citrix chromeOS

Meeting the security challenges of hybrid work

How Citrix DaaS solutions and ChromeOS help organizations implement multi-layered security solutions

Hybrid work demands a new proactive approach to security

The nature of work has changed dramatically over the past two years. Organizations rapidly adopted hybrid work models, providing staff with greater freedom in where, how, and when work gets done.

Along the way, IT implemented a variety of point solutions to enable remote work, and in some cases, this even loosened security controls. Cyber attackers were poised to take advantage of these weaknesses and launched a volley of attacks. Phishing, ransomware attacks, and supply chain threats raged during 2020, putting companies' strategies, intellectual property, and business continuity at risk.

Since that time, company IT teams have realized that they need a comprehensive, integrated, and consistent way to keep workers productive, while securing vital data, assets and networks. And now, more than ever, they are looking to desktop as a service (DaaS) solutions from Citrix and ChromeOS devices as the combined solution to address these changing needs.

What IT and security now need is a comprehensive, integrated, and consistent way to keep workers productive, while securing vital data, assets, and networks.

Citrix DaaS on ChromeOS devices provides a better way to secure the future of work. The joint solution provides built-in, multi-layered security and automated actions to prevent breaches. Citrix DaaS and ChromeOS provide organizations with the most comprehensive, secure, and cost-efficient remote work solution that's available in the market today.

Security threats are growing in an era of hybrid work

61% of organizations have struggled to evolve security to support remote work.[1]

In 2021, global cyber breach remediation costs are expected to exceed

$6 trillion.[2]

IT needs to evolve hybrid work security

The rush to support remote work mandates introduced new gaps into security architectures that IT teams now need to address with a long-term approach. Here are some key considerations for your hybrid work strategy:

Reduce reliance on VPNs

Remote access VPNs are not the failsafe that many think they are. VPNs may be connected to insecure home Wi-Fi routers, have poorly configured encryption, or do not use multi-factor authentication. Security teams should use DaaS solutions to provide encrypted, VPN-less access to apps, data, and resources that run in the cloud, significantly lowering the threat level.

Adopt zero trust security

Traditional security solutions like VPNs were designed on the principle of "implicitly trusting" something known. But modern-day attacks take advantage of compromised credentials, stolen devices, and the ability to insert malicious content.

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 security solutions continually authenticate users, from initial access request to session ends.

Decrease device risks

Working from public locations increases the chance a device is lost or stolen. Considering that a **laptop has a 1-in-10 chance of being stolen and only a 2 percent chance of being recovered,** the best approach is to keep all data off devices and store it in the cloud.[3]

This approach also minimizes the impact of a malware or ransomware because IT can remotely disable and wipe a compromised device. Users' profiles, data, apps, and desktops, remain secure and available in the cloud.

Streamline IT management

Using multiple standalone solutions and manual processes to manage endpoints doesn't scale. IT needs a holistic, integrated security and management solution that centrally pushes the latest application and OS security updates from the cloud. This integrated, centralized approach saves IT a significant amount of time and resources. It also improves a company's security posture by reducing the number solutions that IT needs to manage at any one time.

30 percent of home workers let another person use their work laptop[4]

Citrix DaaS and ChromeOS meet the demands of hybrid work

Citrix and Google have partnered for over a decade to enable the future of hybrid work for organizations everywhere. **Citrix DaaS on ChromeOS provides organizations with a secure remote work solution that provides employees with one-click access to any type of app or desktop.** IT administrators benefit from this integrated, cloud-first solution with granular security policies and centralized management capabilities. With built-in, multi-layered security, as well as automated actions, the combined Citrix DaaS and ChromeOS solution helps organizations enable, secure, and scale remote work for hybrid teams globally.

Citrix DaaS solutions on ChromeOS devices are:

Secure

Data is stored in the cloud, connections are encrypted, and software and operating systems are kept up-to-date.

Seamless

Employees get access to virtual desktops and Windows, Linux, web, and SaaS apps.

Simplified

Citrix DaaS on ChromeOS is faster to deploy, easier to manage, and reduces overall IT maintenance requirements and costs.

