ccs insight

Modernising IT Security

with Cloud Device Computing Platforms

September 2018

In conjunction with

Google Cloud

Contents

Executive Summary

Data security has become more challenging than ever in the modern enterprise. The accelerating use of cloud applications and mobile devices by today's cloud workers has eroded the traditional security perimeter of the enterprise and with it, the control of company data.

Weak security is a costly business: reputation-damaging data breaches are now headline news and strict legislation in the form of Europe's General Data Protection Regulation (GDPR), which carries significant financial penalties, is now in force.

IT decision-makers have therefore made security their top priority in 2018. In CCS Insight's survey of IT decision-makers conducted with Samsung in 2017, half of respondents listed cybersecurity as one of their top three challenges. In fact, 58 percent of respondents said that data security is now a high priority in their company's overall business strategy.

Facing a daunting combination of external and internal IT security challenges, as well as a need to deliver a high-quality employee experience, organizations are re-evaluating their strategies for IT security and device computing. In this report, we highlight the advantages of cloud-based operating systems and devices as important elements of modern workplace security. CCS Insight estimates there are still more than 300 million PCs over four years old in businesses; cyberattacks that exploit vulnerabilities in ageing systems are on the rise.

Cloud device platforms will help organizations overcome some of the most significant security and administrative challenges. They can meet the widening range of security requirements faced by most organisations and improve on the inflexible and monolithic systems of the past. Above all, they will help ensure that highly mobile cloud workers have a better, more productive and secure experience of the digital workplace.

This report aims to be a practical guide for CIOs, IT security managers and device purchasers responsible for the future of workplace technology and security in their organizations. It examines the principles of cloud-based device platforms, the security challenges they can help overcome and the new protections they deliver.

With customer examples and practical recommendations, the report should be an educational prompt to implement the technologies, partnerships and business processes needed to capture the security benefits offered by these computing platforms.

The External Threat Environment

Changing Work Styles and the Rise of the Cloud Worker

Over the past decade, the rise of mobile working — defined as spending at least 25 percent of work time away from a primary workplace — has meant that technology has evolved from stationary employees working on desktops and laptops provided by the IT department to a cloud-connected and mobile-centric model that spans a diverse mix of personal and company-owned apps and devices.

This has naturally fuelled a high dependency on mobile and cloud technology in the workplace over the past few years. According to CCS Insight's survey of employees in four countries in 2017, 86 percent of employees believe mobile technology has a positive impact on their overall performance, with almost half stating it has a "substantially positive" effect.

We estimate that 48 percent of the white-collar workforce in developed nations will be classified as mobile, cloud workers by 2020.

Where's Waldo or Wally?

These changes, however, have also given rise to trends that have rendered IT security one of today's biggest business challenges.

Cloud security firm Netskope estimates that 98 percent of Fortune 500 companies were affected by malware in 2017 and 69 percent were hit by phishing attacks. CCS Insight's survey of IT decision-makers conducted with Samsung in 2017 found that a huge 87 percent of respondents said their company devices had been infected with viruses. And 45 percent said it was likely their organization would be hit with a cyberattack within the next 24 months.

An increasing amount of corporate data now travels outside the corporate firewall thanks to cloud working; for most firms, identifying and remediating cyber-threats feels like a "Where's Waldo?" or "Where's Wally?" image: a "needle in the haystack" affair, difficult to solve with current resources and technology.

Here we identify the main challenges, both external and internal, that businesses face with data security. Collectively they are prompting IT departments around the globe to rethink their device computing strategies.

The Rise of Digital Sprawl and Unmanaged Apps

As mobile and cloud working continues to accelerate, one of the most significant trends in enterprise technology over the past few years has been growth in employee access to third-party cloud applications like Microsoft Office 365, Google G Suite, WhatsApp and Dropbox on corporate devices.

CCS Insight's research has found that on average, employees used between six and seven mobile cloud apps for work purposes in 2017, an increase of about 50 percent on 2016. The average number of connected devices used by employees for business or personal purposes is 4.8, up from 4.6 in 2016. Okta, a provider of identity management software, reports that in 2016 its customers in the technology sector increased their use of cloud apps by 27 percent.

Unscrupulous app developers prey on these trends and users that don't understand the risks associated with downloading apps. Although rogue or harmful apps are small in number, it only takes one employee to install an infected application to put the organization in jeopardy. Risk is magnified when applications are unmanaged by corporate IT departments; CCS Insight estimates that more than half of the mobile apps used at work are unmanaged.

