citrix™ chromeOS

The strength of simplicity

Security for an era of hybrid work and digital business growth

Complexity is increasing

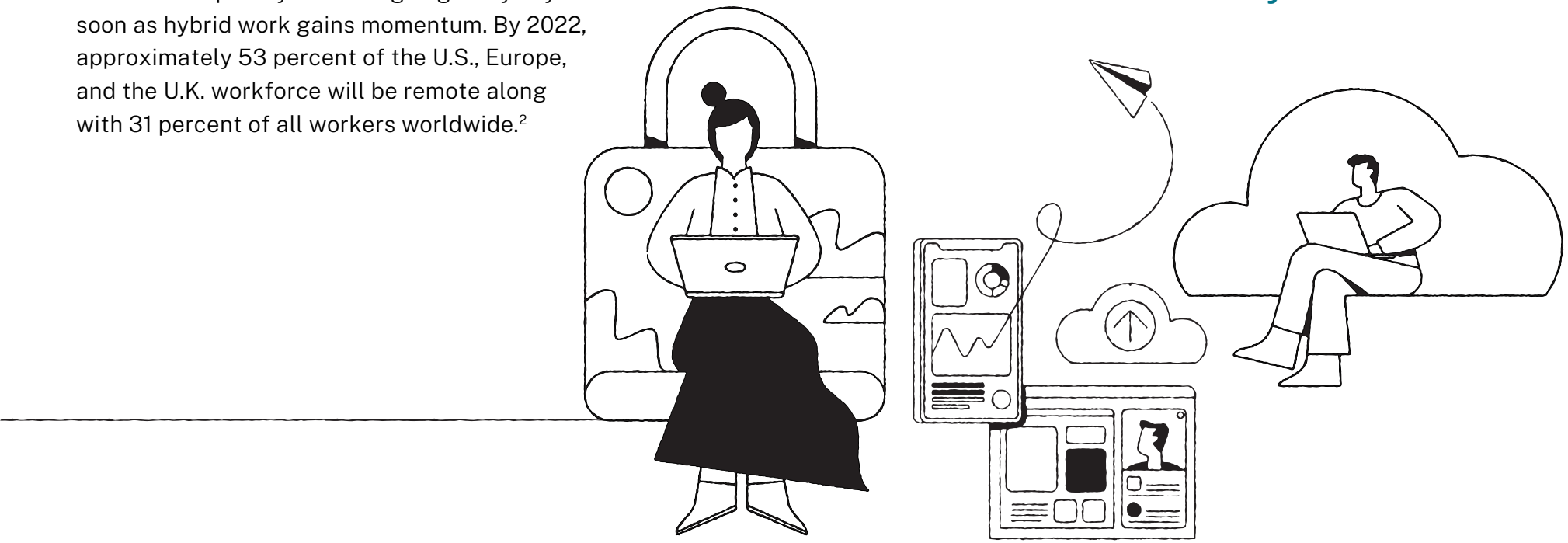
With sophisticated cybersecurity threats sharply on the rise, securing a vastly disparate and distributed workforce is becoming tougher every day. IT teams are challenged with the complexity of safeguarding devices, apps, and the infrastructure for hundreds or thousands of new remote employees. Many organizations simply can't keep up and some ninety percent of security leaders believe they're falling short in addressing cyber risks.[1]

And this complexity won't be going away anytime soon as hybrid work gains momentum. By 2022, approximately 53 percent of the U.S., Europe, and the U.K. workforce will be remote along with 31 percent of all workers worldwide.[2]

As this complexity grows, it's making the enterprise increasingly vulnerable. With more entryways and points of interaction than ever, cybercriminals have more targets and a better chance of exploiting vulnerabilities. There's also more likelihood that inconsistent security measures can open the door for cyberthreats that can spread rapidly once any entry point has been compromised.

90%

of security leaders believe they're falling short in addressing cyber risks.



Today's security landscape is fragmented

Most vendors only offer point solutions at either the device, the app, or at the perimeter. They don't deliver a security model that extends end to end. To cope, IT teams end up collecting multiple solutions from multiple vendors to manage security risks at every level.