Improving the security of hybrid work with Citrix DaaS and ChromeOS

Citrix DaaS and ChromeOS meet companies' security imperatives today and follow industry best practices for securing hybrid work.

Using natively secure devices and services

ChromeOS and Citrix DaaS were designed from the ground up with security in mind. Because all apps and data are delivered from the cloud, storing nothing on the device, the combined solution is ideal for remote work.

Citrix DaaS enables apps and desktop resources to be hosted on public or private clouds and can be configured to constantly secure all connections to apps and desktops with zero trust security policies and Transport Layer Security encryption. In addition, Citrix DaaS and ChromeOS automatically provide cloud-delivered security updates and patches so that each employee's workspace is always up-to-date.

Enabling zero trust security models

As endpoint risks grow, organizations need a different approach to security that adopts the principle of "never trust, always verify" with all access requests. By so doing, they assume that access attempts are malicious until proven otherwise.

Citrix DaaS and ChromeOS devices enable zero trust models by delivering security at the application level, while continually verifying user identity. IT can use **Citrix Secure Private Access** to set up fine-grained policies that provide fine-grained policies that provide contextual access to Citrix DaaS resources. That means user identity, device, location, time, behavior, and other key factors are considered to make sure user identity and sessions are legitimate.

Google BeyondCorp Enterprise provides secure access to web apps by shifting access controls to the user and device. If devices and user credentials aren't verified, access requests are denied. **Citrix Secure Internet Access** provides another layer of cloud-based security that protects all users, regardless of their location, against the latest threats.

Providing granular access privileges

Citrix DaaS solutions give administrators granular control over users by applying policies at different levels of the network — from the local level to the organizational unit level. By controlling these policies, IT determines if a user, device, or groups of users and devices can connect, print, copy or paste, or map local drives. These granular controls minimize security concerns with third-party contingency workers, for example. In addition, Chrome Enterprise also enables IT to enforce 500+ device policies for end-to-end security and control.

There have been zero reported ransomware attacks on ChromeOS devices, whether they are used by businesses or consumers.[5]

How Citrix DaaS and ChromeOS simplify IT management

IT wants to deliver an exceptional user experience while streamlining management processes. Citrix DaaS provides simpler, scalable processes that provide ongoing benefits to IT teams as they handle greater business growth.

Centralizing IT management

Citrix DaaS and ChromeOS provide integrated, centralized management of devices, users, apps, and desktops from the cloud. As a result, IT administrators can seamlessly and remotely push through security updates automatically in the background, as employees continue to work.

