

# Redesigning Computing

for the Cloud Worker and Digital Workplace

July 2018

In conjunction with

Google Cloud

# Contents

# Summary

## **Competitive uncertainty, changing employee work styles and increasing demands on productivity have forced many organizations to re-evaluate their strategies for workplace IT and device computing.**

In addition, new requirements to improve security and compliance have given greater urgency to these endeavours. 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 the rise; and new legislation in the form of Europe's stringent General Data Protection Regulation is now in force.

In this report, we highlight the advantages of cloud-based operating systems and devices as a part of a modern approach to end-user computing. As important elements of workplace IT in the future, cloud device platforms will help organizations overcome some of the most significant security and administrative challenges, and usher in new forms of business value. Above all, they will help ensure that today's highly-mobile cloud workers have an improved and more productive experience of the digital workplace.

This report aims to be a practical guide for CIOs, IT managers and device purchasers responsible for the future of workplace technology in their organizations. It examines the principles of cloud-based device platforms, the market drivers and the challenges that such platforms can help companies to overcome.

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

# Introduction

## **Reimagining Workplace Technology for Competitive Advantage**

Companies face more and more challenges in today's digital economy. The accelerating pace of technology continues to transform business models, blur industry boundaries, and give rise to new, at times unforeseen, competitive threats.

Customer insights, employee engagement and operational excellence have become more important than ever. Firms with motivated employees that can implement better and faster decisions have a better chance of gaining competitive advantage in this uncertain climate.

The demand for greater productivity has also radically changed employees' working styles, fuelling a high dependency on mobile and cloud technology in the workplace. 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.

Additionally, CCS Insight's survey of IT decision-makers, conducted in November 2017 in conjunction with Samsung, found that 85 percent of companies in the US and Europe are using cloud services in their organizations, with 27 percent of the total using the cloud for all applications. One third of these cloud-only firms said their employees were "extremely productive" as a result, three times more than the proportion among companies that used cloud services for only some applications or did not use them at all.

More than ever, CIOs and IT leaders are realizing they must create competitive advantage by reimagining their workplaces. They need new IT strategies that ensure operational excellence, security and administrative flexibility but also meet the financial demands of their organization. Crucially, they need employees, today's cloud workers, to have an improved and more productive experience of the digital workplace.

Organizations are now looking to meet these requirements by redesigning their end-user computing environments to support cloud-based operating systems and devices. The rewards that organizations can reap through this approach to computing can be substantial. As this report highlights, organizations using this strategy have not only improved IT security and employee satisfaction levels, they have also lowered device costs and achieved a significant return on their investment.

# The Challenge

Most businesses struggle to achieve the heights that can be attained by the adoption of modern workplace technologies. CIOs are constrained, having to balance the conflicting needs of the organization and its employees as well as servicing new business requirements. And they often have to do so with yesterday's technology.

As a result, workplace IT projects have tended to grapple with tactical problems, such as working with a range of different devices, how to manage them or draw up policies, rather than enabling workflows or reinventing processes that improve productivity, collaboration and strategic value.

This reality is largely the result of several significant IT challenges that currently hold back many organizations. Here we outline four of them: legacy technology, budget constraints, a poor employee experience, and security.

## Legacy Technology

Most companies have ageing IT infrastructure, back-end systems and entrenched processes that can form operational barriers to bringing innovation to business processes and employee technology. Nowhere is this more evident than when it comes to company PCs and operating systems.

CCS Insight estimates there are more than 300 million PCs being used inside organizations today that are over four years old. According to our surveys, firms most typically replace company laptops every three to four years.

IT departments typically administer these devices with older management tools and processes. These can involve time-consuming procedures to set up devices, configure software and maintain antivirus protection, for example.

CCS Insight estimates there are more than **300 million** PCs being used inside organizations today that are over **four years old**.

## Budget Constraints

Enterprise IT budgets continue to be squeezed as IT teams face the challenges of simultaneously needing to invest in modernizing systems and adding innovation to the business, all while maintaining legacy infrastructure.

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 issues and maintaining legacy infrastructure, rather than devoting efforts to new projects that drive growth and transformation.

