Solution Brief

5 priorities for securing hybrid work

Creating a long-term remote work strategy with Citrix and Chrome OS

In an instant, workforces of all types went remote and so did their devices, apps, and data. To keep businesses running, IT prioritized rapid provisioning of widespread remote access capabilities that often came at the cost of security.

Now it's clear that the shift to hybrid work is here to stay, with Gartner predicting 31 percent of the worldwide workforce will be remote in 2022.[1] IT organizations must transition from short-term, reactive approaches to a more secure, scalable, and simplified approach to managing hybrid workforces.

Citrix and Chrome OS have been helping organizations achieve this for years with an integrated solution for secure hybrid work. **Citrix Desktops as a Service (DaaS) solutions on Chrome OS provide organizations with a secure, cost-effective remote work solution** that enables IT teams to centrally manage, monitor, and define employee access to any type of app or virtual desktop. With built-in, multi-layered security features, as well as automated actions to prevent future security breaches, the combined Citrix and Chrome OS solution provides your organization with the most comprehensive, secure, and cost-efficient remote work solution available in the market today.

As you plot your long-term hybrid work strategy, here are five ways to simplify, strengthen, and improve it with Citrix and Chrome OS. By doing so, your devices, apps, and network will be more secure, the IT management and operational overhead will be simplified, and the overall employee experience improved.

1 Separate data from devices with Desktops as a Service (DaaS)

The rush to support remote work led to increased usage of VPNs as the primary remote access method. While VPNs provided access, they failed to give IT granular control over access levels and assume the endpoint is safe. And considering that a laptop has a 1-in-10 chance of being stolen and only a two-percent chance of being recovered, a VPN leaves the device and all the data highly vulnerable.[2] A better approach is to begin with devices that are secure by design and then use **desktops as a service (DaaS)** to deliver the applications, IT services, and even Windows desktops.

One of the most secure types of devices available in the market today are Chrome OS devices. Chrome OS is a speedy, simple, and secure OS from Google that powers Chromebooks. The cloud-based architecture of Chrome OS means that devices have fewer software components to update and manage, and they use the latest security intelligence to protect the device. Not only is the device encrypted, but the firmware, OS, and browser code go through a "verified boot" process that ensures nothing on the device has been maliciously altered. **In fact, there has never been a reported ransomware attack on a Chrome OS device.[3]**

In order to transform secure devices into productive business workspaces for all employees, organizations need to leverage DaaS solutions to expand the devices' capabilities. **Citrix DaaS solutions are a secure and consistent way to deliver virtual apps and desktops from the cloud to any device.** Citrix DaaS solutions allow IT to provision apps — traditional Windows, legacy, Linux, and SaaS — as well as full Windows or Linux virtual desktops. Using the Citrix Workspace app to access Citrix DaaS on Chrome OS devices, employees simply need to boot up and login to gain access to everything they need to be productive. Every app and piece of data that is being accessed with Citrix is not only encrypted, but run securely in the cloud, not on the device. In the rare event that a Chrome OS device is compromised, IT can remotely disable and wipe the device, leaving the user's profile, data, apps, and desktops intact and secure in the cloud.

2 Adopt Zero Trust Network Access with Citrix and Chrome OS

Appliance-based security solutions that use VPNs and datacenter-based security stacks were designed on the principle of **"implicitly trusting"** something known. Unfortunately, the notion of implicit trust is exploited by many modern-day attacks that exploit 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,"** assuming all users, devices, and URLs are suspicious unless they prove otherwise. Zero trust thus enables IT teams to continuously monitor and assess user activities throughout the session and automate security actions based on detected anomalies.

To adopt a zero trust model, IT 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.

Citrix Secure Private Access and **Google BeyondCorp Enterprise** are robust and intelligent zero trust security solutions to leverage with Citrix DaaS on Chrome OS deployment to create multi-layered security. Citrix Secure Private Access is a VPN-less solution that delivers zero trust access with adaptive authentication and single sign-on to IT-sanctioned applications. It provides secure access at the application layer to prevent network-level attacks while enforcing contextual access control policies. These policies are driven by continuous assessment and verification of the end user's identity, geolocation, device posture check, and user risk score.

BeyondCorp Enterprise shifts access control from the network perimeter to the user and device. Regardless of location, if the Chrome OS device and user credentials cannot be validated, access permissions are denied.

3 Centralize IT monitoring and management capabilities

Every new IT tool or service comes with its own set of consoles to operate, monitor, and master. Keeping a watchful eye and troubleshooting everything significantly increases IT's work. To ease the management burden, IT should centralize and consolidate how apps and Windows or Linux desktops are provisioned, managed, and delivered. Especially with a widely distributed workforce, an integrated, cloud-first management console is essential to keeping resources secure and IT costs down.

