WINTER

CYBER SECURITY

2017 SURVEY

Welcome to the future of Cyber Security

Check Point SOFTWARE TECHNOLOGIES LTD.

CONTACT

SOUTHAMPTON HQ
Centurion House,
Barnes Wallis Road,
Segensworth, PO15 5TT
United Kingdom

PHONE

SOUTHAMPTON HQ	(+44) 0345 647 3000
LONDON	(+44) 0345 647 3100
HEATHROW	(+44) 0345 647 3200

ONLINE

Email : info@vohkus.com
Web : www.vohkus.com

TECHNOLOGY EDGE >|< BUSINESS EDGE®

INTRODUCTION

The future is no longer on a distant horizon: Mobility has overtaken the desktop as a fundamental part of how business is conducted; cloud adoption is prompting businesses to transform how they roll out applications and services with the promise of a more agile and automated IT infrastructure; IoT is connecting greater numbers of devices; and big data is gathering information on everything from telemetry readings of sensors to how many calories have been burned during an afternoon walk. The security implications among all of these elements are significant.

The sophistication of modern malware combined with the fact that our networks are more interconnected than ever means we are all vulnerable. Despite all the money spent on cyber security, networks are continually breached and the severity of attacks seems to be on the rise. That begs the question: Are we taking the right actions and investing in the right places? Also, is our security strategy in alignment with rapidly changing business needs or are we leaving our networks, endpoints and data ripe for further attacks?

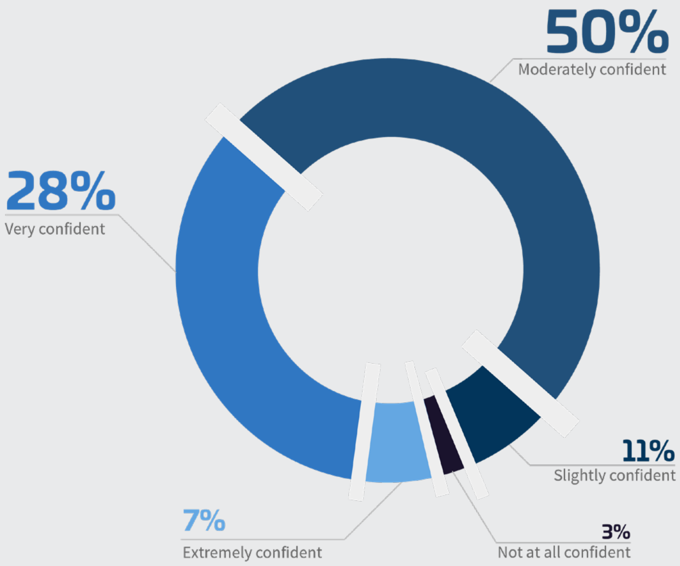
To get a better read on how businesses today are approaching the latest trends, Check Point teamed up with Crowd Research Partners to survey 1,900 IT professionals in USbased companies with 1,000 or more employees. This report explores current cyber security trends, organizations' investment priorities, and solution choices for cloud security, threat management, mobile security and more.

Q1

How confident are you in your organisation's overall security posture?

Slightly more than one-third (35%) of the respondents either feel Extremely Confident or Very Confident with their organization's security posture. More interestingly that means nearly 65% are not confident. Many organizations remain vulnerable to security breaches because they feel security is too complicated, they don't have the resources to manage security, there are too many unknowns, or they simply don't understand the ramifications of utilizing preventative security measures.

Addressing your organization's security posture means investing in the right technology, processes and procedures as well as taking the right approach. Unfortunately, many organizations simply take the wrong security approach. Utilizing multiple systems with separate management controls is costly and ineffective. A better approach to help organizations propel their business forward is where you have a single consolidated system where all threats are identified and all threats are blocked, keeping attacks outside of your network.



