of respondents cite a very effective initiative while 37% feel their programs are somewhat effective. Ten percent of organizations claim very ineffective training efforts.

Q: How effective is your current security training program?

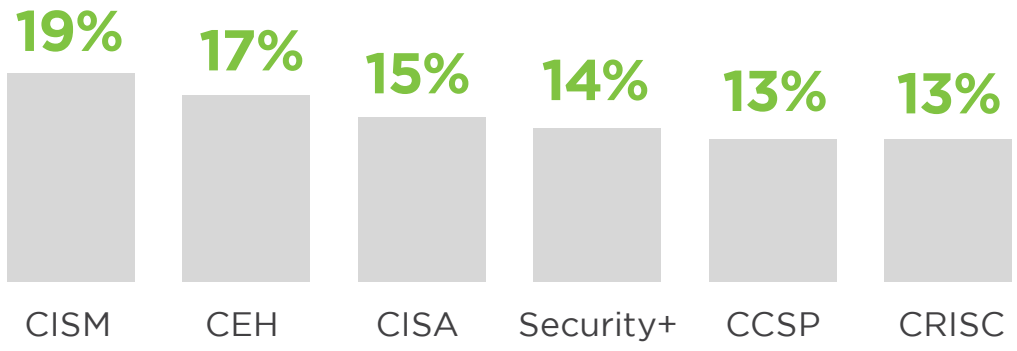


SECURITY CERTIFICATIONS

Securing today's complex and dynamic IT environments requires a blend of well trained and specialized resources. Survey respondents name CISSP as the security credential most valued by employers by a margin of 3 to 1. A distant second and third certification include CISM (19%) and CEH (17%).

Q: Regardless of whether you have these security certifications, how valued by your employers are these certifications?

Most valued credential

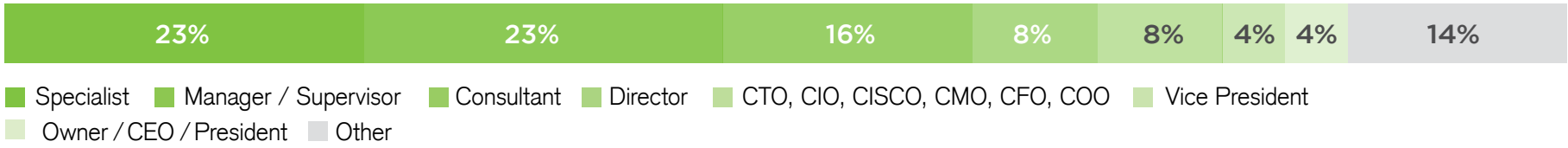


METHODOLOGY AND DEMOGRAPHICS

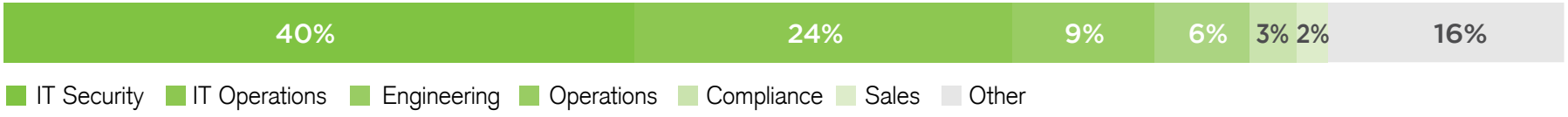
METHODOLOGY & DEMOGRAPHICS

The 2017 Cybersecurity Trends Report is based on the results of a comprehensive online survey of over 1,900 cybersecurity professionals to gain more insight into the latest security threats faced by organizations and the solutions to prevent and remediate them. The respondents range from technical executives to managers and IT security practitioners. They represent organizations of varying sizes across many industries. Their answers provide a comprehensive perspective on the state of cybersecurity today.