Management and monitoring of employees' apps and desktops is centralized in a unified cloud console with Citrix DaaS solutions. Apps and desktops are centrally configured and packaged into profiles, then delivered from the cloud in a one-to-many fashion. Citrix DaaS solutions enable IT admins to maintain complete control over applications, policies, and users from one location. When it is time to make a policy change or roll out an update, IT only needs to do this once, then instantly make those updates available to every user without touching devices.

To gain better visibility, Citrix DaaS on Chrome OS devices enables IT to monitor and analyze all application behavior as well as data and network access from one place. Threat detection and resolution can now happen from the cloud, rather than fixing problems for individual users or devices. These efficiencies not only make life easier for IT, but they also add up to significant savings. **ESG reports that a typical mid-sized organization can reduce IT admin costs by more than 60 percent and lower the TCO by more than $650,000 over three years with Chrome Enterprise.**[1]

To further reduce IT workloads, you can implement automation solutions like Citrix Analytics for Security to monitor and secure users and resources automatically. Citrix Analytics provides continuous risk assessments across all aspects of Citrix DaaS deployments, including apps, files, Chrome OS devices, and networks. When an anomaly is detected based upon user risk behavior, the solution triggers workflows to prevent any further security threat, reducing the manual work for IT and resulting in timely enforcement with fewer breaches.

4 Apply granular access and policy controls

As varied as job functions are, so are the apps that different groups need access to. For example, contact center agents may only require access to one or two specialized applications, while designers and engineers require a very different set of apps. Therefore, a one-size-fits-all approach for app access and controls will rarely work.

Instead, IT should take a granular approach to defining who gets access to what, when, and how. **Citrix DaaS** and **Citrix Secure Private Access** solutions use a robust set of policies to control which user groups have access to specific application sets. If a worker changes roles, IT can simply associate the user with the new applications and permissions they need without installing anything on the actual device.

Citrix uses the same approach to control security requirements such as requiring multi-factor authentication or controlling access based on geography, IP address, or other changing conditions. The granularity goes even further, allowing IT to conditionally control individual actions within an app or Windows desktop. For example, with Citrix DaaS solutions, IT can control if a user is allowed to print and then further refine access to certain printers or only within certain networks. The same goes for saving files, mapping drives, accessing USB sticks, or connecting to cameras and microphones. IT can even use **Kiosk mode on Chrome OS devices** and limit access only to the Citrix Workspace experience, preventing access to anything else on the device.

At the internet access level, **Citrix Secure Internet Access** provides cloud-delivered services that add additional layers of security. Citrix Secure Access is positioned between the device and the internet and offers comprehensive security functionality including a Secure Web Gateway, Cloud Access Security Brokers, firewall, malware protection, data loss prevention, and more. All of this integrated into a high-performance, auto-updated cloud-delivered architecture.

5 Focus on the employee experience

If IT provides employees with subpar technology and tools, employees will invariably find workarounds that improve their personal productivity at the cost of security and compliance. To prevent the temptation to bypass security controls or simply use their own unmanaged personal device, it is vital for IT to provide simple and usable ways to work without compromising security.

IT can enhance employee collaboration and productivity by using Citrix DaaS solutions to deliver the Citrix Workspace experience on Chrome OS devices. Chrome OS devices boot in seconds and make it easier to get to work, without the setup and configuration steps associated with traditional devices. Even on their first day of the job, all the employee needs to do is boot, connect to Wi-Fi, and use the pre-configured Citrix Workspace app to access the apps, services, and data they need. There is no extra software to install, VPNs to connect through, or time-draining helpdesk setup steps to take.

Recognizing that personal and work time overlap, IT can confidently allow people to browse on a company-provided Chrome OS device without backhauling traffic to the datacenter for inspection. **Citrix Secure Internet Access** restricts access to inappropriate content and sites and **Citrix Secure Private Access** allows employees to securely navigate the web without introducing risk to the corporate environment. Isolated browsing sessions protect users and networks from threats that can be introduced by malicious websites loaded with malware.

Citrix and Chrome OS make hybrid work better

By adopting Citrix DaaS and Chrome OS devices, organizations can achieve these five strategic priorities, securing hybrid work now and in the future. Together, Citrix and Chrome OS strengthen the security of your devices and apps, simplify IT management, and give employees a better experience.

Secure hybrid work today.
Visit **Citrix.com/Google**

[1] ESG Economic Value Validation – Quantifying the Value of Google Chromebooks with Chrome Enterprise Upgrade
[2] Laptop and Mobile Device Theft Awareness – The University of Pittsburgh
[3] Google, Free your business from ransomware with Chrome OS

citrix chrome OS

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