CITRIX CLOUD SOLUTIONS — DEVICETRUST

deviceTRUST — Boosting Citrix Security with Contextual Access

Citrix

Access to your data centre must be authorised, authenticated, and audited — at the device level, at the network level, and at the application level. deviceTRUST brings all three into real time. Not just at the moment a session starts, but continuously throughout it — reacting the instant anything about the device, network, or location changes.

Real-Time Contextual Access | In-Session Policy Enforcement | Zero Trust — Turbocharged | Acquired by Citrix (Dec 2024) — Now in Citrix UHMC

OAS · Protect. Detect. Recover.

Prepared 11 September 2026

THE CORE CONCEPT

The Critical Difference — Conditional vs Contextual Access

To understand what deviceTRUST does, it helps to understand what it is not. Most organisations are familiar with conditional access — but contextual access is a fundamentally different and more powerful security model.

Conditional access — a gate at the start

- Conditional access checks whether a device meets defined requirements at the moment a session is requested. Is the firewall running? Is antivirus current? Is the device on the approved network? Access granted. The session opens, and the checking stops. From that point on, whatever happens on the device or network is outside the security model's view. A user could disable their firewall, plug in an unauthorised USB drive, or move to a public Wi-Fi network, and the session continues, unchallenged.
- "Your device passed the check at 9:00am. At 10:30am your firewall service stopped. We don't know, and we don't respond."

Contextual access — continuous, real-time enforcement

- deviceTRUST monitors the device context throughout the entire session, not just at the point of entry. Every defined property is continuously re-evaluated: security software state, network location, connected peripherals, geolocation, OS patch level, and more. The moment any context changes in a way that violates policy, deviceTRUST reacts immediately, locking the session, restricting application access, notifying the user, or revoking access entirely. Access is continuously earned, not statically granted.
- "Your device was compliant at 9:00am. At 10:30am your firewall stopped. Session locked. The user sees a notification explaining what needs to be fixed."

PLATFORM OVERVIEW

What Is Citrix deviceTRUST?

deviceTRUST is the contextual security engine that sits inside the Citrix environment — reading device properties in real time, evaluating them against defined policies, and triggering immediate actions when conditions change. Here are the four things every organisation needs to understand about it.

Integrated into Citrix Workspace App

The deviceTRUST Client Extension ships inside Citrix Workspace App 2503 and later, with no separate agent for end users to install. Policies are deployed centrally via Group Policy or the Citrix management infrastructure, making rollout straightforward across an existing Citrix estate.

Continuous — Not Just at Logon

Context is evaluated continuously throughout every active session. If something changes on the device — a firewall is disabled, an unauthorised USB device is inserted, the network location changes, or the device moves to a prohibited country — deviceTRUST detects it immediately and executes the configured response without waiting for the next authentication cycle.

Granular Policy, Granular Response

Responses to context changes are fully configurable, from a user-facing notification and a grace period to remediate, through restricting specific application access, to immediately locking or disconnecting the session. Administrators can define exactly which context change triggers which response, with pre-built templates for common scenarios.

Works Beyond Citrix

While purpose-built for Citrix CVAD and DaaS environments, deviceTRUST also works with Microsoft Azure Virtual Desktop, Remote Desktop Session Host, and local device environments. This means the same contextual security policy can extend across your entire virtual workspace estate, not just Citrix sessions.

BUSINESS CHALLENGES & SOLUTIONS

Four Corporate Security Challenges — and How deviceTRUST Addresses Each

These are the four real-world security challenges that organisations face when delivering virtual applications and desktops to a hybrid workforce, and the specific way deviceTRUST closes each gap.

Corporate Device Enforcement

Unmanaged and unauthorised devices accessing VDI and virtual applications increase the risk of malware, data breaches, and regulatory non-compliance across environments that cannot verify what device is connecting. deviceTRUST ensures that only pre-approved, corporately managed devices, or devices meeting defined compliance criteria, can establish and maintain access to VDI, virtual apps, and DaaS. Access is denied at logon for non-compliant devices, and revoked mid-session if a device falls out of compliance. Unknown or unmanaged devices are stopped before they can reach corporate resources.

Real-Time Network Verification

Users connecting from unsecured or untrusted networks, including public Wi-Fi, home broadband without VPN, or networks outside approved geographies, expose corporate sessions to interception, man-in-the-middle attacks, and data loss. deviceTRUST continuously evaluates the network from which a user is connecting, verifying that it matches trusted network definitions. Access can be denied at logon from unauthorised networks, and actively revoked mid-session if a user moves from a trusted to an untrusted network. Geo-fencing policies can restrict access to specific countries or regions, with immediate session action if the location changes.

Continuous Compliance Enforcement

Devices can lose compliance during an active session, security software disabled, OS updates overdue, firewall deactivated, or prohibited peripheral devices connected, with no mechanism to detect and respond while the session continues. Unlike conditional access solutions that only check at the start, deviceTRUST monitors device compliance throughout the session. If an antivirus product is disabled, a firewall is turned off, an unauthorised USB drive is inserted, or OS patch levels fall outside acceptable thresholds, deviceTRUST detects the change in real time and triggers the configured response immediately and without manual intervention.