New Compliance

European businesses are rapidly making security changes as the GDPR comes into force in May 2018. One of the key motivations for the regulations, as stated by the authors of the GDPR, is the impact of the rising number of mobile devices such as laptops, tablets and smartphones.

GDPR is built on the premise that data should be private and that individuals have rights regarding their data. This area has gained prominence in the US following reports that allege Cambridge Analytica abused a loophole in Facebook, allowing it to harvest data from an estimated 50 million people without their consent, and then target voters with messages supporting Donald Trump's campaign in the US presidential election. The GDPR seeks to regulate such data interactions and the incidents surrounding Facebook indicate that similar legislation will arrive in the US in the future.

A key requirement of the GDPR is that companies must report any loss of customer data within 72 hours of discovery. High-profile attacks, like the breach of customer data at Equifax in 2017, in which customer data of 147 million people was exposed, are more likely to be prevented in the wake of the legislation as companies improve their data governance to comply with the regulation.

The GDPR is a catalyst for not only improved security, but also enhanced data governance thanks to greater investment in IT. Companies that plan to simply comply with the regulation are likely to miss an opportunity to transform their IT operations.

Increasing Financial and Reputational Costs

Perhaps most importantly, the cost of having poor security procedures is mounting. The World Economic Forum estimates that cybercrime currently costs the global economy $445 billion a year.

Danish transport and logistics conglomerate Maersk stated in its second-quarter financial report in August 2017 that the NotPetya attack in 2017 had cost the firm between $200 million and $300 million.

GDPR brings the potential for further costs, with fines of up to €20 million or 4 percent of global annual turnover, whichever is the larger, in the event of a serious data breach.

Top-level employees are not immune to potential reputation-damaging social engineering attacks. A good example of this is Barclays CEO Jes Staley, who admitted he had fallen for a relatively simple e-mail hoax in 2017.

The Internal Security Challenge

Adding to the challenges brought on by changes to the external security and compliance environment are significant security barriers within companies.

Legacy Technology

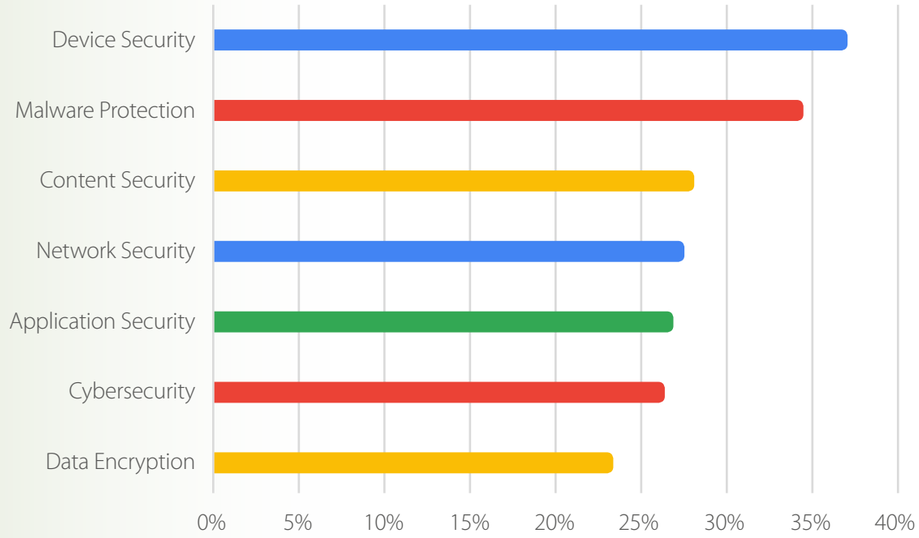
Part of the fabric of operations inside most businesses — and in many cases performing critical tasks — older technology systems often pose security risks to companies as they can form an attractive target for hackers.

Nowhere is this more evident than when it comes to company devices. CCS Insight estimates there are more than 300 million corporate PCs in use that are over four years old. As the ransomware attacks of NotPetya and WannaCry in 2017 illustrated, it is often older, unpatched devices and systems that are the most vulnerable to cyberattacks.

In addition, IT departments typically administer devices with older management tools and processes. These can involve time-consuming and often manual procedures to set up devices, configure software and maintain antivirus protection. All of these can inhibit response times when problems occur.

Ageing technology is often a drain on dwindling IT resources. CCS Insight estimates that IT departments spend as much as 85 percent of their time and resources just "keeping the lights on", performing such activities as handling support problems and maintaining infrastructure, rather than devoting efforts to new projects that drive growth and transformation.

