deviceTRUST

Contextual policy-based access with Amazon WorkSpaces

Simple. Dynamic. Integrated.

Joint Solution

Amazon WorkSpaces is a managed, secure cloud desktop service. With Amazon WorkSpaces, your users get a fast, responsive desktop of their choice that they can access anywhere, anytime, from any supported device.

Amazon WorkSpaces supports a minimum of 3 authentication requirements including a directory unique registration code, username and password. This can be enhanced with MFA and client-side corporate certificates. Additionally, customers can “whitelist” IP address so that users can only connect from known networks.

For many customers these services included authentication mechanisms are sufficient to protect access to corporate Amazon WorkSpaces. For enterprise customers and those with a more advanced security requirements there is a need for additional protection. deviceTRUST offers customers of Amazon WorkSpaces the ability to apply policy based, contextually aware access controls to user desktops and applications. Occurring immediately after user authentication, deviceTRUST enforces the more advanced security requirements for your enterprise.

Benefits

- Meet Security, Compliance and Regulatory requirements by incorporating the endpoint and user context into business policies
- One central context platform with a rich set of detailed context
- Seamless integration into existing Amazon WorkSpaces management and reporting solutions
- Easy and fast implementation with no need for additional infrastructure
- Subscription based licensing
- Immediate Return of Investment (ROI)

deviceTRUST

Email: info@devicetrust.com
https://devicetrust.com
Twitter: @deviceTRUST

deviceTRUST

Simple

deviceTRUST makes the context of the endpoint and the user available inside Amazon WorkSpaces. It enables seamless support for internal and external network access, integrates transparently with existing VPN solutions or any kind of network connection and requires no additional infrastructure making implementation easy.

Dynamic

deviceTRUST ensures that all changes to the endpoint and user context results in an immediate update to the context within the Amazon WorkSpaces. Dynamic triggers allow the desktop to react to these changes. For maximum flexibility, these triggers can execute any script or process in the context of the logged-on user or with system privileges.

Integrated

The context of the user and endpoint is written to the Microsoft Event Log, allowing easy integration with existing SIEM and reporting solutions.

Features

No infrastructure: deviceTRUST does not require any additional infrastructure. This enables a rapid and effective implementation and results in low implementation and operational costs.

Intuitive management: Configuration within Microsoft Active Directory Group Policy Objects (GPO).

Easy start: Group membership allows you to easily target the users enabled for deviceTRUST functionality.

Seamless integration: The intelligent technology provides the context of the endpoint into the Amazon WorkSpace, enabling easy consumption by all existing management solutions.

Always up-to-date: The context of an endpoint is kept up-to-date during the entire user session. This guarantees that all security and compliance requirements are met even if the status of the endpoint changes.

Conditional Access: Control access to the Amazon WorkSpace depending upon whether a deviceTRUST client is installed and defined properties of the endpoint, independently from how the virtual session is accessed (internal / external network access). If the endpoint does not meet your requirements, the Amazon WorkSpace can be blocked for the user during logon and during the entire session.

User messages: User specific notifications can be displayed depending on context.

Available properties: Policy settings can define which context properties of the endpoint are given to deviceTRUST.

Geolocation: deviceTRUST makes it possible to provide the location of an endpoint regardless of the network connection used.

Note: *Geolocation requires integration with a GEO location provider, and may be subject to third party terms and conditions.*

Trigger: Respond to events within the users' Amazon WorkSpace session.

Easy deployment: All deviceTRUST components can be installed with existing software deployment solutions. The client can be installed also from the deviceTRUST web site.

Detailed information: deviceTRUST delivers more than 400 hardware, software, network, security, performance, printer and location properties into the Amazon WorkSpace.

Detailed security information: Detailed information about endpoint security state including Windows Update, Windows Defender and Windows Firewall.

Microsoft® AppLocker Support: Dynamically configure Microsoft® AppLocker to grant or deny access to applications inside the Amazon WorkSpace, e.g. to meet compliance and license requirements.

Application termination: Terminate running applications if user and endpoint context does not meet the compliance or security requirements anymore.

Reporting: Detailed user information, including endpoint context, integrated seamlessly with existing reporting solutions.

Attractive license model: deviceTRUST is licensed on a named-user basis independent how many endpoints a user is using. The subscription model prevents high investments.

Use Cases

Conditional access from a secure endpoint: To meet the corporate compliance requirements, users are required to access Amazon WorkSpaces from secure endpoints only.

Conditional access from a validated network: To meet the corporate compliance requirements, users are required to access Amazon WorkSpaces if the endpoint uses a validated network connection.

Conditional access from authorized countries: To meet the corporate regulatory requirements, users are required to access Amazon WorkSpaces only from authorized countries.

Conditional access from a secure Wi-Fi connection: To meet the corporate security requirements, users are required to access Amazon WorkSpaces if the endpoint uses a secure WPA2 or WPA3 encrypted Wi-Fi connection.

Conditional access from endpoints that are not virtualized: To meet the corporate compliance requirements, users must not access Amazon WorkSpaces from an endpoint that is virtualized.

Conditional access from endpoints that are not remote controlled: To meet the corporate regulatory requirements, users must not be accessing Amazon WorkSpaces from an endpoint that is remote controlled.