This complex security ecosystem and the broad threat surface makes it very complex even for seasoned IT teams to appropriately manage all aspects of enterprise IT security. Additionally, because these tools typically aren't pre-integrated, they lack the unified visibility and control required to efficiently detect and respond to threats.

Adding to these challenges, the demand for security skills is far outpacing the supply. Forty-two percent of system administrators report they don't have sufficient staff to manage threats, and 39 percent say their teams have a security skills gap.[3]

In light of so many concerns, it's clear that the traditional approaches to security aren't going to cut it. The answer to reducing security risks in this incredibly complex era is not adding more tools, more hardware, and more skills for IT teams to master.

29%

of organizations use between 31 and 50 security tools, and 23 percent use 50 to 100.[4]

65%

of IT professionals say that too many security tools are a key barrier to increased cybersecurity.[5]

42%

of system administrators report they don't have sufficient staff to manage threats, and 39 percent say their teams have a security skills gap.[6]

Security needs a new, scalable paradigm

To achieve hybrid work scalability and visibility, you need to take an integrated, comprehensive approach to security. By consolidating vendor security solutions, you improve end to end, multi-layered security, which not only frees up expensive IT resources, but also provides better visibility into potential security risks.

Add automation, AI, and machine learning to these tools to flag any unusual activity for human attention, and IT can take back more time and reduce the dependency on manual monitoring.

What would the ideal multi-layered security platform look like? Essentially, it would protect people, devices, apps, data, and the network.

- **Secure by design devices** that ensures users and data are protected regardless of the attack vector—whether malware tries to enter from a USB stick, a LAN connection, or an internet connection.

- **Protection at the app and desktop level** that ensures that apps are free from malware and ransomware, and are enabled with identity-aware, access controls.

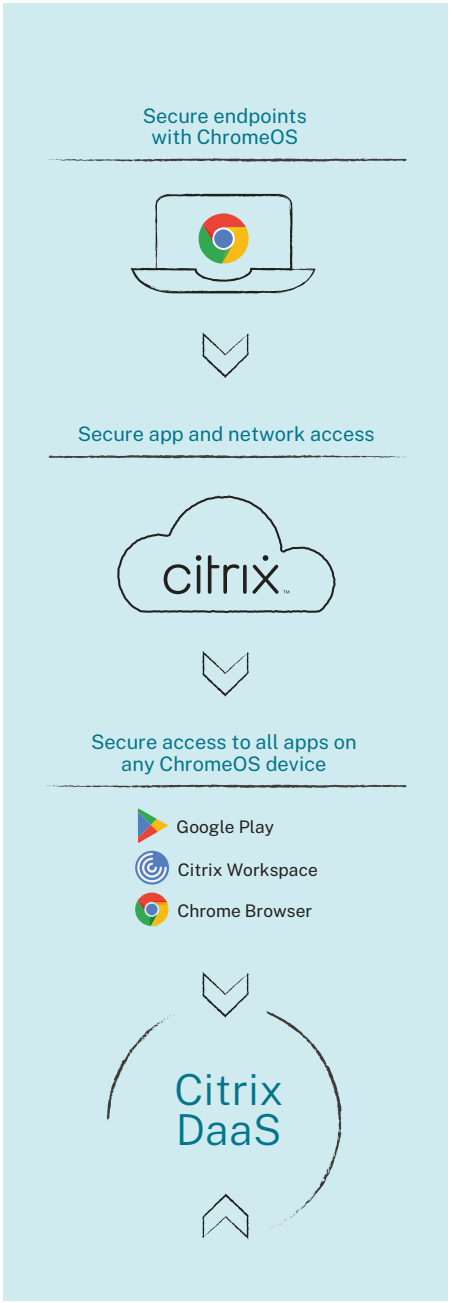
- **Cloud-delivered, app and network security** that sits between devices and the applications and websites being accessed, controlling who gets access to what, and under what conditions.

How can Citrix and ChromeOS help?

Multi-layered security — From devices to the cloud

Citrix and ChromeOS share a common vision to simplify IT for agility and scale. Together, they deliver a combined solution that provides a cloud-native, multi-layered approach to security and app delivery that relieves multiple IT administrative burdens and streamlines management across devices, apps, and infrastructure.