Unsurprisingly, priorities are shifting for security in most organisations as a result of these trends. When CCS Insight asked IT decision-makers about their highest priorities when buying mobile security technology, device security was top of the list, followed by malware protection and document security. These areas reflect some of the most significant security concerns in organizations at the moment.



What are your top three priorities when buying mobile security technology?
Sample: 403

A Half-Hearted Policy

One way companies are trying to combat a reliance on legacy systems and save money is by tolerating more personal devices and applications being used in the workplace. However, increased tolerance has not been matched by an increase in security policy to support the use of these devices. CCS Insight found that just 54 percent of workplace devices in use in organizations are managed at a corporate level; that is, using security and management software and corporate policies.

This half-hearted approach to security policy poses some important challenges under the GDPR. Many companies regard staff as the biggest threat to GDPR adherence, as it is natural that employees will lose company devices, unwittingly use an insecure Wi-Fi hot spot or download content or apps from inappropriate sources.

As employees increasingly use a mix of personal and company devices as if they were their own, the potential for loss of personal or company data is heightened. In a post-GDPR world, this potential carries a significant financial risk.

Getting the Balance Right

A common challenge with IT security for most organizations has been finding the right balance between protecting corporate data and allowing employees to be as productive as possible while on the move. However, as we highlight in this report, organizations can no longer afford to compromise security.

Additionally, evaluating solutions can be tricky. Firms must understand the necessary trade-offs between securing corporate data and the potentially negative impact this can have on employee efficiency.

Companies must also address growing employee privacy concerns, especially when it comes to supporting personal technology in the workplace. CCS Insight's survey of workers in Europe and the US found that 63 percent of employees said they would be concerned for their privacy if their company made them install security software on a personal device used for work.

Cloud Device Computing Platforms

CCS Insight believes that organizations can overcome these challenges over the next 12 to 18 months by redesigning their end-user computing environment to support cloud-based operating systems and devices. Doing so can bring a wide and evolving range of management, security and cost benefits to businesses.

Unlike traditional PC client systems, these computing platforms are designed for the cloud, offering a consistent flow of new features that help ensure today's highly-mobile cloud workers have an improved and more productive experience of the digital workplace.

CCS Insight has identified five key principles of cloud-based device computing platforms and the benefits they deliver. Collectively, they form a critical aspect of the future of end-user computing and IT security inside organizations.

Connected

Cloud-based operating systems and devices are designed to meet the connectivity and experience needs of employees. "Always on", with regular, automatic updates and a flow of new features supplied from the cloud, they are fast, lightweight and reliable. These enhancements improve performance and they protect against device obsolescence and problems such as costly PC crashes.

Scalable

One of the unique advantages for IT administrators is that cloud-based device platforms are highly scalable in terms of management. They offer centralised device management for set-up and configuration and include a range of PC management and policy enforcement features that work at user, group and organization levels, as well as device, application and network management scenarios. Importantly, they also integrate with existing IT security infrastructure such as identity management and VPN systems.

Perhaps their most significant capability is that they deliver regular and automatic system updates. These ensure device fleets are up to date and running the latest features and security patches, which enables greater IT flexibility and cost savings. CCS Insight estimates that devices running cloud-based operating systems could reduce traditional PC management costs by as much as 40 percent.

Flexible

Cloud-based devices serve a wide variety of enterprise usage scenarios, adding flexibility to an organization's device strategy. Employees can securely sign into their individual profile to access corporate information on any supported device, opening up opportunities for shared computers, kiosks, single-task and specific devices all on a single platform. This can help the repurposing of devices, reduce the number and type of devices owned and lower hardware costs.

Total Cost of Ownership

Cloud-based operating systems and devices offer significant business value in the form of improved productivity, cost reduction and efficiency. CCS Insight has observed some organizations achieving more than 300 percent return on their investment within three years through a commitment to cloud-based device platforms. In some instances, they have also lowered their device costs by as much as 60 percent and reduced traditional PC management costs by as much as 40 percent.

Secure

On the back of the WannaCry, Spectre and Meltdown incidents over the past year, there is a mounting perception that devices running older operating systems could be creating significant security gaps in organizations. Unsurprisingly, device security has therefore become the top priority for security in most organisations.

One of the most attractive principles of cloud-based device platforms is that they can help companies overcome many of the security obstacles we highlighted earlier in this report with a range of security and administration features that span hardware, the operating system and applications.