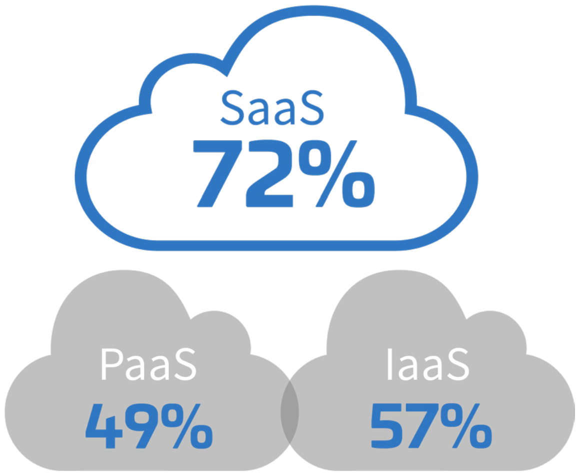
Q2

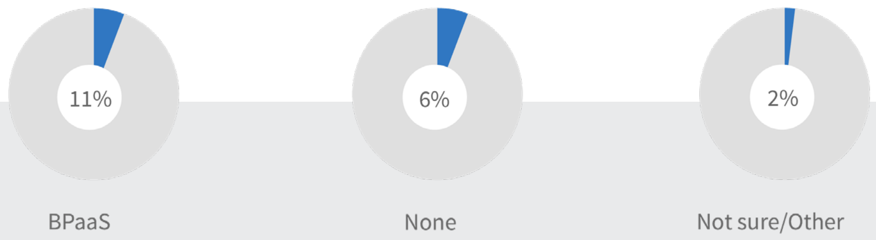
What cloud service delivery model(s) is your organisation currently using?

The need to run processes more efficiently, improve time-to-market and enhance user experience is driving more and more enterprises to embrace the cloud as part of their IT strategy. It is interesting to note that "Cloud" still has many different meanings; IaaS, SaaS, PaaS and so on. Equally interesting is the fact that enterprises today deploy a variety of cloud delivery models to streamline processes and increase agility.

IT teams usually have good visibility into and control over their on-premise networks. But when it comes to cloud environments, it's not as easy to see and react to threats. Regardless of how your organization defines "Cloud", it's important to make sure your security can adapt to your organizations' cloud strategies.

CLOUD SERVICE DELIVERY MODELS

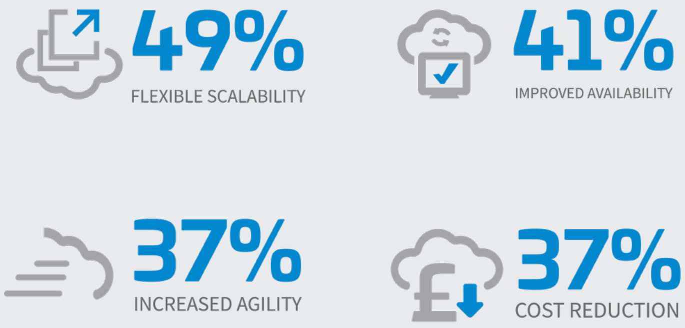


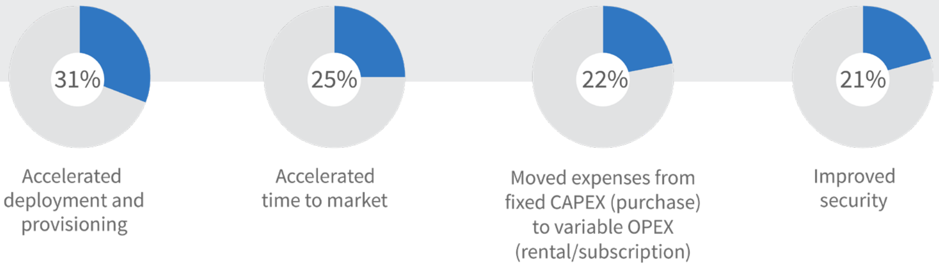


Q3

What overall benefits have you realised from your cloud deployment?

Enterprise IT is rapidly evolving from a hardware-centric to an application-centric model. This enables greater business agility to streamline processes and realize significant CAPEX savings. However, when we look closely at the benefits cited for the cloud, these are in direct contrast with how we implement network security. The changeover to cloud computing makes this a good time to rethink the security strategy needed to protect your organization's cloud assets and services as well as what this means for your role as an IT professional.





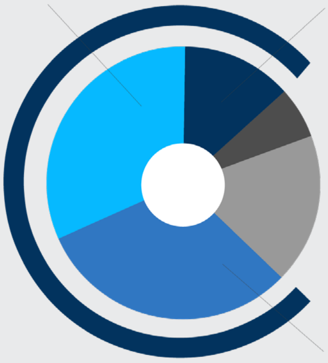
Q4

Please rate your level of overall security concern related to adopting public cloud computing.

