Prepared by AmCham member

CITRIX

Desktop virtualization brings more security

The tension between security and business productivity has never been so acute. To operate at peak performance and competitiveness, organizations need workers to access enterprise resources in more places and in more ways than ever before.

The resulting proliferation of work locations, types of workers and access methods has pushed traditional security strategies to the breaking point. The consumerization of IT adds further complexity as a diverse mix of laptops, smartphones and tablets enter the environment, including both enterprise-owned devices and those purchased by workers. While technologies such as firewalls, anti-virus, access control and perimeter monitoring remain an important base, they are increasingly bypassed, as today's skilled attackers directly target applications and data.

Critical concern – information security

Information security has become an increasingly critical concern for organizations of all kinds. Today's threats are more potent than ever, from the infection of corporate networks by custom malware, to targeted hacking, sophisticated phishing attacks, and outright tampering or theft of assets and intellectual property. The impact on business due to security breaches such as these, including both financial losses and damage to brands and reputations, have increased within the last few years. Security incidents also disrupt the continuity of business operations, which can't return to normal until the breach has been diagnosed and stopped, and damage has been assessed and repaired.

Information security might be achieved

While effective information security is increasingly vital to achieve, it is increasingly challenging to maintain. Trends such as consumerization, worker mobility, cloud computing and workshifting mean that more people, including teleworkers, mobile users, partners, outsourcing providers and other contractors, are accessing enterprise desktops, applications and data from more places and in more ways, than ever before. Consequently, information is now everywhere: on enterprise and consumer-owned endpoints, in public and private clouds, at partner organizations, on the factory floor – the list goes on.

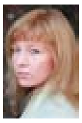
But there is a way for IT to manage risk to meet the organization's requirements for information security, data protection, privacy and compliance—while maximizing business productivity and allowing unfettered growth. The essence of the strategy is to enable the right level of secure access and collaboration for workers, while maximizing control and protection of enterprise data, applications and infrastructure. The enabling technology for this strategy is desktop virtualization.

Desktop virtualization – secure by design

The foundation of desktop virtualization is the centralization of IT resources in the datacenter – an inherently more secure architecture that makes it far simpler to control both information and access. Centrally managed virtualized desktops, applications and data are delivered on-demand as a service, giving workers an experience that looks, feels and acts like their traditional PC no matter how they access it or what kind of device they use. A well-designed desktop virtualization solution offers important advantages over traditional security models.

- Resource centralization – Enterprise applications, data and intellectual property are managed and secured in the datacenter and accessed securely from anywhere, rather than residing on the endpoint devices of every worker in the extended enterprise, greatly reducing business risk. IT gains full visibility and control over centrally managed desktops and applications, and can easily define and enforce policies over which resources specific users or groups can access. Desktop and application access can be turned on and off instantly as needed.
- Policy-based access control – IT can leverage pre-configured policies to determine the appropriate level of user access to applications and data wherever they reside: in the datacenter, in a public or private cloud, even downloaded to a local device for offline use where full isolation, encryption, and strict control over save/copy functionality and peripheral usage prevent data from going astray.
- Any-device access – Because the virtual desktop is hardware- independent, IT can enable secure access and collaboration for every employee, contractor or partner from any personal or corporate-owned device they choose to use. Rather than making distinctions between enterprise-owned and outside devices, IT valuates every device and user according to administrator-defined criteria.
- Built-in data compliance – The centralization of resources, combined with strict access control, makes it much easier to protect against data loss and meet compliance and privacy standards by ensuring full activity logging, reporting and auditing. IT can define and implement policies to ensure conformance with the full spectrum of requirements the organization faces – both internal and external.

The complete solution should be designed to provide the centralized control and management, flexible delivery scenarios, granular, policy-based access control, endpoint protection and compliance support organizations need to manage risk without obstructing business productivity or growth. Citrix XenDesktop, one of the possible solutions, enables on-demand delivery of virtual desktops and applications, complemented by application delivery control, secure access control, and client-side virtualization and encryption. Security is already one of the main reasons organizations are adopting desktop virtualization, along with strategic business priorities such as workshifting, business continuity and IT efficiency. By making desktop virtualization a central element of security, IT can manage risk more effectively while providing optimal flexibility to allow the business to do what it needs to do, the way it needs to do it.



Eva Koutná, Channel Development Manager, Eastern Europe, Citrix Systems