citrix

Solution Brief

Citrix App Protection

Protecting company data accessed through unmanaged devices

While it may not have been critical at the beginning of the year, business continuity planning (BCP) has become a top priority for organizations everywhere. The pandemic forced a massive shift in IT strategies while also altering how and where we work. While many organizations developed these plans on the fly to keep their employees secure, engaged, and productive during a pandemic, ultimately, those plans became part of a long-term strategy to support remote work. These remote work contingency plans can be activated at any time, for weather, geopolitical, or health and safety events, or to improve the employee experience. The first step in many BCPs is to determine how to provide employees with consistent access to mission-critical apps and files. The next, and equally as important, step is to keep the data in those apps and files secure.

When developing a security strategy to support a BCP, a plan for unmanaged devices accessing corporate resources is at the top of every list. Many organizations still rely on desktop devices in the office, but it isn't practical to send workers home with desktops if they work remotely. Employees that work from home are asked to work on personal devices, despite IT departments not having the ability to apply security controls or get insight into the health of those devices.

Even prior to the pandemic, many organizations implemented bring-your-own device (BYOD) programs. BYOD programs are embraced by IT as they lessen the administrative burden of device management.

These strategies don't come without tradeoffs, though. Many organizations have implemented zero trust network access, with the ultimate goal of better protecting their data. The inability to place security controls or detect potential danger from an unmanaged device increases the chances of a data breach, undermining the security strategy.
While most organizations secure corporate-owned devices carefully through anti-virus software, endpoint scans, and more, many end users don't apply the same level of security to their personal devices.
This leaves IT searching for tools that can deliver on the BCP, zero trust network access, and BYOD in an effort to create a best-in-class employee experience that keeps data secure.

Assessing common threats

Keyloggers are one of the oldest forms of malware. Even as malware has evolved and become more sophisticated, keyloggers remain a popular form of malware for a simple reason: they're effective. In fact, keyloggers are so popular that they are in the top three types of malware found in security breaches. Keyloggers work silently on infected devices, sending each keystroke back to an attacker. This exfiltrated data can be used by the attacker to harvest sensitive data like usernames, passwords, or critical corporate information. This creates significant risk for organizations, as attackers can access corporate systems and data without restriction.

45 percent of breaches occur in the cloud but breaches cost less in hybrid environments*

Screenshot malware also poses a risk to organizations. When installed, this malware secretly and periodically captures what's presented on the user's screen. When employees access sensitive company data like financial information, a product roadmap, or a customer list, attackers can grab the information and sell it to the highest bidder. More importantly, many users may access the personal information of other employees, customers, or partners. This can include social security or national identification numbers, bank account information, or IP addresses. When this data kind of data is leaked, the consequences are catastrophic. Not only may the company violate government regulations, but consumers and customers lose trust in the company.

Accidental screen sharing also poses risk. Many employees use web conferencing tools for virtual get-togethers with friends and family. This creates risk because a device used for both personal and business reasons can have a lot of personal and business data. For example, consider an employee wrapping up his work week on his BYO device by finishing a report in a virtual app that houses business-critical data. He launches a web conferencing app to join a virtual happy hour with friends, including some who work for a competitor. But, he forgets to close his business app before joining. He shares his screen with the intention of sharing personal pictures, but he accidentally shows his business app with company data, exposing it to everyone in the meeting.

App Protection secures data on unmanaged devices

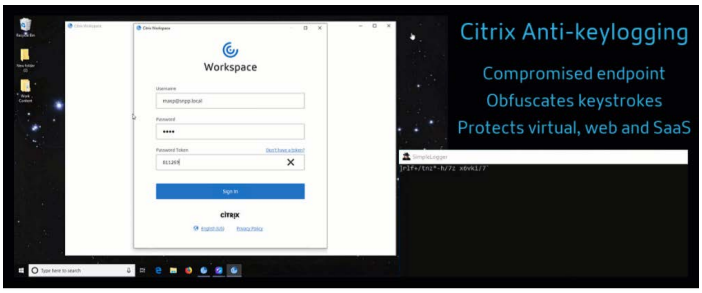
App Protection secures corporate data by defending against keylogging malware, screenshot malware, accidental screen sharing, and DLL injection attacks. This enables end users to securely access corporate resources in Citrix Workspace through any device, even one that's unmanaged. IT can rest easy knowing their data won't be exfiltrated, even if the end user's device is infected with malware. This can help IT institute BCP and BYOD programs at their organization while mitigating the risks associated with unmanaged devices accessing corporate apps and data.