Citrix DaaS solutions and ChromeOS are natively compatible so that IT doesn't need to develop manual integrations. Citrix also broadens the types of apps that can be used on ChromeOS devices to include Windows, Linux, and even legacy apps, simplifies Windows desktop management, and provides granular policy controls. Plus, zero touch provisioning and automated security monitoring further reduce the IT burden.



Citrix and ChromeOS simplify and strengthen security at multiple levels:

1

Endpoint devices.
ChromeOS devices provide robust cyberthreat protection with a read-only OS, built-in encryption, and automated updates with the latest security intelligence.

2

Apps and desktops.
Citrix DaaS solutions provide employees with access to any type of app or desktop, virtually and securely, from the cloud, so nothing is stored on the physical device.

3

Network and app security.
Citrix Secure Internet Access and Citrix Secure Private Access add layers of protection between ChromeOS devices and the applications or websites being accessed.

1 Endpoint devices

Endpoint security solutions work to identify and quarantine a threat after it has already infected a device. With ChromeOS, threats are blocked from ever reaching devices.

In fact, Google has never reported a ransomware attack on any ChromeOS device.

Built-in device security on ChromeOS

Read-only operating system

ChromeOS devices have a hardened, read-only OS that protects against a dangerous class of attacks, helping IT avoid the tedious work of remediating compromised devices and firmware.

Encrypted data and settings

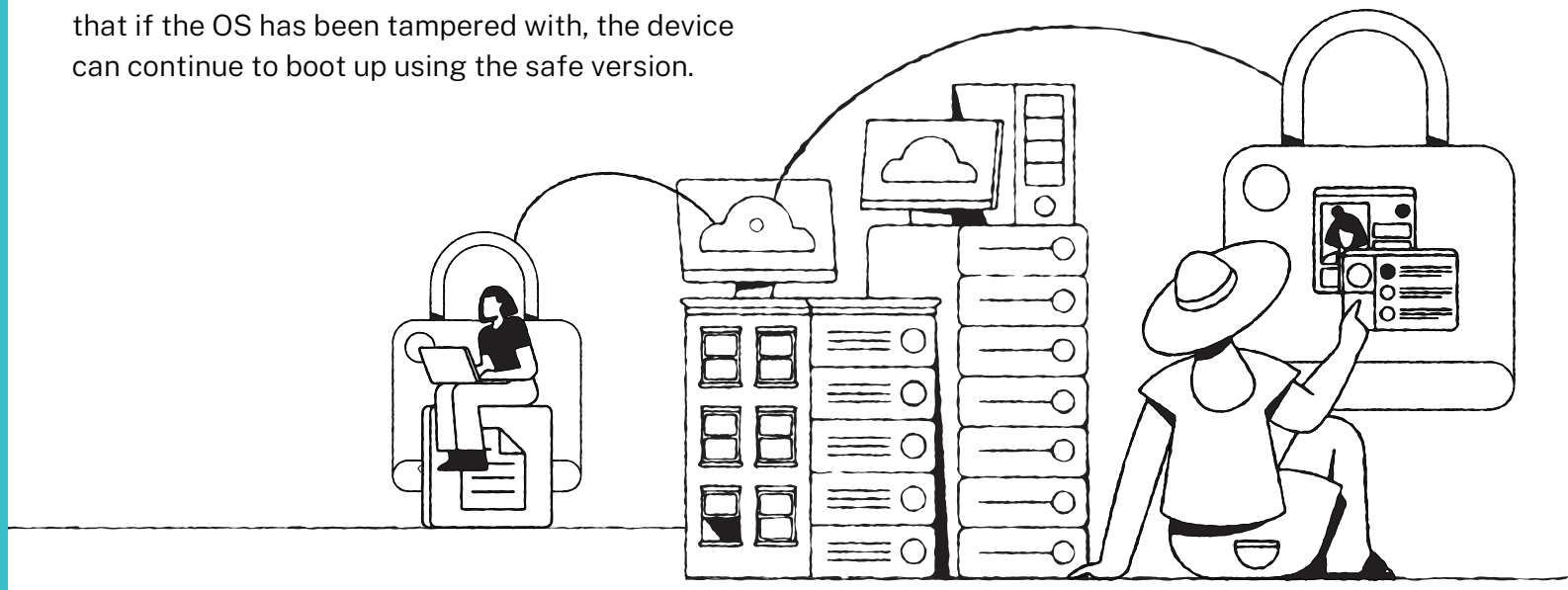
All ChromeOS devices encrypt user data and settings by default with a unique key that cannot be disabled.