While process efficiencies and network agility are key cloud drivers, enterprises of all sizes continually cite cloud security as their top concern. Despite this, cloud adoption continues to rise. Assets and data in the cloud are vulnerable to the same threats targeting our on-premise networks, and thus require the same level of protections.

With networks now spanning multiple providers, a comprehensive cloud security strategy must include consistent protections across all platforms with consolidated visibility and reporting to quickly respond to threats and easily comply with regulatory demands.

81% ORGANIZATIONS HAVE SECURITY CONCERNS

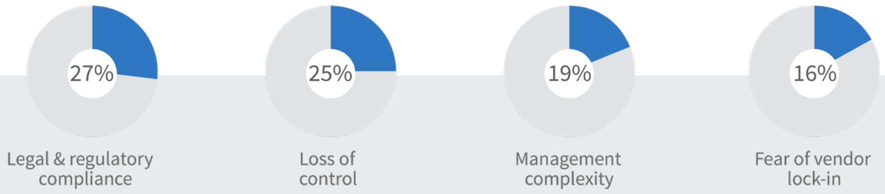


Q5

What are the biggest barriers holding back cloud adoption in your organisation?

Cloud adoption certainly provides many benefits, but enterprise security needs to adapt to this new environment. The end goal of a cloud security strategy must be to permit businesses to realize the full benefits of the cloud without letting security slow them down. Deploying an advanced threat prevention solution that seamlessly works across any cloud platform and supports native automation and orchestration capabilities will address these concerns while allowing enterprises to embrace the cloud with confidence.

34%	General security risks
32%	Lack of staff resources or expertise
29%	Integration with existing IT environment
29%	Data loss & leakage risks



Lack of maturity of cloud service models 16% | Cost / Lack of ROI 15% | None 15% | Lack of budget 14% | Internal resistance and inertia 14% | | Lack of transparency and visibility 13% | Lack of management buy-in 13% | Performance of apps in the cloud 10% | Dissatisfaction with cloud service offerings / performance / pricing 10% | Lack of customizability 8% | Billing & tracking issues 6% | Lack of support by cloud provider 6% | Availability 4% | Not sure / Other 12%

Q6

What are your biggest cloud security headaches?

Security concerns associated with moving data beyond IT control keeps many organizations from fully embracing the cloud. Enterprises want the ability to control their own data and keep it private all while maintaining compliance with regulatory mandates. The loss of visibility and manageability across all traffic and environments means internal breaches can go undetected and move unimpeded throughout your cloud. The same security protections safeguarding on-premise networks, data and workflows must also be part of a comprehensive enterprise cloud security strategy.

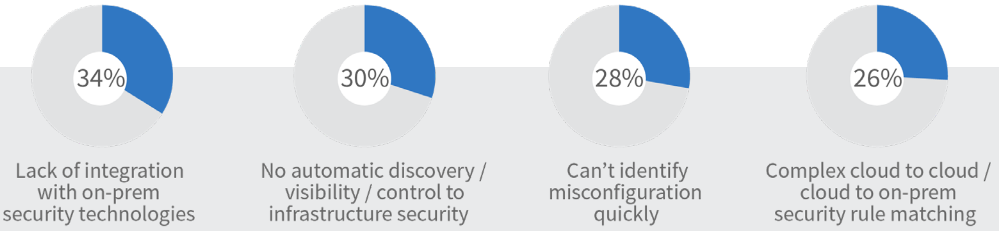
Automatically enforcing of security across multiple datacenters 26% | Lack of feature parity with on-prem security solution 19% | Security can't keep up with pace of changes to new / existing applications 18% |Remediating threats 16% | No flexibility 7% | None 7% | Not sure/Other 18%

43%
VISIBILITY INTO INFRASTRUCTURE SECURITY

38%
SETTING CONSISTENT SECURITY POLICIES

36%
CO MPLIANCE

34%
REPORTING SECURITY THREATS



Q7

What security technologies and controls are most effective to protect data in the cloud?