The average cost of a data breach in 2022 was $4.35 million*

Anti-keylogging

With encryption, App Protection's anti-keylogging capabilities scramble keystrokes for both physical and on-screen keyboards. The anti-keylogging feature encrypts the text before any keylogging tool can access it from the kernel/OS level. A keylogger installed on the client endpoint, reading the data from the OS/driver, would capture hashed text instead of the keystrokes the user is typing.

App protection policies are active not only for published applications and desktops but for Citrix Workspace authentication dialogs as well. Your Citrix Workspace is protected from the moment when users open the first authentication dialog.



App Protection scrambles keystrokes, returning indecipherable text to keyloggers. On the left, you can see the credentials entered into the Citrix Workspace app. On the right, the text returned to the keylogger installed on the device.

Anti-DLL injection

Unauthorized dynamic-link libraries (DLL) injections are another common security attack that injects untrusted modules into the application. The Citrix workspace app can detect DLL injections on Windows and block those attacks, keeping business data secure. There is very little disruption for the user in the case of a blocked DLL injection as well, the workspace app will inform the user of the blocked attack via a pop-up notification and then the user can continue to use the Workspace app as usual.

Anti-Screen capture

Social engineering attacks can also be thwarted by App Protection's anti-screen capture technology in situations where attackers pretend they're IT staff and gain access to machines that store sensitive information. Anti-screen capture prevents an app from attempting to take a screenshot of or a recording of the screen within a virtual app or desktop session. The screen capture software would be unable to detect content within the capture region. The area selected by the app is grayed out or the app captures nothing instead of the screen that it expects to copy.

Another use case for anti-screen capture is preventing the sharing of sensitive data in a virtual meeting or web conferencing applications like Goto-meeting, Microsoft Teams, or Zoom. Mis-delivery (sharing data with the wrong recipient or publishing data to unintended audiences) is a common threat action variety that plagues many industries. Mis-delivery is a primary source of security incidents. Your data and applications should be protected not only from external threats, but also from your own employees.

App Protection prevents unintended sharing by returning a blank screen in web conferences when apps are protected. This ensures that sensitive data is not accidentally leaked from the organization. This can help with compliance in regulated industries, as the intention is not considered when disclosing a data breach.

Contextual app protection

Storefront and workspace also have contextual app protection, which allows administrators to ensure the correct level of access and protection by creating dynamic policies that adapt to a user's context, device, or network posture. This allows admins to apply specific policies depending on if an employee is out of the office, or if an endpoint analysis scan is unsuccessful. Contextual app protection helps reduce the need for manual security intervention, since security policies are applied automatically, reducing the burden on IT.