Verified boot

Every time the device turns on, ChromeOS's verified boot ensures that the device has not been tampered with or corrupted in any way. Each ChromeOS device has two versions of the OS so that if the OS has been tampered with, the device can continue to boot up using the safe version.

Automated security updates

Regular security, firmware, and feature updates happen automatically in the background and can be applied on reboot, taking a matter of seconds to complete. This ensures devices are always protected with the latest threat intelligence. It also eliminates downtime and the headaches involved in routine updates of operating system components for both IT teams and employees.



1 Endpoint devices

How Citrix and ChromeOS work together

Streamlined device management

Administration of ChromeOS devices and Citrix DaaS solutions is accomplished through cloud-delivered administrative consoles. Chrome Enterprise Management is integrated with Citrix so IT can define policies, access levels, and license entitlements.

Zero touch device provisioning

Employees or new devices can be brought on board with minimal IT involvement. Citrix DaaS solutions on ChromeOS devices can be centrally pushed to devices remotely. No manual imaging is required on ChromeOS devices. The result is a zero touch “pre-provisioned” device that includes the Citrix Workspace app and the employee’s unique apps and desktops.

Cloud data protection

IT can be confident that data is secure if an employee's device is lost or stolen. With Citrix and ChromeOS, nothing is stored on the device — all applications and data are stored in the cloud and securely accessed using Citrix Workspace app. If a device is ever lost, damaged, or stolen, an IT admin only needs to remotely wipe the device and ship out a new one. The employee simply picks up where they left off without transferring any files and data or relying on IT for setup.

2 App and Desktops

Citrix DaaS solutions on ChromeOS provide a joint approach for securing applications and application infrastructure. Citrix provides virtualized app and desktop access on ChromeOS devices, while streamlining IT management.

