An IDC Info Snapshot, sponsored by softlanding

Key Considerations for Securing Your Remote Workforce

By: Yogesh Shivhare, Senior Analyst, Security and Infrastructure, IDC

42% of Canadian employees will work remotely at least one day a week post-pandemic, **2x that of pre-pandemic.**

47% of Canadian enterprises cited security risks of a remote workforce as their top concern.

The events of 2020 forced many organizations around the world to adopt or accelerate remote work for their employees, often on incredibly tight timelines. This hurried adoption of remote work led to security vulnerabilities and increased cyberattacks across industries — deploying quickly was the top priority; scaling securely came second. Securing an extensive, distributed, and standardized remote workforce involves the movement toward zero-trust security architectures for network and application security, managed devices, and endpoint delivery services in conjunction with advanced security services that assess and maintain organizations' security posture.

Zero-trust network access technologies complement traditional virtual private networks (VPNs) and provide continuous authorization and access to users and devices based on identity and context rather than on credentials. A robust identity and digital trust management solution delivers access, privilege management, and governance, and when complemented with a network access control (NAC) solution, it enables IT administrators to enforce security policies and block noncompliant endpoint devices.

Businesses, however, **must adopt a multilayered security approach to create multiple security control points for threat detection and prevention as well as to add enough depth at each layer to delay the progression of cyberattacks.**

Single sign-on (SSO) can streamline login workflow across applications while MFA (multifactor authentication) adds another layer of authentication to verify user identity in case credentials are compromised or stolen.

Software-defined secure access (SDSA) is a new category of access security and control solutions that includes software-defined perimeter (SDP) and identity-aware proxy (IAP) approaches. SDSA establishes secure connections based on context-aware, identity-aware, and device-aware policies, from authenticated users to authorized applications. SDSA solutions are designed for a digitally transformed world that eschews static network perimeters. SDSA is built on distributed integrity principles of application- and user-centric protection and least-privilege access, thereby preventing unauthenticated users from connecting to or sending any traffic to unauthorized applications.

Organizations in which applications, infrastructure, and data are distributed across on-premises and cloud locations can benefit tremendously from cloud security gateways (CSGs). CSGs leverage the functionality of traditional security controls and methods and apply them to cloud architectures. CSGs provide extensive functionality including web content security, next-generation firewalls (NGFWs), and cloud encryption. In addition, they provide key data loss protection (DLP) and user behaviour analysis capabilities for cloud environments.

Endpoint security is another cornerstone of securing a remote workforce. Modern endpoint security products do more than just detect malicious code and behaviours: They also offer features that thwart threats during the early stages of an attack and reduce the endpoint's attack surface area and exploitability. Endpoint protection platforms (EPP) may not detect all instances of malicious code or process behaviours immediately and hence are widely complemented with endpoint detection and response (EDR), which provides additional stages of detection by correlating and analyzing multiple forms of endpoint telemetry.

While vendors provide and enhance new cybersecurity technology, cyberthreats also continue to evolve rapidly. Advanced persistent threats (APT) often go undetected for months and can move laterally to compromise a large set of IT systems and data. Businesses must create a robust risk management strategy that not only is reactive to threats but also proactively assesses their security posture, regulatory gaps, and vulnerabilities. Businesses, especially small and medium-sized businesses, typically lack advanced security capabilities and find it difficult to hire and retain security staff to deal with advanced threats. Many, if not most, organizations should consider an external security services provider. A trusted third-party security services provider can combine tools, technologies, procedures, and methodologies to enhance cybersecurity capabilities.

Message from the Sponsor

Empower your people to be productive and secure from anywhere.
Softlanding's two-day workshop will show you how to use Microsoft technologies to:

- Provide meeting experiences to connect teams remotely and onsite
- Simplify day-to-day work with apps and workflows
- Connect people to drive culture, change, and communication
- Manage and secure any device

Request a Secure Work from Anywhere Workshop with Softlanding