## Employee Experience

It is partly because of these challenges that a staggering 36 percent of employees responding to CCS Insight's Employee Mobile Technology Survey, 2017 felt their IT department was out of touch with their workplace technology needs.

The inability of corporate IT departments to deliver a workplace technology experience that matches employees' use of technology in their personal lives has been a long-standing weakness. It has been exacerbated by the rapid adoption of cloud services and mobile apps over the past few years, often outside company policy. Many firms have simply been unable to keep up with an ever-evolving set of personal productivity requirements while guaranteeing security and compliance.

a staggering **36 percent** felt their *"IT department was out of touch with their workplace technology needs."*

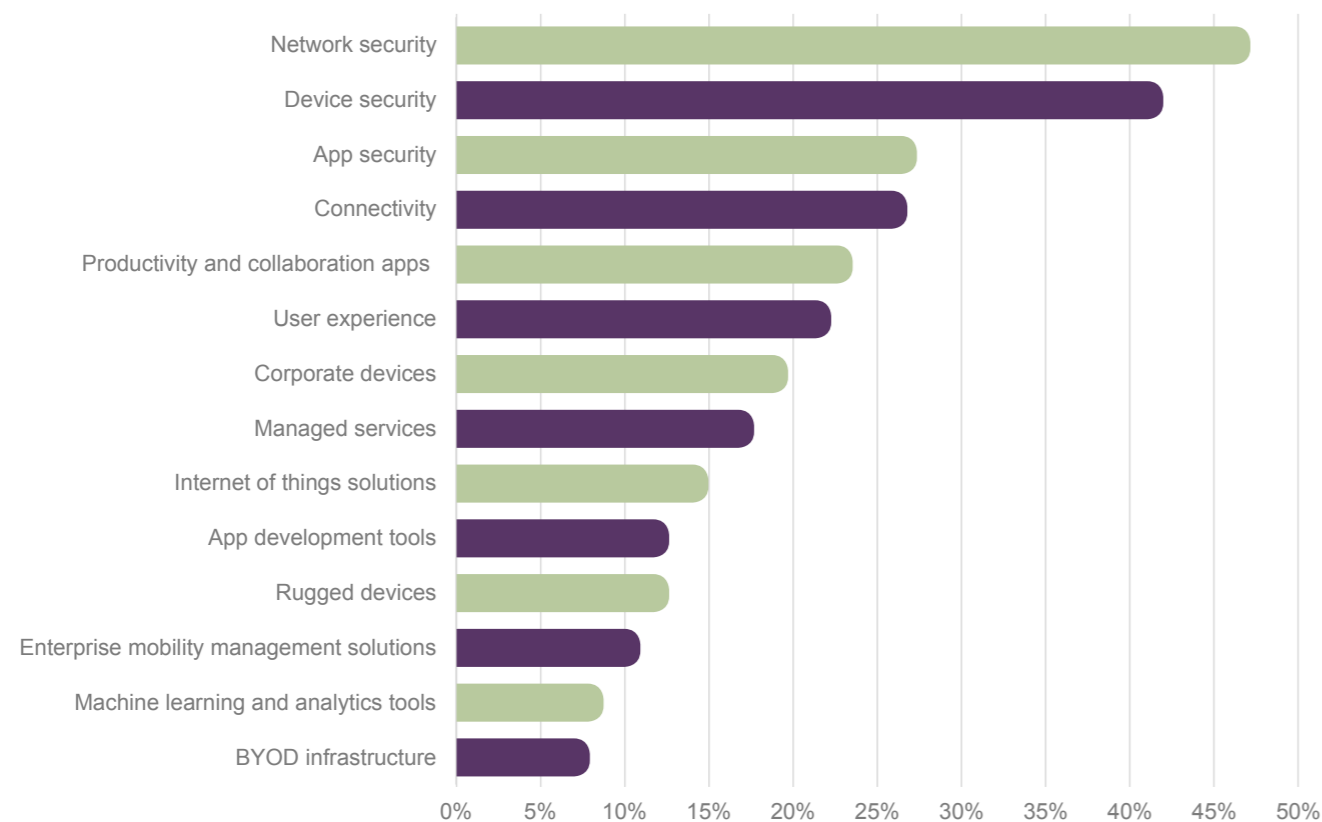


## Security

Security concerns have hit fever pitch over the past year in the wake of several high-profile incidents, including the Equifax data breach, WannaCry ransomware attack and the revelation that many PC processors are prone to the Spectre and Meltdown vulnerabilities.

The European Union's new General Data Protection Regulation also came into force in May 2018, with the threat of fines of up to 4 percent of global turnover for companies that fail to protect customers' data in the event of a breach.

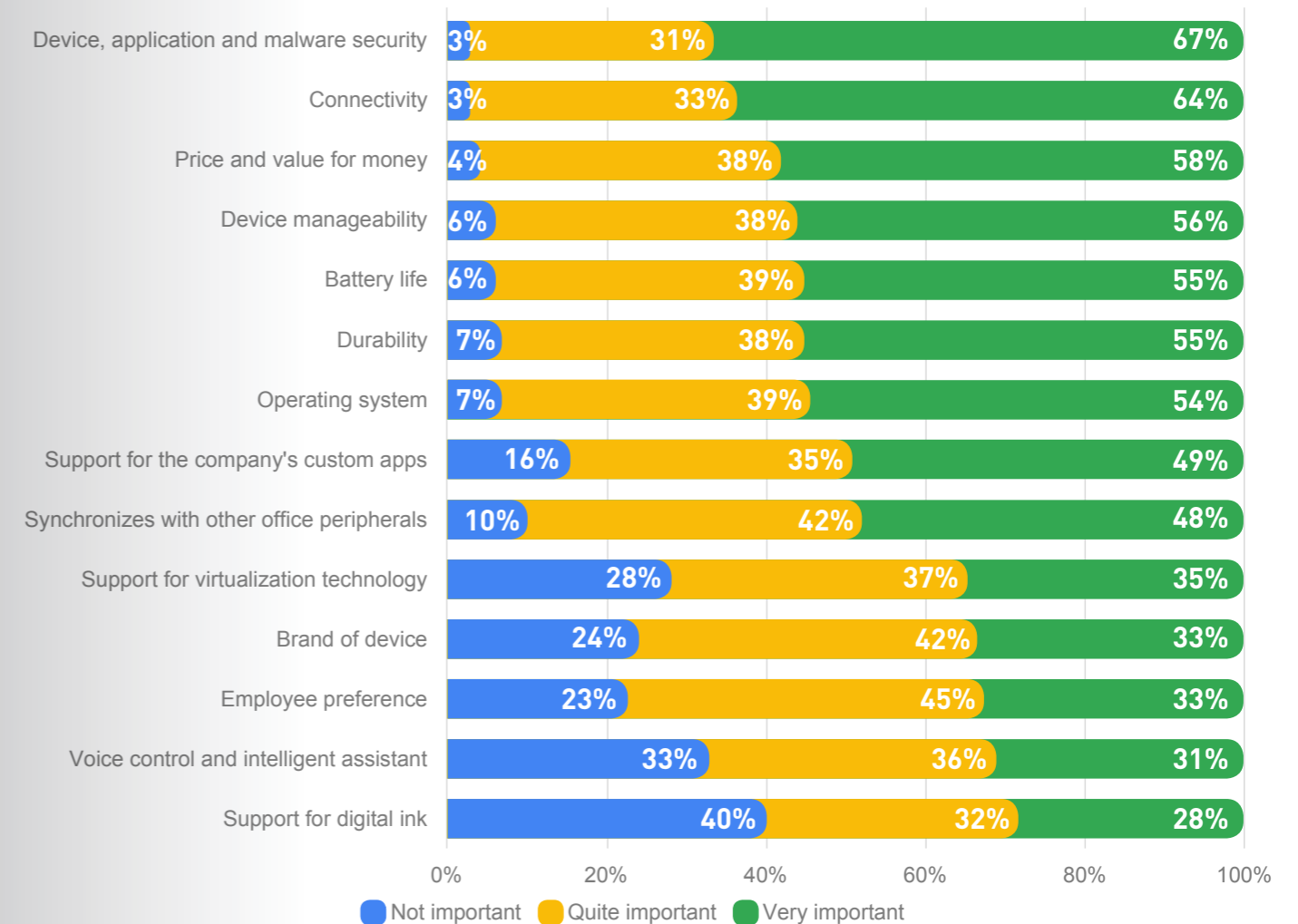
Unsurprisingly, security has become the single biggest barrier to investment in digital workplace technology. In CCS Insight's survey of IT decision makers in 2017, 50 percent of respondents listed cybersecurity as their biggest challenge. Security is also the top investment priority, with particular emphasis on network, device and app security solutions.