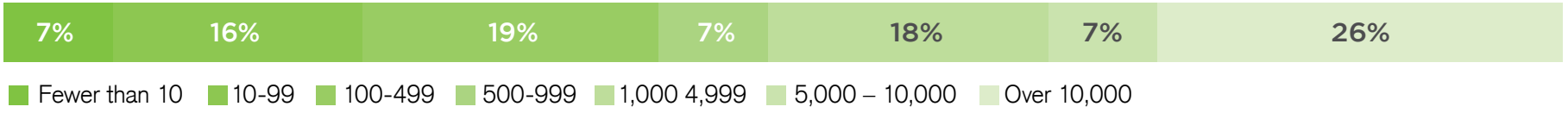
CAREER LEVEL



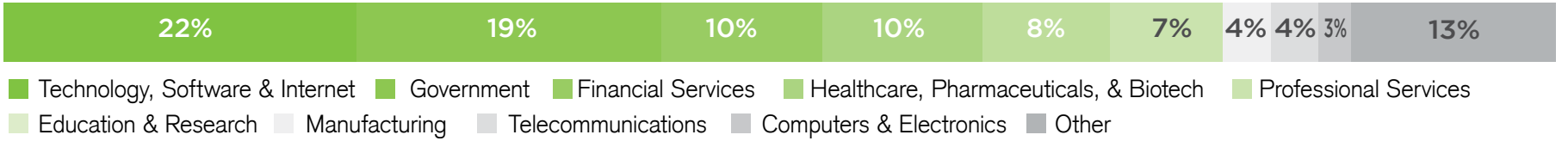
DEPARTMENT



COMPANY SIZE



INDUSTRY



SPONSORS OVERVIEW

SPONSORS

Alert Logic | www.alertlogic.com

Alert Logic® Security-as-a-Service solution delivers deep security insight and continuous protection for cloud, hybrid and on-premises data centers. Providing application, system and network protection from the cloud. The Alert Logic solution analyzes over 400 million events and identifies over 50,000 security incidents monthly for over 3,800 customers.

AlienVault | www.alienvault.com

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award winning approach combines our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, making effective and affordable threat detection attainable for resource constrained IT teams.

Bitglass | www.bitglass.com

Bitglass' Cloud Access Security Broker (CASB) solution provides enterprises with end-to-end data protection from the cloud to the device. It deploys in minutes and works across apps like Office 365, Salesforce, and AWS. Bitglass also protects data on mobile devices without the hassles of MDM.

Delta Risk | www.delta-risk.net

Delta Risk LLC provides cyber security and risk management services to government and commercial clients worldwide. Founded in 2007, Delta Risk offers managed security services, advisory and training, and incident response services to improve cyber security operational capability and protect business operations. Delta Risk is a Chertoff Group company.

SPONSORS

ERPScan | www.erpscan.com

ERPScan is the most respected and credible SAP and Oracle Cybersecurity provider. We function in two hubs, located in the Palo Alto and Amsterdam to operate local offices and partner network spanning 30+ countries around the globe. ERPScan was distinguished by 40+ awards and is the leading SAP SE partner in discovering security vulnerabilities.

Linoma | www.GoAnywhere.com

GoAnywhere MFT is enterprise-level software for automating and securing your file transfers through a single interface. GoAnywhere's security and auditing features help you achieve compliance, increase security, and streamline processes.

(ISC)² | www.isc2.org

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 123,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry.

Lynx Technology Partners | www.lynxGRC.com

Lynx Technology Partners is the trusted Information Security and Risk Management Advisor that customers in highly-regulated industries worldwide depend on to improve security posture, facilitate compliance, reduce risk and refine operational efficiency. Through consulting, security and risk assessments, penetration testing, managed security services and an award-winning GRC solution, Lynx supports many critical projects for security-conscious organizations.

SPONSORS

Raytheon | www.foregroundsecurity.com

Raytheon Foreground Security is a leading cyber security company providing proactive threat hunting, security engineering, assessment and customized security training. By leveraged blended threat intelligence research, analytics and automated machine learning, RFS proactively hunts to expose advanced threats – before they cause damage – and collaboratively partners with Customers to mature their security posture beyond compliance.

Sqrrl | www.sqrrl.com

Sqrrl is the only cybersecurity solution purpose-built for threat hunting. Sqrrl's primary value proposition is to help analysts discover new, unknown threats that were neither previously detected nor properly prioritized.

TopSpin Security | www.topspinsec.com

TopSpin Security provides intelligent deception and post-breach detection solutions that allow organizations to pin-point cyberattacks in real-time and cut time to resolution from days to minutes. TopSpin's unique DECOYnet™ platform combines sophisticated traffic analysis with a fully adaptive intelligent-deception layer keeps all network assets, services and IoT devices safe.

Veriato | www.veriato.com

Veriato develops intelligent, powerful monitoring solutions that provide companies with visibility into human behaviors and activities occurring within their firewall. Our products make organizations more secure and productive.

Zimperium | www.zimperium.com

Zimperium is the industry leader in Mobile Threat Defense offering real-time, on-device protection against both known and unknown cyberattacks via mobile OS, Wi-Fi networks and applications.

CONTACT US

Interested in joining the next security research report?

Contact Crowd Research Partners for more information.

info@crowdresearchpartners.com

Produced by:

Crowd Research Partners

LinkedIn Group Partner
Information Security