deviceTRUST

Contextualizing IT

Simple. Dynamic. Integrated.

Use Case Overview

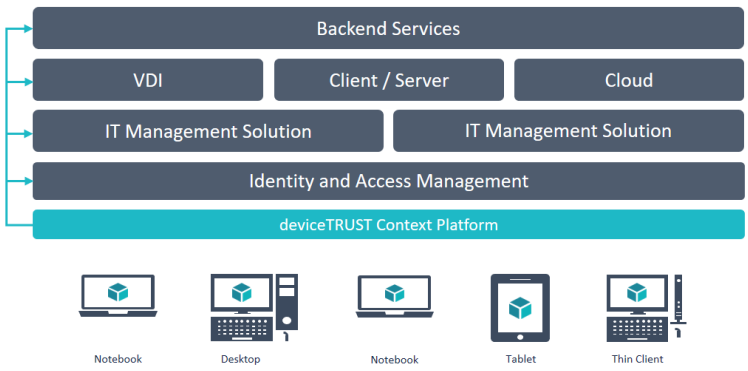
deviceTRUST´s mission is to contextualize the corporate enterprise, allowing users the freedom to access their corporate workspace from any location, on any device, over any network, while giving IT departments the information and control they need to meet their governance requirements.

With its patent pending technologies, deviceTRUST delivers more than 200 hardware, software, network, security, performance and location contextual properties into the virtual and physical workspaces. deviceTRUST can easily integrate with any existing workspace management solution and requires no additional infrastructure. The context is always up-to-date and any change triggers a definable action.

deviceTRUST - Contextualizing IT

Scenarios

- Manage device based licenses
- Access for contractors and partners
- Location based access to network printers and shares
- Meet the remote device security requirements
- Compliant access to a sensitive application and data
- Location based access to finance application
- Ensure access only from corporate owned devices



deviceTRUST

Phone: +49 (6162) 8015950
Email: info@devicetrust.com
https://devicetrust.com
Twitter: @deviceTRUST

deviceTRUST

Contextualizing IT

Simple. Dynamic. Integrated.

Use Case Overview

Manage device based licenses

A customer is using applications, which are licensed on a per-device basis. This means an application license is required for each device that is able to access those applications. These applications are published to the users on a terminal server environment based on Citrix XenApp. The users on any remote device can use technically these applications. However, to ensure a license compliant usage of these applications, it is necessary to accurately identify the remote device. deviceTRUST provides that required identification in the form of the hardware serial number of the remote device into the virtual session. This information, in combination with the existing management solution, enables the customer to grant or deny access to the appropriate application. This guarantees the application usage is in accordance with the device-based license terms of the software vendor.

Security ●○○
Compliance ●●●
Configuration ●●○

Access for contractors and partners

Employees of an external partner need access to business applications published on a Terminal Server environment. The customer already has an authentication solution in place for secure access. IT have additional security requirements that employees of the external partner must only access business applications from company owned devices that are members of the domain of the external partner. Additionally, the user must not have administrative privileges on the remote device. In this scenario, deviceTRUST is used to ensure that the remote device connected to the session is a member of the external partner domain and that the user has no administrative privileges on that remote device. This allows the customer to grant access only if the compliance requirements are met.

Security ●●●
Compliance ●●●
Configuration ●○○

Location based access to network printers and shares

An international company operates from many locations worldwide and has users travelling between these different locations, who are able to access all applications and desktops provided by a central VDI environment. Based on the users' location it is necessary to grant access to specific network printers as well as network shares. deviceTRUST provides the detailed information about the actual location of the remote device into the virtual session of the user and enables the mapping of the compliant network printers and shares via Microsoft GPO logon script and GPP action. This enables the customer to provide a dynamic virtual environment, which is location aware.

Security ●○○
Compliance ●●○
Configuration ●●●

Meet the remote device security requirements

Employees are able to access a virtual environment from external locations with their company owned laptops as well as their own personal devices. The internal security policy requires that at logon and during the entire session, an active firewall as well as an up-to-date anti-virus are running on the remote device. If no firewall or anti-virus is enabled the user is not allowed to access the virtual environment. If one of the two security solutions becomes deactivated during the session runtime, the virtual session must be disconnected. In this scenario, deviceTRUST provides the actual state of the firewall and the anti-virus into the virtual session and keeps this information up to date during the entire session. If the status of one of these components changes, a predefined action will be executed to ensure the virtual session is disconnected.

Security ●●○
Compliance ●●●
Configuration ○○○

deviceTRUST

Contextualizing IT

Simple. Dynamic. Integrated.

Use Case Overview

Compliant access to a sensitive application and data

A customer is publishing a virtual desktop via Citrix XenDesktop, which includes core applications. Additional applications are published into this virtual desktop using a Citrix XenApp environment. The employees are able to access these environments with their corporate owned devices from all internal and external network connections. Some of the published applications are very data sensitive, e.g. the HR application. Typically, users who are members of the Microsoft Active Directory Group “Human Resources” have access to this application. For governmental compliance reasons, users of the HR department are not allowed to access the HR application when they are accessing the environment from an unsecured Wi-Fi connection (e.g. public area). deviceTRUST provides information about the connected Wi-Fi, including its security state into the virtual session. This information is used in combination with the users’ group membership to decide if the user has access to the HR application.

Security	●●○
Compliance	●●●
Configuration	●●○

Location based access to finance application

A company has five locations in Europe. All applications are published via a Terminal Server environment based on Citrix XenApp. All users of the finance department are based on the same floor in one of the offices. As the finance application contains sensitive information, it is required that users of this department cannot access the finance application from any of the other offices or from outside the corporate offices. The information provided by deviceTRUST are used to identify which office location the user is accessing and grant or deny access to the financial application.

Security	●●○
Compliance	●●●
Configuration	●○○

Ensure access only from corporate owned devices

For security and compliance reasons, a financial company must ensure that employees can only access specific business applications and data from a company owned and centrally managed device. Access from non-corporate devices needs to be denied. To meet this requirement, deviceTRUST is used in two ways. First, if a user connects without the deviceTRUST client installed on the remote device, the access to the specific business application is blocked. Secondly, if a deviceTRUST client is installed, deviceTRUST provides the unique hardware serial number of the remote device into the virtual session. This serial number will be validated with the existing management solution to grant or deny access. With deviceTRUST, the customer is able to ensure that only company owned; known devices are accessing the specific business applications.

Security	●●○
Compliance	●●○
Configuration	●○○