### What are the most critical areas of enterprise mobility you plan to invest in over the next 12 months?

Source: CCS Insight Decision-Maker Mobile and Digital Workplace Technology Survey, 2017

Security is also heavily shaping requirements for company devices. In our survey of IT decision-makers, it emerged as the most important factor when purchasing mobile hardware, usurping previous factors such as cost, battery life and connectivity. Two-thirds of IT decision makers said device, application and malware security was a very important factor when purchasing company devices. This was followed by connectivity (cited as important by 64 percent) and value for money (58 percent).



In our past surveys, respondents have regularly cited security as a major barrier and overriding challenge in a range of business operations. We believe there has been an even sharper focus on this theme in 2017, reflecting the concerns of IT buyers responding to recent high-profile security breaches and upcoming regulatory changes.

In fact, 58 percent of respondents to our November 2017 survey of decision-makers conducted with Samsung said that data security is now a high priority in their company's overall business strategy, illustrating the importance of this topic to enterprises.

# The Solution: Cloud Device Computing Platforms

**CCS Insight believes organizations will overcome these challenges over the next few years and advance their workplace IT strategies by redesigning their end-user computing environment to support cloud-based operating systems and devices.**

Unlike traditional PC client systems, these computing platforms are designed for the cloud, offering a consistent flow of new features aimed at improving the computing experience and work styles of today's highly mobile cloud workers. They also bring a wide and evolving range of management, security and cost benefits to businesses as well.

Cloud-based device platforms are accompanied by a mix of shareable and specific devices. These can be deployed flexibly for a number of uses within businesses, including laptops for knowledge workers, kiosks and digital signs for marketing and customer experience scenarios, and single-task devices for field service workers, for instance.

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 workplace IT inside organizations.

## Connected

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

Employees' expectations for their workplace technology are heavily conditioned by their interactions with consumer technology that can often be superior. According to CCS Insight's 2017 survey of employees, weak Internet speeds and poor connectivity are the biggest frustrations with company technology.

Cloud-based operating systems and devices are designed to address these trends. "Always on", with regular, automatic updates and a flow of new features supplied from the cloud, they are fast, lightweight and reliable. They offer performance improvements owing to these enhancements and they protect against device obsolescence and problems such as costly PC crashes, for example.

## 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 basic set-up and configuration and include a range of PC management and policy enforcement features that work across user, group and organization levels as well as device, application and network management scenarios. Importantly, they also integrate with existing IT infrastructure such as identity 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. We estimate that traditional PC management costs with devices running cloud-based operating systems can be reduced by as much as 40 percent with these capabilities.

## Flexible

Cloud-based devices serve a wide variety of enterprise usage scenarios as well, 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.

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

We estimate that traditional PC management costs with devices running cloud-based operating systems can be reduced by as much as **40 percent** with these capabilities.

**87 percent**

of respondents said they had company devices that had been hit by viruses.

## Secure

As we highlighted earlier, security is currently the most critical digital workplace challenge and the top IT requirement when purchasing devices. On the back of the WannaCry, Spectre and Meltdown incidents over the past year, there is a mounting perception that devices with older operating systems could be creating security gaps in organizations.

According to the survey of IT decision-makers conducted with Samsung 2017, 87 percent of respondents said they had company devices that had been hit by viruses. Additionally, 45 percent of enterprises stated they felt it was likely their organization would be hit with a cyberattack within the next 24 months, with 38 percent of the total claiming an attack would have a moderate or major impact on their organization.