- **Hardware:** devices with cloud-based operating systems have specific security features embedded into their firmware. They include dedicated processors for protecting credentials, verified boot with partitioning to protect against malware, single-button factory reset, full disk encryption and cryptographic-based device verification that secures access to company network resources such as VPN gateways, certificates and Wi-Fi networks.
- **Operating system:** operating systems offer "sandbox" features and deliver regular, automatic background updates to ensure the most secure version of the platform is always running. There are also native device management controls such as lock-and-wipe, enforced device enrolment and controlled access to Web resources.
- **Applications:** cloud-based systems also support sandboxed applications and security features including application whitelisting and blacklisting, blocking the side-loading of software, malware detection, inspection and removal, and safe browsing. They also offer reporting features to improve visibility of applications and Web sites accessed on the device.

Security Benefits

Companies looking to modernise and improve their IT security environment will gain several important benefits through the deployment of these platforms:

- **Automatic up-to-date security:** Cloud-based platforms ensure companies stay ahead of latest security threats by taking advantage of regular, automatic system updates that deliver the latest security patches and features, often within 48 hours and on devices that can be supported for more than five years.
- **Minimising malware:** The ongoing prevention, detection and removal of malware are a core tenet of the design of modern cloud-based operating systems. Although no computing platform is impervious to cyberattacks, cloud-based systems enable IT departments and users more controls and agility in responding to and remediating the impact of malware.
- **Usable security:** Most importantly, unlike traditional antivirus software for instance, the automatic security embedded in these platforms offers little to no friction for users of the devices. This makes it much easier for workers, especially non-technical employees, to protect data against the latest security threats without compromising their productivity or device experience.

A good example of a company gaining the benefits of cloud device computing platforms is a retail customer that recently deployed Google Chromeboxes in its branches to display advertising. The devices replaced older, unreliable hardware that required significant manual configuration. The rollout of the new Chrome devices delivered improved device reliability, significantly lowered management and administration overhead and improved the organisation's security. In fact, the devices were so secure during their testing process that the company's security teams had to physically take the Chromeboxes apart to do any damage to them. The firm is now looking at expanding their device roll out to enable kiosks in its branches as the next phase.

Recommendations

Changes in work styles, driven by the rise of cloud and mobile working over the past few years, have rendered IT security as one of today's biggest business challenges. In reality, for most firms, identifying and remediating cyber-threats feels as difficult as finding Waldo or Wally: a seemingly impossible task that can't be achieved with dwindling resources and ageing technology.

However, as this report reveals, modern, cloud-based device computing platforms can be an effective solution to major security problems. These platforms can ensure usable, always-up-to-date protection as well as administrative flexibility and financial value to an organization.

Above all, they can also help ensure that today's highly mobile cloud workers have an improved, more productive and secure experience of the digital workplace.

To be successful and maximise their return on investment, IT decision-makers should follow our top four recommendations for end-user computing strategies.

Prioritize a secure user experience for cloud workers

The user experience will determine whether workplace device strategies succeed or fail. Evaluate devices and platform technologies that can simultaneously improve and offer the right balance between a productive user experience and robust security.

Improve security by accelerating PC upgrades

With support for Windows 7 coming to an end in early 2020, attacks on older operating systems on the rise and the GDPR now in force, all organizations must accelerate PC upgrade cycles to improve IT security.

Consider the advantages of cloud-based operating systems and devices as a means to continually improve organizational security. Select suppliers with experience across a broad range of enterprises and vertical markets. Leading platform suppliers should be able to offer education, best practices and new technologies that help companies strike the right balance between user experience and robust security practices.

Consider device platforms that deliver in three key security areas

Any potential solution must be evaluated in three key security areas: long-term support for regular, automatic updates with new security features; the ability to rapidly minimize the threat posed by malware; and security features that don't impede employees' productivity.

Look for frictionless security embedded into platforms that makes it much easier for workers, especially non-technical employees, to protect data from threats without compromising their productivity or device experience.

Train employees on security risks

Simple but effective security, although a requirement for users, is not enough to fully protect an organization. Take the opportunity to educate employees about security. Many businesses do not do enough to train employees about cybersecurity risks. Training is important for all organizations because employees are the most critical line of defence.

Formal and regular education about the risks of handling customer data is not only essential for data security but also for compliance with legislation like the GDPR.

WWW.CCSINSIGHT.COM

CONTACT US

For EMEA sales, please contact:
+ 44 7766 447744

For US sales, please contact:
+1 408 886 1745

info@ccsinsight.com

@ccsinsight