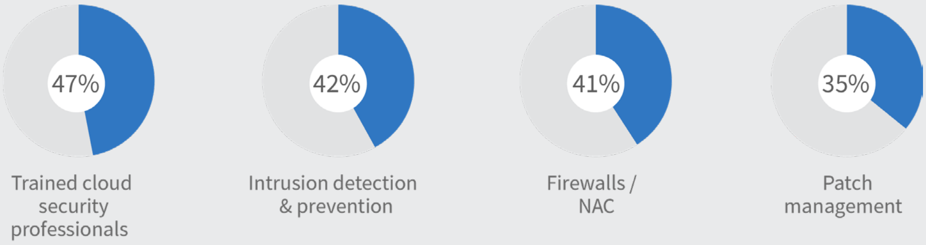
There are a number of technologies enterprises utilize for protecting their data in the cloud, chief among them is data encryption. However, encryption itself isn't a fail-safe solution. Organizations should employ comprehensive protections to ensure their data is safeguarded in the cloud from even the most sophisticated threats.

Data leakage prevention 34% | Log management and analytics 33% | Security Information and Event Management (SIEM) 33% | Network monitoring 32% | Endpoint security controls 30% | Single sign-on/ user authentication 29%Anti-virus/ Anti-malware 27% | Employee usage monitoring 25% | Cyber forensics 22%
Application security scanners 21% | Mobile device management (MDM) 18% | Database scanning and monitoring 17% | Content filtering 16% | Deception-based security 11% | Not sure/Other 12%

76%
DATA ENCRYPTION

69%
NETWORK ENCRYPTION

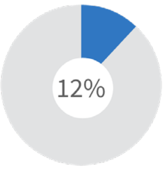
55%
ACCESS CONTROL



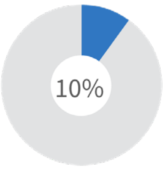
Q8

What is your biggest pain point when it comes to mobile security?

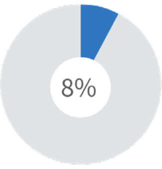
Keeping mobile devices safe from cyberattacks often requires a layered approach that fits into your existing security strategy and infrastructure. Doing so helps make sure you stay abreast of the threats you're facing in real-time so you are better prepared to stop attacks before they seize control of your data.



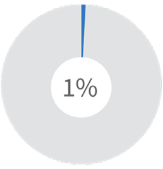
Data loss or leakage occurred



Unauthorized access to corporate data and systems



Disrupted business activities



The company had to pay regulatory fines

31%
ADDITIONAL IT RESOURCES NEEDED TO MANAGE MOBILE SECURITY

24%
INCREASE HELPDESK WORKLOAD

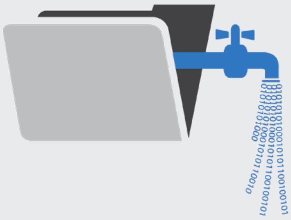
16%
REDUCED EMPLOYEE PRODUCTIVITY

13%
MALWARE INFECTIONS AND RELATED COST

Q9

What are your main security concerns related to BYOD?

Allowing your employees to use their own devices for work purposes introduces security risks. Mobile devices, when combined with personal applications, also present additional challenges over securing and managing these devices that is far more complex than corporate PCs and laptops.

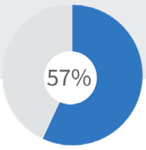


65%
DATA LEAKAGE/LOSS

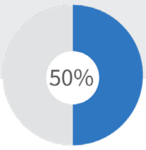
59%
USERS DOWNLOAD UNSAFE APPS OR CONTENT

61%
LOST OR STOLEN DEVICES

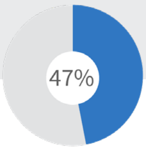
56%
UNAUTHORIZED ACCESS TO COMPANY DATA AND SYSTEMS



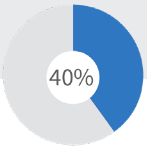
Malware



Vulnerability exploits



Inability to control endpoint security



Ensuring security software is up-to-date

Q10

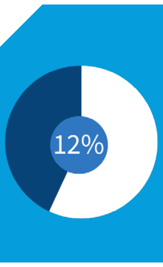
What actual negative impact did mobile threats have on your company in the past 12 months?

Attacking mobile devices is now the best way to penetrate an organization's network. Still, some organizations are either unaware or unconcerned that these attacks pose a real risk. With the sophistication and number of attacks on the rise, the impact to your business can be significant.

