citrix

Solution Brief

Citrix App Protection

Protecting company data accessed through unmanaged devices

Overview

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 coronavirus 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, they can become part of a long-term strategy to support remote work. These plans can be activated anytime, whether you're facing a weather, geopolitical, or health and safety event, or just improving employee experience. The first step in many BCPs is to determine how to keep employees productive by providing them with access to their 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 BCP, a plan for unmanaged devices accessing corporate resources is at the top of nearly every list. Many organizations still rely on desktop devices in the office, and it isn't practical to send workers home with them when the BCP is implemented and employees are working remotely. Employees 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 were implementing BYOD programs. BYOD programs are welcomed by IT as they lessen the administrative burden of device management. Workers love them as well, as they get to use their favorite device for work, enhancing the employee experience.

These strategies don't come without tradeoffs, though. Many organizations are implementing zero trust, with data protection as the top outcome to deliver. The inability to place security controls or determine potential dangers from an unmanaged device increases the chances of a data breach, undermining the holistic strategy. While most organizations secure corporate-owned devices carefully through anti-virus software, endpoint scans, and MDM, many end users don't apply the same level of security to their personal endpoints. This leaves IT searching for tools that balance BCP, zero trust, and BYOD in an effort to deliver a best-in-class employee experience that keeps data secure.

Assessing the threats

Keyloggers are one of the oldest forms of malware. Even as malware has evolved and become more sophisticated, keyloggers have persisted 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. Keylogger malware works silently on infected devices, sending each key stroke 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.

1 in 13 web requests leads to malware

Screenshot malware also creates elevated risk for organizations. When installed, this malware secretly and periodically captures what's presented on the user's screen. When employees access sensitive company data like company financials, 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 personally identifiable 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 is exfiltrated, the company may be out of compliance with regulations like the GDPR. Companies in fields like healthcare or finance also have to consider industry regulations. A data breach may put them out of compliance with those regulations, leading to significant fines.

Accidental screen sharing also poses risk. Many people are now using web conferencing tools for virtual get-togethers with friends and family. This also creates risk because device use for personal and business reasons gets blurred. 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 at 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

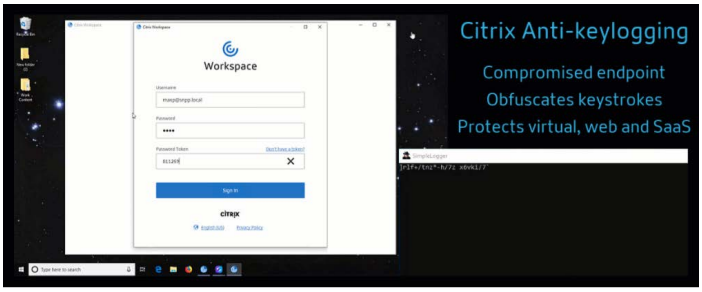
App Protection secures corporate data by defending against key logging malware, screenshot malware, and accidental screen sharing. This enables end users to securely access their corporate resources in Citrix Workspace through any device, even one that's unmanaged. IT can rest easy knowing their data 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 is $3.92 milion

Anti-keylogging

With encryption, App Protection's anti-keylogging capabilities scramble the text the user is typing 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 your users open the first authentication dialog.



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

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 have sensitive corporate information on them. 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 section that it expects to copy. The anti-screen capture feature applies to snip and sketch, snipping tool, and "Shift+Ctrl+Print Screen" on Windows. The protection extends to files from Citrix Files or any other connectors like Google Drive or Microsoft OneDrive that are accessed from within Citrix Workspace app. The apps are protected from screen scrapers, as are all the microapps and their notifications from within Workspace.

Another use case for anti-screen capture is preventing sharing of sensitive data in a virtual meeting or web conferencing applications like GoToMeeting, Microsoft Teams or Zoom. Misdelivery (sharing data with the wrong recipient or publishing data to unintended audiences) is a common threat action variety that plagues many industries. In 2019, misdelivery has been a primary source of security incidents in the healthcare industry. Your data and applications should be protected not only from external threats, but also from your own employees. Internal actors have been involved in 34% of security incidents in 2019, but this number is higher in some industries. For example 45% of breaches in the education industry and a whopping 59% of breaches in healthcare were attributed to an internal threat.