Dynamic In-Session Access Control

Organisations need to control what applications and data users can access based on their current context — location, device type, network, or security posture — without being able to update access policies dynamically during an active session without disconnecting users. deviceTRUST can modify what is accessible within an active session as context changes, restricting application access, adjusting clipboard and print policies, or limiting drive redirection, all without disconnecting the user. This enables nuanced scenarios such as allowing access to sensitive applications only when on the corporate network, while still allowing standard applications when working remotely, all within a single continuous session.

CORE CAPABILITIES

Six Ways deviceTRUST Strengthens Your Security Posture

deviceTRUST covers six critical dimensions of contextual access control, giving administrators precise, real-time enforcement across every aspect of the device, network, and session environment.

Device Identity & Compliance Verification

deviceTRUST reads hardware identifiers, domain membership, OS version, Workspace App version, installed security software, patch level, and certificate state, building a device identity profile that is continuously re-evaluated. Only devices that satisfy all configured compliance criteria can access corporate resources, and the check never stops.

DEVICE POSTURE

Geolocation & Network Access Control

Access policies can be bound to geographic regions, specific IP ranges, or named network profiles. deviceTRUST uses real-time location properties to deny access from prohibited countries at logon, and can revoke or restrict an active session if a user's location changes to an unauthorised zone during the session, without requiring re-authentication.

GEO-FENCING

Dynamic In-Session Application Control

Context changes during a session do not need to result in disconnection. deviceTRUST can restrict access to specific published applications, adjust virtual channel policies such as clipboard redirection and printing rights, or lock the session screen, all while keeping the session alive and the user informed. Restrictions are reversed automatically when compliance is restored.

IN-SESSION POLICY

Peripheral & USB Device Control

deviceTRUST monitors connected peripheral devices in real time, detecting when a USB drive, storage device, or other peripheral is inserted during an active session. Policies can whitelist approved storage media, and automatically lock session access or block drive redirection when an unauthorised device is detected, protecting against data exfiltration through physical media.

DATA LOSS PREVENTION

BYOD & Unmanaged Device Scenarios

deviceTRUST enables organisations to define differentiated access policies for managed corporate devices versus personal BYOD devices, allowing both to connect, but applying stricter session restrictions to unmanaged endpoints. Users on personal devices may access a limited set of applications, with clipboard and printing disabled, while corporate device users receive full access, all within the same Citrix infrastructure.

BYOD POLICY

Audit Trail & Compliance Reporting

Every context evaluation, policy decision, and enforcement action is logged, providing a complete audit trail of what was checked, when, what was found, and what action was taken. This audit data supports regulatory compliance reporting, security incident investigations, and the AAA (authorise, authenticate, audit) framework that is the foundation of a credible Zero Trust posture.

FULL AUDIT TRAIL

HOW IT WORKS

Three Components, Plus a First Line of Defence.

deviceTRUST is built on a streamlined three-component architecture, lightweight, straightforward to deploy, and designed to integrate natively into your existing Citrix environment without additional hardware, complemented by the Citrix Device Posture Service as an additional layer of defence before logon.

THE CONSOLE

Policy Management

The centrally managed policy editor where administrators define device contexts, configure compliance rules, set action triggers, and build session control policies. Ships with pre-built templates for common security use cases, from compliance checks and USB control to geofencing and BYOD restrictions. Policies are distributed via Group Policy (GPO) or file-based deployment.

THE AGENT

Session Host

Installed on the Citrix Virtual Apps and Desktops host (VDA), DaaS host, or RDSH server, included directly in the CVAD VDA installer from version 2503. The Agent is the enforcement engine: it receives context data from the Client Extension, evaluates it against the active policy, and executes the defined actions when context changes are detected within a running user session.

THE CLIENT EXTENSION

Endpoint

Integrated into Citrix Workspace App 2503 and later, with no separate installation required for end users. The Client Extension runs on the user's device (Windows, macOS) and continuously collects device context — hardware identity, security software state, network location, peripheral devices, geolocation, and more — forwarding it to the Agent over the existing Citrix session channel.

THE FIRST LINE OF DEFENCE

Device Posture Service

deviceTRUST works alongside the Citrix Device Posture Service in a complementary two-layer model. The Device Posture Service performs endpoint health checks before authentication, blocking non-compliant devices before they can even attempt to log in. Once a session is established, deviceTRUST takes over for continuous in-session monitoring and enforcement. Together, the two services provide protection at every stage: before logon, at logon, and throughout the session lifecycle.

REAL-WORLD SCENARIOS

What deviceTRUST Actually Does — In Practice

These are real examples of contextual access enforcement, the kind of situations that happen every day in hybrid work environments, and that traditional conditional access cannot address once a session is open.