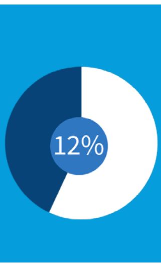
Disrupted business activities 11% | Unauthorized access to corporate data and systems 10%The company had to pay regulatory fines 2% | Other 1%

25%
ADDITIONAL IT RESOURCES NEEDED TO MANAGE MOBILE SECURITY

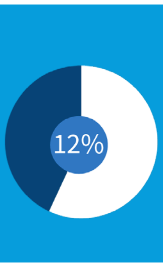
23%
INCREASED HELPDESK WORKLOAD



Data loss or leakage occurred



Reduced employee productivity

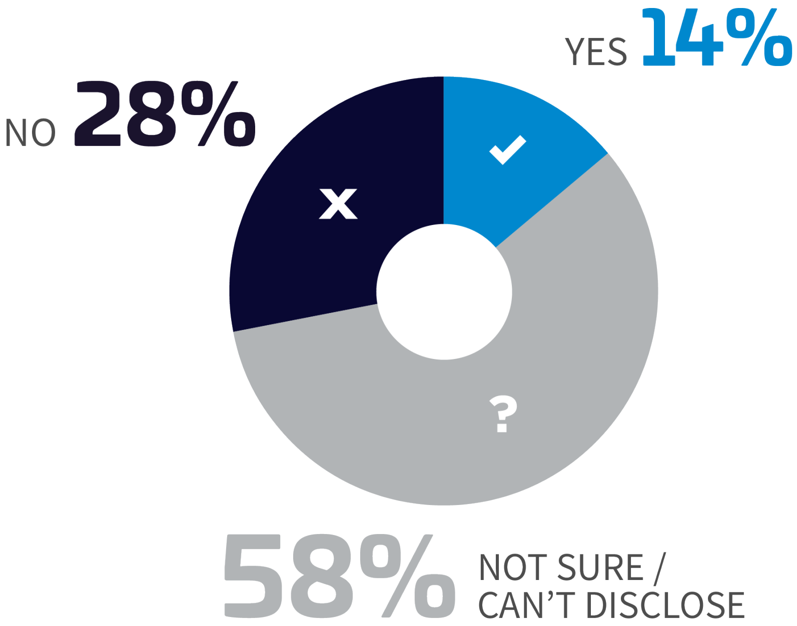


Malware infections and related cost

Q11

Have mobile devices been involved in security breaches in your organisation in the past?

Whether organizations care to admit it or not, cyberattacks on mobile devices are happening right now. Some of these attacks we know about, but many we don't. Just because you think you haven't been attacked doesn't mean you haven't – it just means you don't have visibility into your enterprise mobile security posture.

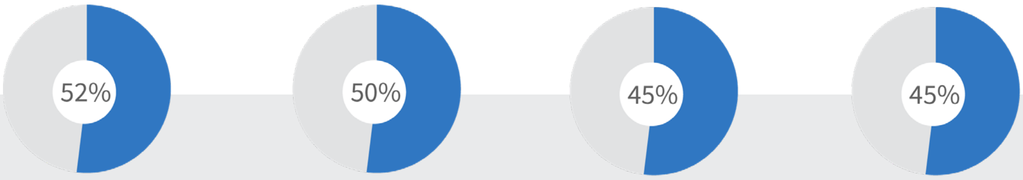


Q12

In your opinion, what key capabilities are required for mobile threat defense solutions?

PCs and laptops are different animals than smartphones and tablets. So it's no surprise that keeping these devices safe requires a different approach than traditional network security often provides.

68%
MALWARE PROTECTION



Vulnerability exploit defense

Device configuration

Role-based access control

Integration with other Endpoint Management System

64%
LOGGING, MONITORING AND REPORTING

58%
EASE OF DEPLOYMENT

54%
NETWORK / WIFI ATTACK DEFENSE

With IoT, mobile, and cloud reliance, we gain great benefits but also are more at risk.

Yet, many businesses don't understand the danger and want to simply upgrade what's already in place.

The sophistication of modern malware and tactics used by hackers means we are all vulnerable. It's time to take a different view and build the security architecture of a future that is already underway.

Check Point provides an architecture and solution set that addresses the full spectrum of threats from on-premises to mobile to cloud. This comprehensive approach is designed to help you secure any environment you operate in—while keeping attacks outside your networks.

Get in touch to find out what your business needs to keep data private and protected.