DXC.technology

Industry Perspective

Better workplace or better security?

Companies can choose both.

In modern workplace management, we connect authenticated users securely to enterprise information and provide analytics (reports) to the customer (corporate).

Since the introduction of the mainframe, companies have been following a long, twisting road to the digital enterprise. Employees, for the most part, have been pulled along that path, using whatever tools and technologies their company deemed suitable to offer. Sometimes for the better, sometimes not.

That's no longer the case. Converging forces of mobility, cloud and digital devices are shifting control of workplace technologies and tools to employees. As David Moschella, a research fellow at the Leading Edge Forum, explains in his book *Seeing Digital*, individuals are taking charge of the digital workplace. More than ever, he notes, employees make the call on what kind of workplace experience a company must deliver, the devices and software they'll use, and the time and place in which they'll use it.

That level of personalization is achievable by any company, and in an age of competition for skilled workers, highly necessary. For companies, the bigger challenge is: Can it be done securely? The choices that employees make to achieve a personalized experience should not compromise security. Likewise, security should not hinder the experience. But to do that, security can't be just bolted on. It must be an integral part of the workplace experience.

The digital workplace answers the fundamental question of how to secure enterprise data without compromising the user experience.

Shifting the security perspective

The traditional approach to security had us put up barriers to "keep out the bad guys." In a modern context, that only creates barriers that legitimate users must overcome — multiple layers of authentication, verification, etc. — which has a detrimental effect on their experience.

Rather than presuming that we can keep all users, devices and internal networks safe, the modern workforce makes us face the challenge from a different point of view. We must ensure users requesting corporate data are authorized to do so and can access it in a trusted way that keeps data under corporate control.

To emphasize the importance of this new paradigm, in the new style of workplace management, devices, software and the network are secondary. In modern workplace management, we connect authenticated users securely to enterprise information and provide analytics (reports) to the customer (corporate).

To better understand this interplay, here's an example:

Meet Sally. Sally is a salesperson for Garth Enterprises, a company in the future that offers a digital workplace for its employees. In her home office, Sally prepares a presentation for one of her customers, collecting material from the Garth corporate network, browsing related customer presentations and related offerings.

Throughout all of this, Sally is not challenged (at least not that she notices) because her use conforms to four of the five trust principles of security:

- Something physical she has (in this case, a trusted computer)
- Who she is (she has been identified by facial recognition)
- Where she is (she is working from her usual location, a trusted home network)
- How she behaves (Sally is working during her normal business hours and the corporate data she's using is in line with her historic behavior)

What about the fifth principle of security — something she knows, like a password or PIN? In this scenario, Sally isn't prompted for her password because security personnel at Garth Enterprises have at least four solid reasons to trust Sally's activities. Multi-factor authentication (MFA) allows the company to confirm Sally's identity based on a combination of these factors to derive a security rating that is high enough to allow her access to the data she seeks.

On her way to the client Sally takes a break at a restaurant and, using public Wi-Fi, re-checks her presentation and reads her email. This time only the first two trust principles apply, which means there could be a reason to challenge Sally's identity. However, her trusted laptop has a Bluetooth connection with her mobile phone, which would lock her PC automatically if the paired device goes out of range, a feature called "dynamic lock." This feature is good enough to conclude that it is indeed Sally requesting this additional corporate data. Furthermore, intelligent security has checked this public Wi-Fi access point for known problems and found none.

The client asks Sally to present using the client's workstation in the client's meeting room. Sally uses this computer to connect to her corporate cloud drive to access her presentation. Now, she needs to provide her username and password because there is no other trust principle in place. She receives a challenge on her phone through MFA, and she is also notified of this access with an email.

Journey to the digital workplace

Most of Sally's experience and the security surrounding the company's data are already possible through modern workplace management today. Workplace management, sometimes referred to as "device management," exists to help

authenticated users securely connect to and consume corporate data. It doesn't fill every security role — authenticating users and protecting corporate data are responsibilities that lie elsewhere — but it plays a key role in enabling devices to access corporate data securely.

