Cyber security for the modern workplace

Simplification of security technologies, a focus on cost optimisation, and considering users and data are the keys to securing the modern workplace environment.

Introduction

Information security protection has come a long way in the last two decades. It started out with organisations designating their internal network as the trusted zone and everything outside their network as the untrusted zone. We used firewalls to restrict access from all untrusted zones into the trusted zone and gave assets within the trusted zone unfettered access to one another. From a workstation perspective, security was once considered good practice when anti-virus software was installed, and remote users had a VPN to connect to the corporate network.

Since that time, the threat landscape has changed, yet our approach to securing a workstation hasn't. We have continued to add security tools onto workstations to plug the next hole – multi-factor authentication, personal firewalls, host intrusion detection / prevention, encryption, vulnerability scanning agents, data loss prevention (DLP) and endpoint detection and response (EDR) tools. As a result, workstations are slow, complex and difficult to manage. When the purpose of a workstation is to drive a business outcome, there are serious questions as to whether the balance is correct between the cost, user experience and security outcomes.

Today, in the age of offsite data centres, public cloud environments and the need for remote access from any device and any location, a secure environment is much more fluid and harder to manage. However, the maturing of various technology capabilities, a continued focus on cost optimisation, and the COVID-19 working from home requirement has forced a rapid change in approach. Security professionals have both an opportunity (and a challenge) on how to rethink the approach to enabling user and business functions while still providing a secure environment.

Key principles

Organisations should consider adopting the following principles, which are common at those organisations best meeting the challenge:

Extend control and enforcement points to the cloud — Organisations are shifting workloads to the public cloud and increasingly using more software as a service (SaaS) applications. When coupled with a greater number of remote workers, it doesn't make sense to tie key security controls to a workstation accessing an organisations data centre. Extend security controls and enforcement points from the data centre to the cloud to minimise the 'tromboning' of traffic between the workstation, cloud and data centre. This simplifies how a user accesses what they need to do their job, regardless of location and drives a better user experience.

Maximise the use of native capability — Native security capabilities within operating systems have matured significantly in the past two to three years. While not all security capabilities within the operating system are as good as third-party tools, maximise the use of what is deemed suitable, and plug the gaps with third party tools only where required. Such an approach assists in simplifying the workstation and minimising licence costs.

Use the most complete tools, not the 'best of breed' — Many large organisations have taken the approach in the past of selecting 'best of breed' security tools for each security control on a workstation. While in theory this delivers a better security outcome, from experience many organisations that adopt this approach struggle to achieve the outcome. Integration, compatibility and workstation resource challenges can be problematic; this is coupled with higher costs for products as well as for training and cross-skilling of staff. Instead, aim to identify a workstation security product that provides the most complete coverage (as close to best of breed as possible), and only add additional tools where specifically required.

Move towards the 'Zero Trust' model — Zero Trust implements the "deny all, allow some" least-privilege principle even within a trusted environment. The model assumes that everything around a network asset is hostile, including network assets from the trusted zone. Zero Trust has been around since 2010 and was initially focused on network access control. However, the principle and technology capabilities have massively evolved since then, with a much greater focus on data security. The DXC paper "Zero Trust for maximum security" explores this concept in greater detail.

Key challenges

In adopting the principles outlined above to drive towards a simplified and more cost-effective secure workstation the following challenges are likely to be encountered:

Integrate the workplace security strategy with other strategies — A workplace security strategy cannot be developed in isolation. To adopt the principles outlined above, a workplace security strategy / architecture must be developed in conjunction with other strategies covering areas such as user experience and personas, application delivery, network, identity and access management, and the broader security strategy. In large organisations, achieving alignment across these disciplines can be difficult.

Understand data — In most situations, organisations adopt a one-size-fits all approach to workstation security. While this approach will work for most users, users dealing with sensitive information are likely to have inadequate security whereas those using less sensitive information may be over-controlled. Experience indicate there are large user groups that are potentially over controlled. To provide a better outcome it is important to have a thorough, business driven understanding of what data is being accessed and how it is being accessed.

Understand the identity requirements and implications — As well as a strong understanding of data, the adoption of Zero Trust also requires a deep understanding of identity – including assets, devices, services, data and users. Based on experience, some organisations may require significant effort to improve their identity management in order to adopt Zero Trust.

Recognise that this is a shift over time, not a big bang — Outside of a 'greenfields' organisation, implementation of the key principles to achieve a simpler, more cost-effective workstation security environment can't be achieved with a big bang approach. Present technologies, approaches and practices take time to be re-designed and adopted. They are also impacted by financial, regulatory, resourcing and organisation change / culture factors.

Conclusion

In a world where COVID-19 has driven both remote working and a significant focus on cost, the existing approach to workstation security cannot continue. Through adopting the key principles, organisations are able to simplify their workstation security environment and optimise costs. When designed and implemented well, these principles will also deliver an enhanced security outcome and a better end user experience.

About the author

Tim Miller is a seasoned security professional with over 15 years' information security experience. He has worked in a broad range of domains and industries including financial services, federal government, telecommunications and retail organisations.

Learn more at
dxc.com/security