Built-in app protection with Citrix DaaS solutions and ChromeOS

Apps of any type

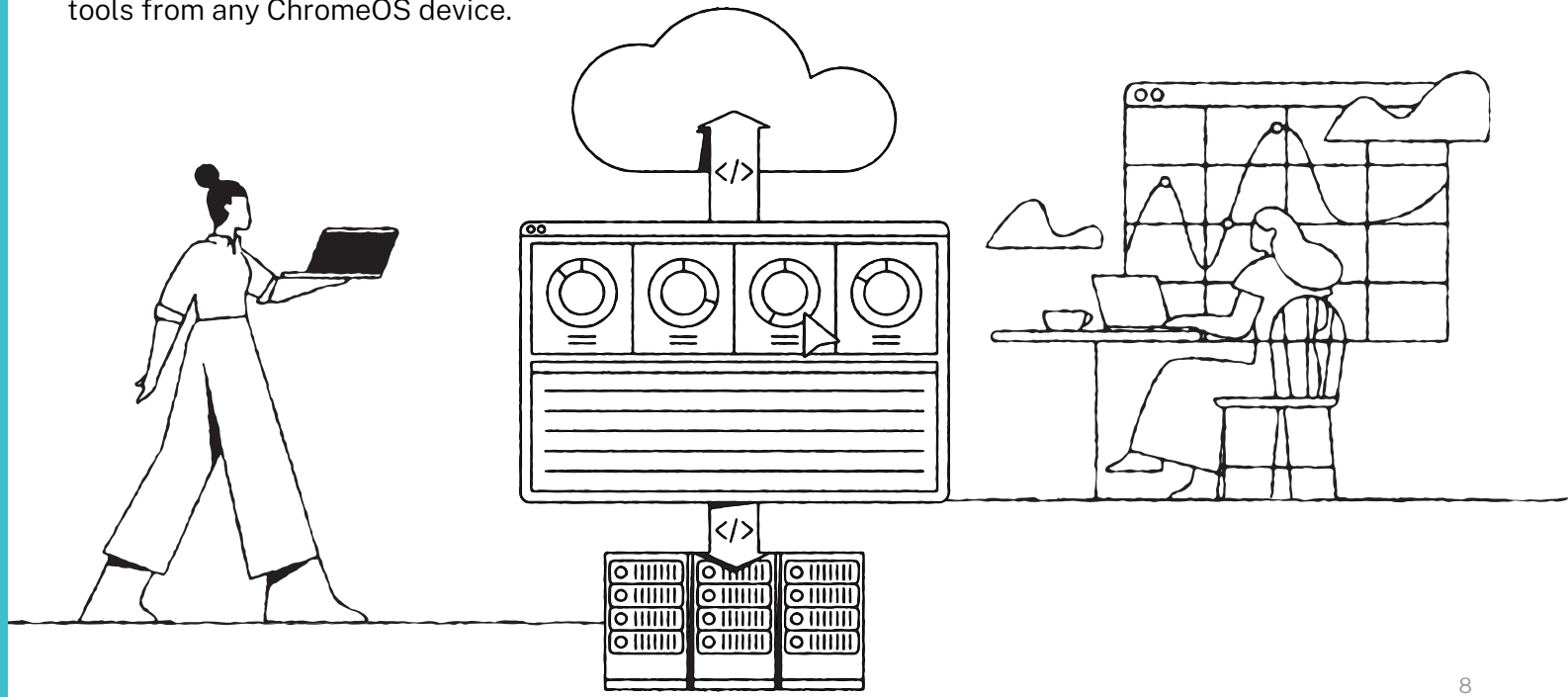
Citrix enables IT to deliver on-demand apps of any type to any ChromeOS device. This solution provides an inherently secure architecture for providing remote access to business-critical applications, including legacy and full-featured Windows apps and Linux, regardless of the operating system the apps were designed for.

High-powered secure desktops

Citrix DaaS solutions provide users with powerful, full-feature Windows or Linux virtual desktops that are completely secure from the device that launches it. IT admins can configure policies to restrict user access to only their Citrix virtual desktop, ensuring all work happens in a secure, monitored environment.

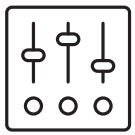
Citrix Workspace app

Citrix Workspace app provides employees with simple, secure one-click access to virtualized apps and desktops, files, SaaS apps, and tools from any ChromeOS device.



2 App and Desktops

How Citrix DaaS solutions and ChromeOS work together



Centralized security management and app provisioning

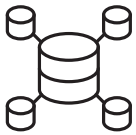
A centralized management plane provides IT teams with easy-to-use granular control over app and desktop security policies. Citrix DaaS monitoring and management solutions enable IT to push security updates for applications and desktops to every ChromeOS device, keeping employees productive while their environments stay secure.

Single Sign-On

IT can configure SSO from the ChromeOS device to go directly into the Citrix Workspace app. This way, once a user logs into a ChromeOS device, they are instantly launched into their unique, productive workspace without the multiple, often frustrating, security sign-ins that other solutions require.

Streamlined, secure user access

The Citrix Workspace experience provides ChromeOS users with a unified, customized view of their virtual apps and desktops by simply logging in through the Citrix Workspace app.



Simplified audits and compliance alignment

Citrix DaaS solutions on ChromeOS simplify audits and regulatory compliance by providing investigators with a centralized audit trail for determining who accessed what applications and data. This, alongside a robust set of industry certifications such as SOC 2 Type 2, ISO 27001, and HIPAA, makes it easy for IT to leverage ChromeOS devices and Citrix DaaS solutions to adhere to strict industry compliance guidelines.

3 Network and app security

Citrix provides additional layers of security to protect ChromeOS devices as they connect to and from the network. These layers further protect the organization from ransomware and malware, which safeguards backend infrastructure from the risk of data exfiltration.