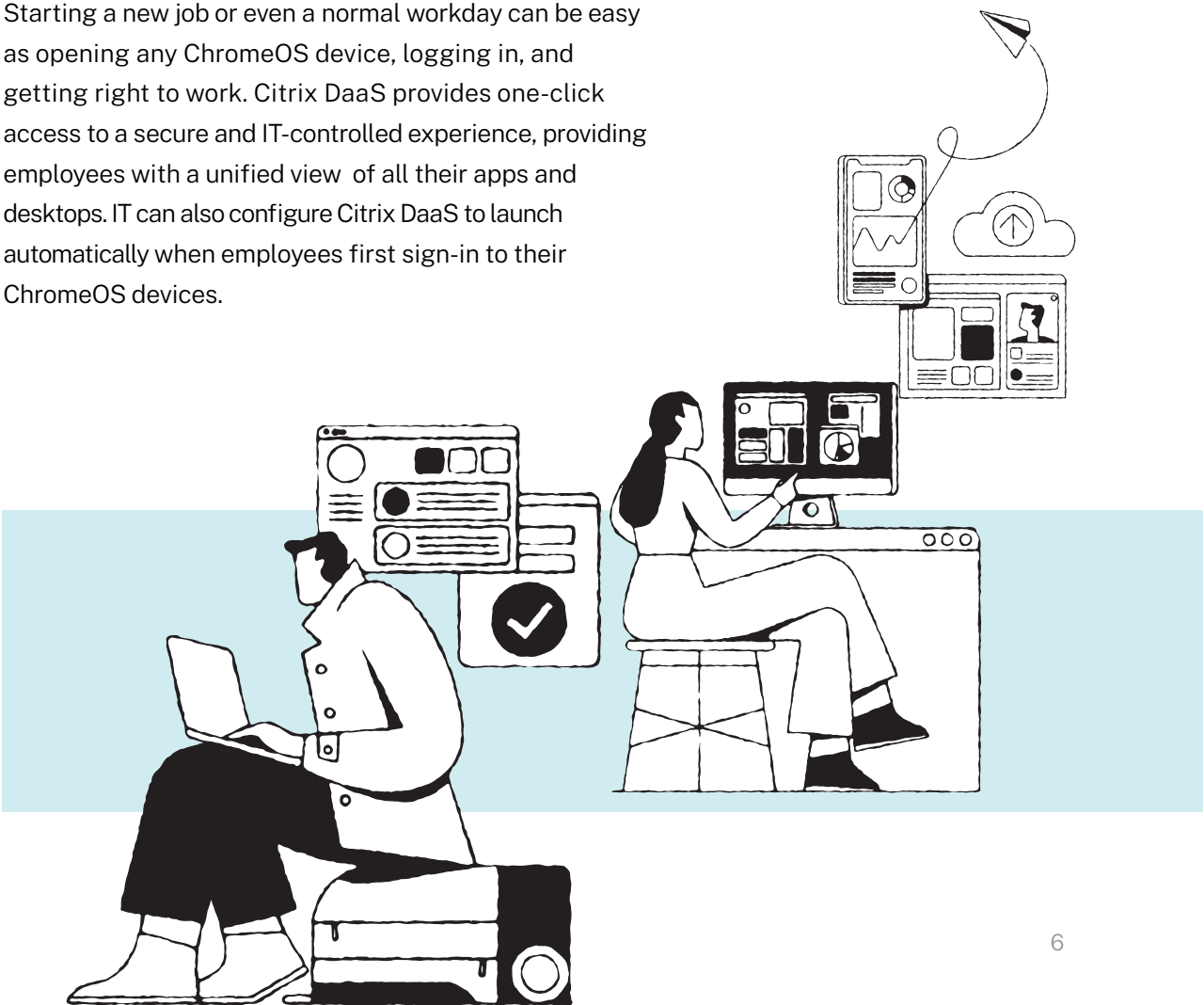
Additionally, with Citrix's native integration with **Chrome Enterprise** management console, IT can rapidly provision ChromeOS devices with the Citrix Workspace app without ever touching a device. In addition, **Citrix Analytics for Security** provides insights into applications, devices, and networks, automating security enforcements based on user behavior and other anomalies that are detected.

Delivering any app or desktop

Citrix extends user access to all types of virtualized apps on ChromeOS devices, including legacy and full-featured Windows apps, regardless of the operating system the apps were designed for. Similarly, some workers may require the use of a traditional Windows or Linux desktop.

Providing an exceptional user experience

Starting a new job or even a normal workday can be easy as opening any ChromeOS device, logging in, and getting right to work. Citrix DaaS provides one-click access to a secure and IT-controlled experience, providing employees with a unified view of all their apps and desktops. IT can also configure Citrix DaaS to launch automatically when employees first sign-in to their ChromeOS devices.



Strengthening security to help organizations grow

Citrix DaaS and ChromeOS help build the secure digital workspace experiences your people need to do their best work. Whether your teams are working in the office, at home, or on the go, they get a secure hybrid work experience that enables them to think, create, and innovate.

Learn more at **Citrix.com/google**

citrix™ chromeOS

Endnotes

[1] Kevin Casey, Hybrid work by the numbers: 14 stats to see
[2] Daniel Newman, The New Normal: Hybrid Work Means Greater Focus On Endpoint Security
[3] The University of Pittsburgh, Laptop and Mobile Device Theft Awareness
[4] Ibid
[5] Google, Free your business from ransomware with ChromeOS