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.

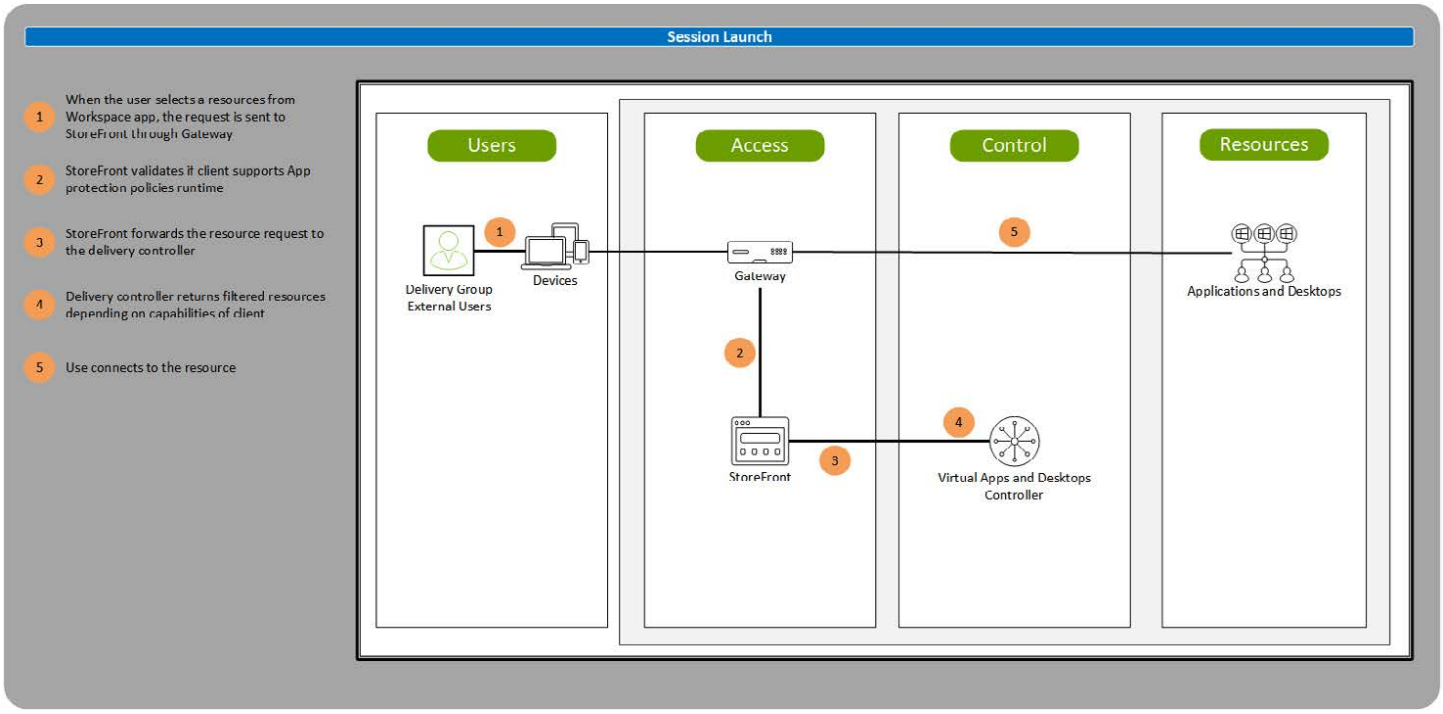
How does it work?

App Protection policies protect client endpoints running Windows 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. However, as OSes evolve, new ways of capturing screens and logging keys can emerge. While Citrix continues to identify and address, it cannot guarantee full protection in specific configurations and deployments.

When a user logs into StoreFront, 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 a check if the App Protection components are installed.

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 users if they cannot access them because they client does not support App Protection policies
- Anti-screen capture is enabled only when protected window is on-screen (users can minimize it if they need to take screenshot of unprotected window)
- Anti-keylogging protection is enabled only when 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.

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