Granular, multi-layered security

Citrix Secure Internet Access

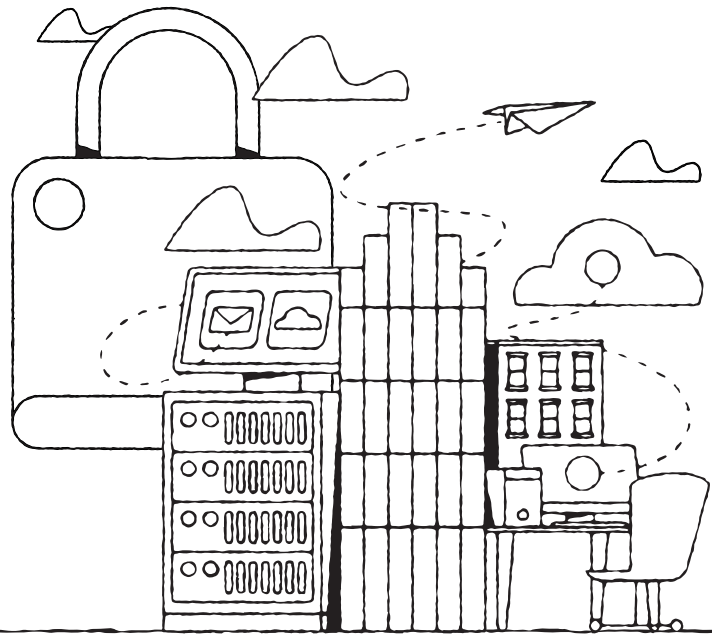
Citrix Secure Internet Access is a comprehensive, cloud-delivered security service that replaces traditional, on-premises security appliances. This Citrix DaaS security solution protects direct internet access to SaaS applications and the web, and includes a firewall, Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), malware protection, data loss prevention (DLP), and sandboxing.

Citrix Secure Private Access

Citrix Secure Private Access provides zero trust network access (ZTNA) with adaptive authentication and single sign-on (SSO) to IT sanctioned applications. This Citrix DaaS security solution goes beyond traditional SSO capabilities by providing enhanced cloud-based security controls for SaaS and enterprise web apps, which enable IT to provide conditional access to cloud apps as well as limit user actions according to admin-governed access policies.

Citrix Analytics for Security

Citrix Analytics for Security continuously assesses the behavior of Citrix DaaS users to proactively detect and resolve security threats. This Citrix DaaS security solution generates individualized user risk scores based on user behavior to surface potential high-risk users. It detects malicious user activity and prevents harm to the business with prescriptive, automated remediation actions.



3 Network and app security

How Citrix and ChromeOS work together

Cloud-delivered security

Citrix Secure Internet Access is positioned between ChromeOS devices, your apps, and the web. This means both your infrastructure and your users are always protected from compromised internet sites, malware, zero-day attacks, ransomware, and other external threats. Citrix Secure Internet Access is a globally available and scalable cloud solution that's delivered through over 100 points of presence (PoP). Cloud delivery simplifies IT administration, while also ensuring there's no added latency from backhauled connections. Employees remain secure regardless of their physical location without any impact on their experience.