It's important to distinguish modern workplace management from its predecessor, what we would call "traditional" workplace or device management. Traditional workplace management reflects the highly centralized command-and-control style of IT that evolved over decades. Users and devices are located onsite with a direct network connection. Corporate IT controls all aspects of the infrastructure, the devices, the applications and the network, and enforces this control with locked-down workplaces, an application portfolio that serves as a whitelist of allowed apps and a firewall that restricts access to external internet sites.

To a growing degree, work no longer fits this centralized model. Workplace boundaries are disappearing, and much of today's workplace technology is supplied by employees who prefer their own personal devices to company-supplied assets. This shift is causing companies justifiable concern as they try to find that balance between a user's experience and securing corporate data.

The modern workplace comes with a completely new set of security requirements as it moves away from the locked-down, whitelist environment. The skills and effort required to meet the new challenges using traditional workplace management tools is simply beyond the means of the average company. That's what makes the transition to modern workplace management so important.

Co-exist or co-manage?

There are two typical ways a company can implement workplace management that enables the user experience and provides the level of security required for a new personalized enterprise work experience.

Co-existence is a popular approach that enables a company to maintain a traditional environment while establishing a separate modern environment. Users who need the flexibility of a modern workplace arrangement, such as programmers or heavy Microsoft Office users, are good candidates to become part of the new environment. This can begin with a pilot program, adding more users as the modern environment is enhanced with tools and applications.

If you start with a pilot, the first thing to do is take stock of existing applications, group policy security settings and infrastructure components that are no longer meeting either the user experience or the security requirements of the digital workplace.

In moving forward, we must remove as much ballast of the traditional era as possible, either by making infrastructure and applications compatible with modern management or by replacing them. Some applications and some data may require a virtual layer, either because the application and infrastructure are not compliant with the cloud-based architecture of the digital workplace or we realize that some corporate secrets are best managed through "air-gapped access" available from virtual desktops.

Another way to implement modern workplace management is to choose an agile, co-management approach where every device is managed by both traditional and modern management tools concurrently, and users can be slowly weaned off traditional locked infrastructure and apps. This removes the requirement that all apps and infrastructure must be modern management ready.

Co-management helps optimize PC life cycle timeframes and gives users more self-service options such as a push-button reset to try to fix a balky computer. It also sets the foundation for enhanced security with features such as conditional access, single sign-on and some internet-initiated user-support actions like restart, remote control and factory reset.

Modern management

As a next step, a company might implement full modern management for personal devices, replacing group policy security settings with a best-practice baseline security approach. At this stage all devices have moved from the traditional environment to the modern environment.

Full modern management allows companies to leverage full cloud-based security using machine learning and analytics to counter insider threats, and employees enjoy a faster boot experience because fewer policies need to be applied.

In this new workplace, companies also benefit from a reduced application portfolio and make more use of software-as-a-service (SaaS) apps, resulting in a rationalized, standardized portfolio populated with apps that are compliant with modern management. Employees gain a self-directed user experience, even on corporate assets, because modern workplace management puts them in full administrative control.

Continuing the journey

Much of this is achievable today with available tools and the right skills, and there's much more to come. User experience and security will benefit from rapidly maturing technologies such as machine learning, smart products, software agents, wearables, blockchain, speech/facial recognition, robotics, augmented reality, algorithms and 5G wireless bandwidth. Modern workplace solutions are bringing these technologies together to offer workers like Sally the freedom to use devices and applications the company can trust without the need to see or test them.

DXC Technology is helping companies navigate this road to the digital workplace with a family of workplace solutions that provide a consumer-like experience with enterprise security and instant collaboration. Wherever you are on your digital workplace journey, you can trust DXC as your partner and guide.

Learn more at www.dxc.technology/workplace_and_mobility

About the author

Ben Santing is a recognized Tech Master and senior technical architect in DXC Workplace and Mobility. Ben's last projects related to the security of identity and corporate data, or Security Services for the Digital Workplace. Before this, he was lead architect of DXC Device as a Services, which offers a unique choice of enterprise graded services and hardware combined as a service. He has recently become the Architect of the proactive, predictive support and analytics service in Digital Support.