Cloud-based device platforms can help companies overcome key security obstacles 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 the firmware. These include dedicated processors for protecting credentials, verified boot with partitioning to protect against malware, full disc 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 support 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.

## Total cost of ownership

Above all, cloud-based operating systems and devices offer significant business value in the form of improved productivity, cost reduction and efficiency. Businesses often make device purchases before fully understanding how investments deliver value. CIOs, IT managers and device purchasers must continually measure the benefits against business objectives.

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.

Some organizations achieve more than **300 percent** return on their investment within three years through a commitment to cloud-based device platforms.



# Recommendations

## More than ever, CIOs and IT leaders are realizing that they must drive competitive advantage and adapt to changing work styles by reimagining their workplaces.

Even though many organizations are still at an early stage in this journey, the case study presented in this report and many other examples have shown that cloud-based operating systems and device computing platforms can help enterprises overcome major technology challenges and be the source of significant business value.

We believe modern platforms such as Chrome OS presented in the case study can address the widening range of computing preferences and work styles of today's highly mobile cloud workers. They also significantly improve on the inflexible and monolithic systems of the past, ensuring better security, operational excellence and administrative flexibility, as well as financial value to the organization.

Ultimately, the advantages of cloud-based device computing platforms can become a crucial factor in enabling competitive advantage and a modern, digital workplace. To be fully successful, IT professionals must consider our top three recommendations.

## 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 stronger legislation in the form of Europe's General Data Protection Regulation, all organizations must now 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.

## Prioritize the user experience

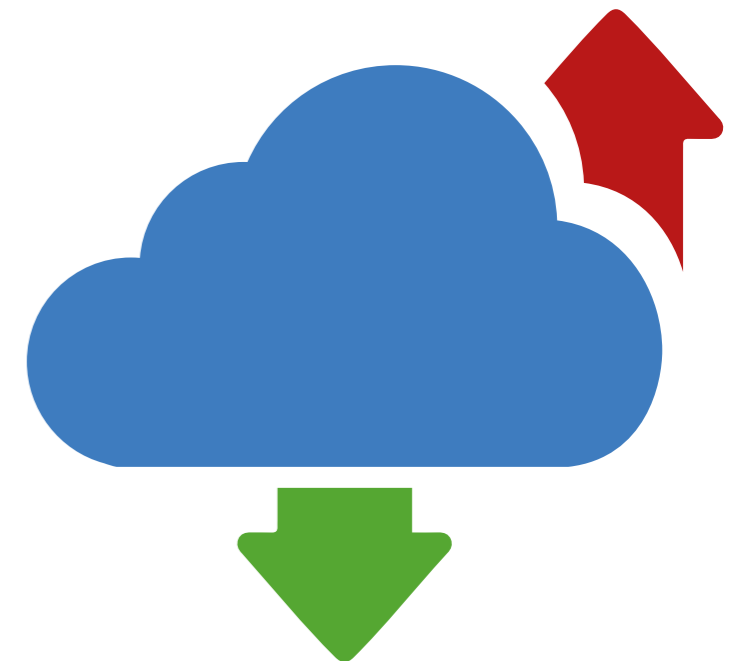
Ultimately, the user experience will determine whether workplace device strategies succeed or fail.

Evaluate devices and platform technologies that will affect the employee experience over the next two to three years. Consider a solution that delivers consistent performance improvements and addresses some of the key areas where employees express frustration today such as connectivity, speed and reliability.

## Invest in a flexible device platform to support the digital workplace

All organizations must prioritize device functions that make employees more productive on the move. However, also consider the ability of specific device platforms to address additional workplace technology uses and scenarios beyond knowledge workers as well. Additional areas that can reduce cost and improve return on investment include shared devices, kiosks, digital signs and single-purpose device scenarios.

Platforms that can address a flexible range of deployment scenarios while improving security and manageability will prove more advantageous in the long term.







[WWW.CCSINSIGHT.COM](http://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](mailto:info@ccsinsight.com)

 [@ccsinsight](https://twitter.com/ccsinsight)