Automated security enforcement

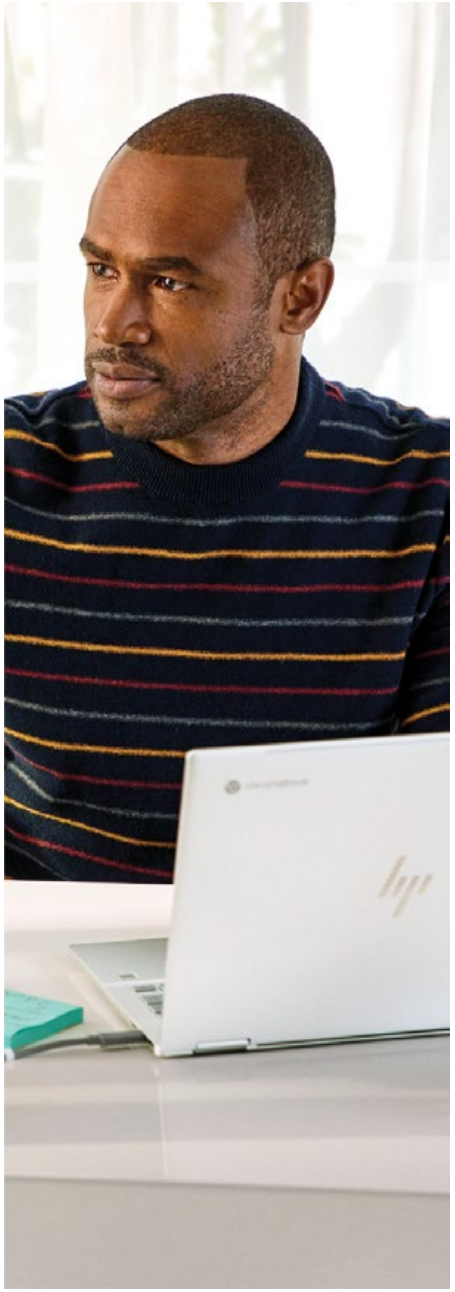
Citrix Analytics for Security provides insights into ChromeOS devices, applications, and networks that help automate security enforcements based on user behavior and anomalies detected. This automation provides timely security enforcement to reduce the risk of costly security breaches while also reducing the IT burden.

VPN-less, zero trust security

Citrix Secure Private Access delivers deeper layers of security for Citrix DaaS by providing protection from malicious content like keyloggers and screen capturing malware, browser isolation policies, and contextual, adaptive authentication features that consider multiple real-time user conditions before authorizing user access to applications. With Citrix Secure Private Access, ChromeOS users can connect to the network and work outside of its perimeter on private corporate applications and SaaS applications while staying completely secure. Meanwhile, IT benefits from enhanced cloud-based control of ChromeOS user access to SaaS and enterprise-hosted web apps using a solution that's based on the principles of zero trust.

Simplicity drives positive change

Moving to a hybrid work architecture that is inherently more secure significantly reduces costs associated with possible data breaches. Beyond that, there are numerous long-term benefits and savings associated with simplifying and modernizing security infrastructure.



Gain business agility

Consolidating IT systems and security vendors helps create an agile environment that's easily adaptable to today's fast-evolving business world. As a result, the enterprise can scale up hybrid work on-demand and be ready for any contingency.

Reduce TCO

By adopting ChromeOS devices, enterprises can reduce deployment, upgrade, and training costs that result in a savings of up to $482 per device per year.[7] Adding to that, Citrix DaaS reliability and ease of use reduces help-desk calls by about 33 percent and cuts remaining call times in half.[8]

Support IT innovation

Removing complexity frees IT teams to work on new, innovative digital services. They also gain an opportunity to focus on other important security initiatives, like proactive cybersecurity posture analyses, delivering new and strategic digital services, and more.

Scale back data center hardware

Citrix DaaS solutions and Chrome Enterprise are 100 percent cloud-delivered. By replacing data center hardware with cloud-delivered services, enterprises can reduce infrastructure costs and operational overhead. This also allows enterprises to reduce their carbon footprint.

Citrix and ChromeOS, stronger together

Citrix and ChromeOS deliver a comprehensive, multi-layered security ecosystem that protects devices, workspaces, infrastructure, applications, and content. Together, they strengthen security across the enterprise by simplifying protection at every step. Employees benefit from secure ChromeOS devices that deliver high performing, streamlined access to apps and desktops without additional security sign-ins. IT teams gain access to cloud-based granular security management tools, as well as automated monitoring tools for security visibility. And the enterprise gets a secure, hybrid work solution that not only prevents security breaches, but also significantly reduces IT maintenance and operational costs.

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

Source:

1 IDG. “2021 IDG Security Priorities Study,” October 2021
2 Gartner. “Hybrid and Remote Workers Change How They Use IT Equipment,” July 2021
3 Netwirks. “2021 Sysadmin Report,” July, 2021
4 IBM. “Cyber Resilient Organization Study 2021,” July 2021
5 Ibid.
6 Ibid.
7 The Enterprise Strategy Group, Inc. “Quantifying the Value of Google Chromebooks with Chrome Enterprise Upgrade,” June 2018
8 Citrix. “What are the cost benefits of DaaS?”