citrix

Checklist

Seven Keys to Delivering Secure Remote Access

While keeping systems secure has never been easy, it was certainly simpler when everyone came to the office to work. Now, distributed employees work on a variety of networks not secured by IT and on devices your organization may not manage. This makes it more challenging to gain visibility into the potentially risky actions employees may be taking and how those actions may impact corporate data security.

At the same time, it is essential to acknowledge that applications and data do not only live inside corporate datacenters anymore but are instead distributed across several different cloud services and on-premises. Moreover, even busines critical enterprise applications are delivered from the cloud.

But as we rely more on the cloud, your attack surface is larger and the number of security threats are rapidly evolving. Your attack surface now includes the devices, applications, files, and networks that remote employees use to get work done. While each one is critical to driving productivity, each is a potential weakness an attacker can exploit.

Here are the seven keys to securely deliver applications wherever your employees work.

1. Zero Trust Network Access (ZTNA) to All IT-Sanctioned Applications

Providing flexibility increases user adoption and drives efficiency, but it's important to ensure security protects apps and data without interfering in how users get work done.

Appliance-based solutions like VPNs and SWGs were designed on the principle of "implicitly trusting" something known. Unfortunately, the notion of "Implicit Trust" is exploited by many modern-day attacks that use compromised credentials, insert malicious content, or use a stolen or compromised device to access information and steal intellectual property.

Zero Trust goes against the principle of Implicit Trust and focuses on **"Never Trust, Always Verify."**

Traditional solutions only focus on authenticating and authorizing users at the time of login, or blocking suspicious URLs only once they are blacklisted. In contrast, Zero Trust assumes all users and URLs are suspicious unless they prove otherwise. Zero Trust thus enables you to continuously monitor and assess user activities throughout the session and automate security controls based on anomalies detected.

To adopt Zero Trust for securing your applications and data, you must deliver security for remote employees at the application layer to prevent network-level attacks while enforcing contextual access control driven by continuous assessment. This requires capabilities to scan end-user devices before and after a session is established and define how users are authenticated and authorized to access their applications.

2. Exceptional Experiences

If users have a poor IT experience, they will find workarounds that can impact productivity and security. Appliance-based solutions like VPNs and SWGs were designed for a small percentage of remote employees, and they only provide security for a subset of applications. With more employees taking on mobile or remote work, appliance-based solutions are hard to scale, requiring backhauling traffic and a separate login experience. To prevent these issues, it is vital for IT to provide a solution that offers the best possible user experience and security. This often means moving beyond VPNs and adopting more unified workspaces that equip employees with the right tools wherever they work.

3. Single Sign-On (SSO) to All IT-Sanctioned Applications

Whether BYOD, corporate devices, a dedicated desktop, or a shared device, your remote access solution should simplify the user experience. Features like Single SignOn (SSO) provide secure access to all IT-sanctioned applications, virtual apps and desktops, and document repositories. SSO solutions also simplify access for users as they do not need to remember nor manage multiple usernames and passwords. Furthermore, users can leverage a single pane of glass for all their applications and files — minimizing the burden on IT to resolve password problems or reset expired access privileges.

4. Adaptive Authentication and Device Posture Checks

Adaptive authentication with device posture assessment intelligently routes the user to the suitable authentication mechanism based on role, geo-location, and device posture check. For example, a contractor on an unidentified device may be prompted for additional authentication steps, or an employee accessing an application from an unusual location may be denied access.

Application access can be enabled based on user role, location, and device posture analysis. With device posture assessment, IT can scan endpoints based on various factors such as anti-virus, OS, firewall, registries, and more.

5. Application Performance

Poor application performance leaves users frustrated and unproductive. But with technology that increases visibility and control across application performance, IT can reduce application, network latency and outages. This results in better uptime, improved helpdesk SLAs, and reduced likelihood that users work around security controls as a result of poor application performance.

6. Automatically Detect and Defend Against Potential Risk

Analytics provide insights into applications, files, devices, and networks, which helps IT automate security enforcements based on user behavior and detected anomalies. Continuous risk assessment and adaptive enforcement help IT reduce manual work, provide timely enforcement, and minimize the risk of unauthorized breaches.

Solutions like Remote Browsing enable IT to be confident that end users can securely navigate the web without introducing risk to the corporate environment. This protects you from threats that may be introduced by malicious websites by ensuring these browsers are isolated off the corporate network and devices.

7. IT Consolidation and M&A

Consolidating management of IT services, networks, clouds, and applications into a unified platform helps reduce IT complexity, improve employee productivity in a better end-user experience, lower the total cost of ownership, and prevent security gaps in your infrastructure that could increase compliance risks.

As organizations acquire other companies, it is critically important for IT to quickly onboard new employees and allow the business to carry on with minimum disruption. However, it is hard to scale appliance-based solutions as new employees can take weeks to procure, install, and make them available to use. Therefore, it is vital for IT to limit access for these users to only certain apps and not provide full network access until everything is ready.

Conclusion

As you plan how your IT modernization will deliver a secure and productive environment for your hybrid workforce, you need to explore fully integrated solutions delivered as a cloud service. A multi-vendor solution makes it nearly impossible to centralize security management and automation. None of the security policies and user risk profile work across multi-vendor products, which forces security administrators to execute slow, manual processes.

Citrix's Unified Secure Access offers a fully unified and ready-to-deploy solution that enables you to maximize performance, minimize risk, and drive workforce productivity anywhere and on any device.

citrix

Enterprise Sales
North America | 800-424-8749
Worldwide | +1 408-790-8000

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway, Santa Clara, CA 95054, United States