TRIGGER — SECURITY SOFTWARE

Firewall Disabled Mid-Session

A remote worker disables their Windows Firewall during an active Citrix session, intentionally or as a side effect of another action. The device no longer meets the defined compliance policy. Session is locked immediately. The user sees a notification explaining that the firewall must be re-enabled to restore access. Session unlocks automatically when compliance is restored.

TRIGGER — PERIPHERAL DEVICE

Unauthorised USB Drive Inserted

During an active session, a user inserts a USB storage device that is not on the organisation's approved peripheral list, creating a potential data exfiltration path via the session's drive redirection. Drive redirection is immediately disabled for the session, blocking access to the USB device from within Citrix. The session continues. The restriction lifts automatically when the device is removed.

TRIGGER — NETWORK LOCATION

User Connects from Prohibited Country

An employee travelling internationally attempts to connect to the corporate Citrix environment from a country that falls outside the organisation's approved geolocation policy, or moves to a prohibited region during an active session. Access is denied at logon, or the active session is immediately revoked if the location change occurs during a session. The user receives a message explaining the geo-policy restriction.

TRIGGER — DEVICE STATUS

Wrong Citrix Workspace App Version

A user's Citrix Workspace App is detected as running a version below the minimum required by policy, potentially missing security patches or compatibility features that the organisation has mandated. Access to the Citrix environment is blocked. The user is presented with a clear message explaining the version requirement and how to update, removing ambiguity and reducing helpdesk load for this class of issue.

TRIGGER — DEVICE TYPE

Personal BYOD Device Connecting

An employee uses their personal laptop to connect to the Citrix environment from home. The device is not domain-joined and does not have a corporate device certificate, identifying it as a BYOD endpoint. Session opens with a restricted policy profile: clipboard redirection, printing, and local drive access are disabled. The user can access approved applications but cannot transfer data to the local device.

TRIGGER — NETWORK CHANGE

User Moves to Public Wi-Fi

A user working from a hotel connects to the public Wi-Fi network during an active session, moving from an encrypted, trusted network to an untrusted, open network that does not meet the organisation's network security policy. The session is restricted or disconnected immediately upon detecting the network change. The user is advised to connect via VPN or move to a trusted network to restore full session access.

ACKNOWLEDGEMENT

Field Research Acknowledgement

The six scenarios above were inspired by James Kindon's field research and community writing on Citrix and deviceTRUST, published at jkindon.com.

HOW IT'S DELIVERED

Delivered as a Managed Service by OAS

deviceTRUST is a powerful security tool, but its value depends entirely on how well its policies are designed, tested, and maintained. This is not a deploy-and-forget product. It requires structured engagement, careful policy design, and ongoing refinement as your organisation's requirements evolve.

Security Requirements Workshop

OAS works with your team to map your specific compliance requirements, device types, user populations, network environments, and risk tolerances into a structured policy framework, before a single rule is written. Getting this right upfront prevents both security gaps and unnecessary user disruption.

DISCOVERY & DESIGN

Session Control Design & Deployment

OAS designs and deploys your deviceTRUST session control policies, building the context definitions, configuring the action triggers, and testing each scenario in a controlled environment before any policy reaches production users. Pre-built templates are used where appropriate and customised for your environment.

POLICY BUILD

Monitoring & Incident Response

OAS monitors deviceTRUST enforcement logs for patterns of repeated policy violations, unusual access attempts, or blocked sessions that may indicate a security incident in progress, distinguishing between user error and genuine threat activity and escalating accordingly.

ALWAYS ON

Policy Evolution & Tuning

As your organisation grows, acquires new device types, expands to new geographies, or changes compliance requirements, deviceTRUST policies must evolve with it. OAS provides ongoing policy review and refinement, ensuring that enforcement remains accurate and that legitimate users are never unnecessarily disrupted.

ONGOING REFINEMENT

deviceTRUST is not a bolt-on security product — it is integrated directly into Citrix Workspace App, the client that users already download and install on their laptops, desktops, and mobile devices. Once deployed, it acquires the pre-defined security templates and access controls configured by your Citrix administrators, and enforces them continuously throughout every session. It is the capability that operationalises Citrix's any device, any location, any application promise, by ensuring that access is always authorised, authenticated, and audited in real time. Acquired by Citrix in December 2024, deviceTRUST is now included in the Citrix Universal Hybrid Multi-Cloud subscription.

Citrix Overview **Citrix DaaS** **Secure Private Access** **NetScaler** **uberAgent**

Ready to Turbocharge Your Zero Trust Strategy?

Speak to an OAS consultant about designing and deploying a deviceTRUST session control strategy for your Citrix environment. The first step is a structured requirements engagement, not a product install.

TELEPHONE

+27 11 485 3454

EMAIL

info@oas.co.za

WEB

https://www.oas.co.za

OFFICE

25 Durham Street, Raedene Estate, Johannesburg

Request a demo: https://www.oas.co.za/contact/demo

Open Architecture Systems — Protect. Detect. Recover. Citrix Platinum Partner since 1987.