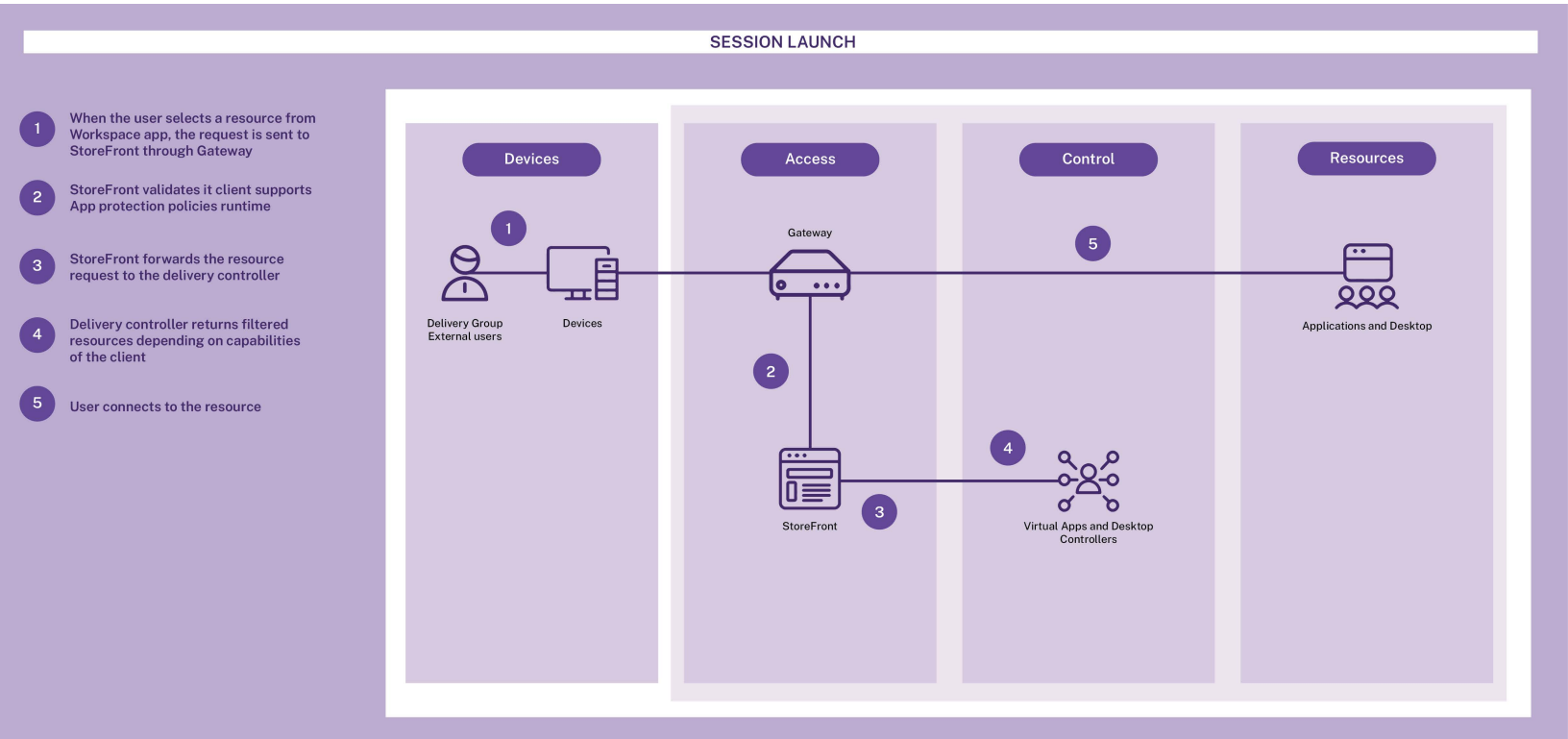
How does it work?

App Protection policies protect client endpoints running Windows, Linux, and macOS operating systems. App Protection policies work by controlling access to specific API calls of the underlying OS, required to capture screens or keyboard presses. So, App Protection policies can provide protection even against custom and purpose-built hacker tools.

When a user logs into Workspace or Storefront, the security capabilities of the endpoint are assessed and matched against available resources. Applications and desktops protected by App Protection policies are visible only if an endpoint meets the security requirements. One such requirement is to check if the App Protection components are installed. If you use hybrid launch or browser-based access to the Workspace app, there is now additional support for App Protection for Workspace for Web users and Storefront for Web customers with the Citrix Workspace Web extension and Storefront customizations respectively.
This gives admins more flexibility with how they configure their environments with App Protection.

It is often assumed that you have to sacrifice user experience to get better security. App Protection policies are implemented in a way that is seamless to the end users:

- Protected resources are hidden from unauthorized users
- Anti-screen capture is enabled only when the protected window is on-screen (users can minimize it if they need to take a screenshot of an unprotected window)
- Anti-keylogging protection is enabled only when the protected window is in focus



Summary

Work is forever changed. The days of IT instituting a "castle-and-moat" strategy for securing their apps, data, and employees no longer apply. IT security strategy must be modified to meet the new reality, including a plan for safeguarding corporate resources accessed from unmanaged devices. Unmanaged devices create risk as they may be infected with screenshot or keylogger malware, which can exfiltrate corporate data. App Protection scrambles keystrokes entered into a device, returning unusable, hashed text to the attacker. It also returns screenshots as blank screens, protecting sensitive corporate data that was presented on the device.

**Zorabedian, John. (July 27, 2022) What's New in the 2022 Cost of a Data Breach Report. Security Intelligence. https://securityintelligence.com/posts/whats-new-2022-cost-of-a-data-breach-report/*

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