Customer FAQs:
Acquisition of deviceTRUST and Strong Network and general availability of Citrix® Secure Private Access for hybrid environments

Contents

1. What is Cloud Software Group announcing?

Cloud Software Group is announcing the acquisition of two companies, deviceTRUST GmbH and strong.network S.A., that provide enterprise security solutions in addition to announcing the general availability of Citrix® Secure Private Access for hybrid environments. For details about the announcement, [see the press release](#).

2. What are the two companies that Cloud Software Group has acquired?

Cloud Software Group has completed the acquisition of two companies:

deviceTRUST is a Germany-based software startup that provides continuous real-time contextual access based on real-time security conditions to give organizations greater control over their network access.

Strong Network is a Switzerland-based software startup that provides secure cloud development environments to solve the IT efficiency and security problems of running a distributed code development team.

Both acquisitions closed for an undisclosed price. Through the acquisitions of deviceTRUST and Strong Network, Citrix customers will gain real-time protection for their VDI and DaaS users and secure cloud development environments for developers.

3. What value does deviceTRUST add to the Citrix platform?

deviceTRUST expands existing Citrix zero-trust capabilities by providing real-time continuous monitoring and policy enforcement for virtualized sessions in Citrix Virtual Apps and Desktops™ and DaaS environments and for local application access. It can be used on top of Azure Virtual Desktop and Windows 365 as well, providing zero-trust security within a virtualized session.

The deviceTRUST® technology further enhances existing Citrix capabilities for securing unmanaged devices.

4. What value does Strong Network add to the Citrix platform?

Strong Network adds new capabilities to the Citrix platform by providing secure browser-based cloud development environments (CDEs) where application developers do their coding work in the cloud from either unmanaged or managed devices. Strong Network also supports local integrated development environments (IDEs) for on-premises deployments, including air-gapped environments.

Built to support a distributed developer workforce at scale, the Strong Network™ platform provides ready-to-go coding environments for modern cloud-native application development. It also reduces the cost of remotely onboarding developers, which includes substantially reducing the infrastructure cost of delivering traditional developer desktops via VDI or DaaS.

In addition to securing and accelerating developer workflows, Strong Network provides automation and governance capabilities for DevOps and DevSecOps, including comprehensive visibility and control throughout the software development lifecycle (SDLC) to restrict access to data and to secure development assets in compliance with the National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO) security standards.

5. What value does Citrix Secure Private Access for hybrid deployment add to the Citrix platform?

Citrix Secure Private Access for hybrid deployment is a zero trust network access (ZTNA) solution that provides secure access to private web and client-server applications by leveraging existing infrastructure with NetScaler® Gateway on-premises, Citrix StoreFront™ on-premises, and cloud-based management.

The hybrid deployment mode for Citrix Secure Private Access gives you end-to-end control so that you can route sensitive application traffic through your own network infrastructure while leveraging the simplicity of cloud for management and observability. This end-to-end control helps you meet regulatory requirements for workloads running in hybrid environments.

6. How does deviceTRUST work?

The deviceTRUST product works by integrating with your existing infrastructure, such as Active Directory or other identity providers, and leveraging a lightweight agent installed on the VDA and a client extension installed on the endpoints. This agent collects detailed information about the device, including its hardware and software configuration, security posture, and location.

The collected data is then evaluated against pre-defined policies set by your organization. These policies can be granular, allowing you to define specific criteria for access based on factors like device compliance, user role, and location.

When a user attempts to access a protected resource, deviceTRUST intercepts the request and analyzes the device information against the relevant policies. If the device

meets the required criteria, access is granted seamlessly. If not, access can be denied or the user may be prompted to take corrective actions, such as updating antivirus software or connecting to a secure network.

7. How does Strong Network work?

The Strong Network platform provides secure cloud development environments (CDEs) where developers do their work in the cloud from either unmanaged or managed devices.

A CDE is a container or virtual machine (VM) dedicated to software development. Accessing it is similar to connecting to a remote machine through a terminal command window like you would with an SSH client. The remote machine can be a physical host or a virtual process like a container or virtual machine (VM).

The goal of a CDE is to provide developers with a ready-to-use, fully configured development environment. CDEs typically run on a Linux OS together with a series of applications and packages to enable developers to write code online.

Using CDEs enables you to offer a self-service option where developers can access pre-set environments without IT help. These environments include approved software, packages, and computing capabilities provided by the CDE. Self-service access to environments is best for internal employees. Managed access to environments is often the preferred method for contractors or temporary employees.

CDEs can be managed, updated, and enhanced online without accessing the developer's computer, and they can be monitored in real time to obtain productivity and security metrics.

8. How can I access deviceTRUST?

You will receive an entitlement for deviceTRUST in your My Citrix portal where you can download the deviceTRUST software and license file. You will need to install deviceTRUST agents into the VDAs running in Citrix DaaS™ and Citrix Virtual Apps and Desktops.

In addition, a deviceTRUST client extension needs to be installed on the endpoint devices connecting into the virtual delivery agents (VDAs). When this is complete, the deviceTRUST management console can define access policies that will control the

zero-trust policies that are enforced by deviceTRUST. End users will access Citrix as they always have. deviceTRUST will handle the continuous enforcement of the ZTNA policies that you have defined.

9. How can I access Strong Network?

If you are entitled to Strong Network, you can access it within the same Citrix StoreFront portal as existing Windows and macOS environments to provide developers with a single, centralized platform to access all the tools they need.

End users can access the Strong Network platform via web-based integrated development environments (IDEs), local IDEs, or terminals through Citrix® Developer Workspace (CDW).

10. Where can I find deviceTRUST and Strong Network product documentation?

deviceTRUST and Strong Network product documentation will remain at their current documentation sites for the near future:

- [deviceTRUST documentation](#)
- [Strong Network documentation](#)

11. As a current deviceTRUST customer, who should I contact for support?

deviceTRUST customers should contact [Citrix® Support](#) for any support related issues.

12. As a current Strong Network customer, who should I contact for support?

Strong Network customers should continue to contact [Strong Network Support](#).

13. Which Citrix subscriptions include deviceTRUST capabilities?

Starting December 15, 2024, deviceTrust will be available to Citrix customers who have a Citrix Platform License and will be provisioned manually.

Starting mid-January 2025, customers who have either the Citrix Platform License or the Universal Hybrid Multi-Cloud License or legacy DaaS subscription licenses (DaaS,

Universal, CVAD service) will be able to download the deviceTRUST license file from their MyAccount page.

14. Which Citrix subscriptions include Strong Network capabilities?

Starting December 15, 2024, Strong Network will be available to Citrix customers with a Citrix Platform License (CPL) and to Citrix customers with delta CPL pre-entitlements.

Strong Network entitlements are not available with the Universal Hybrid Multi-Cloud License.

15. How do I request a deviceTRUST trial?

If you are not already entitled to deviceTRUST, you may request a trial from your Citrix representative.

16. How do I request a Strong Network trial?

Trials are not currently available for Strong Network, but may be offered in the future. Please contact your Citrix representative for details.

17. How do I request a hybrid Citrix Secure Private Access trial?

Please contact your Citrix representative to request a trial.

---

other countries. All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification.