Citrix Ups Security Game

New feature in Citrix Virtual Apps and Desktops provides protection for unmanaged personal devices fueling remote work

FORT LAUDERDALE, Fla. – April 30, 2020 – When remote work moved from something a few people did on occasion to a mandate for nearly all employees, companies around the world scrambled to scale up their resources and enable it. Many fell short, leaving employees to use personal devices to access the systems and information they need to do their jobs. And that's created a gaping security hole. To help plug it, Citrix Systems, Inc. (NASDAQ:CTXS), has launched App Protection, which enables companies to protect apps and data on unmanaged endpoints and ensure their corporate systems and information remain safe.

"Endpoints are the penultimate control point for the implementation of device, application, and data security. The rapid acceleration of remote work sparked by the COVID-19 pandemic and proliferation of unmanaged personal devices being used for business has created a special challenge, as decentralization is not the friend of security," said Frank Dickson, Program Vice President, Security & Trust, IDC. "And specialized and sophisticated tools are required to overcome it."

Dion Hinchcliffe, VP and Principal Analyst at Constellation Research – and Executive Fellow, Tuck School of Business, Center for Digital Strategies, agrees. "The recent mass global shift to remote work has in part been enabled by the ability to use available devices at hand, including unmanaged ones. Yet this has opened up a vast new cybersecurity attack surface area and put even more burdens on workers struggling to adapt to their new environment," he says. "App Protection provides an invaluable safety net so both workers and employers can rest assured that remote work devices are not leaking critical information, allowing everyone to focus on what matters most: a safe, secure, and productive digital workplace."

Business is Now Personal

As employees around the world adjust to the new normal of working from home, many are using whichever endpoint gives them the quickest access to the resources they need to get work done. And this often includes personal devices such as laptops, tablets and phones. "Key logging and screen capture malware are common on these endpoints and provide bad actors with easy entry to corporate networks and sensitive information," said Eric Kenney, Senior Product Marketing Manager, Citrix.

Malware Beware

When present on a device, key logging malware captures each key stroke entered by a user, including user names and passwords. Screen-capture malware periodically takes a snapshot of the user's screen, saving it to a hidden folder on the device or directly uploading it to the attacker's server where the information can be exploited. App Protection is uniquely designed to prevent this.

A Blank Stare

The unique feature thwarts keylogging and screen-capturing malware that may live on personal devices by scrambling keystrokes entered into a device and sending the attacker undecipherable text. It also prevents data exfiltration from screen shot malware by turning all screen shots into blank pictures. With App Protection enabled, employees can stay productive by working on a personal, unmanaged endpoint without sacrificing security. To see App Protection in action and learn more about how your organization can leverage the capability to keep your employees, their devices and your corporate systems and information safe, click here.

# # #