Zero-Trust mobile security in a perimeter-less world

PROTECTING DATA IN A PERIMETER-LESS WORLD

Organisations often view their security strategies like a castle. The office network had multiple layers of perimeter security solutions (e.g. firewall, web gateways etc.) to make it as secure as possible, protecting the crown jewels of business data. A great strategy when everyone worked inside the office.

Remote working is great for operational efficiency, so organisations need a security model that supports employees as they work from anywhere, from a range of devices. The traditional perimeter model poses challenges for organisational security, exposing your company to the risks from malware and data breaches from IT devices that are unknown and unsafe.

To address security blindspots and weaknesses, and maintain a strong defence around corporate data, a different approach is needed.

What do CISOs worry about?

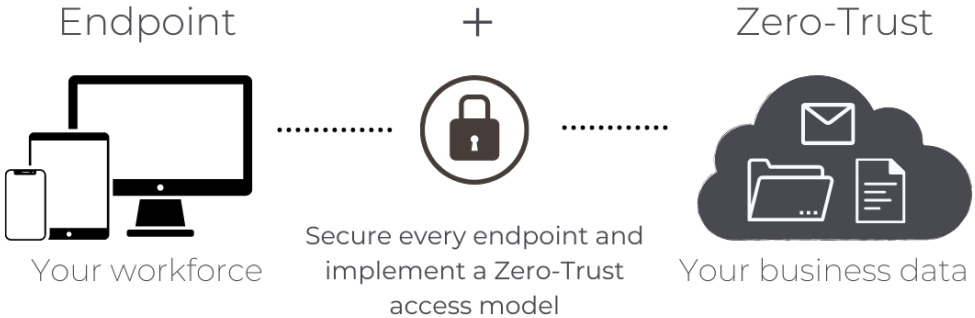
"employees using their own devices to access corporate data" 40%

"employees using unauthorized apps to access corporate data" 33%

Ivanti, EMEA CISO Survey: How the pandemic has shifted CISO priorities, 2021

"If you want to stop breaches, zero trust is the best way how." *Charlie Gero, Akamai Technologies*

Zero-Trust solves these issues by inherently distrusting any device or network until they are authenticated and proven to be safe. One method of enforcing Zero-Trust principles on mobiles is by ***blocking access to business resources from devices that have not been verified as trustworthy***. Combined with a move away from perimeter-based security strategies and toward validating security health of all devices, Zero-Trust is a highly effective model to secure private data and keep out threats.



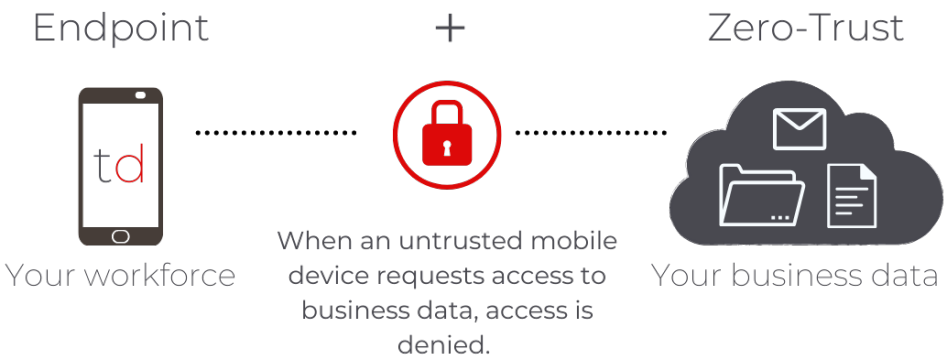
THE BENEFITS OF CONDITIONAL ACCESS

- Reduces the risk of data breaches, fines and damages from cyberthreats
- Enables secure remote working without compromising efficiency
- Protects your private data on mobiles, anywhere and on any network
- Automatically allows access to company data when a user's device is validated as trusted, and restricts access if it becomes untrusted

HOW TRUSTD UNIQUELY ENABLES ZERO-TRUST

Trustd acts as a Policy Enforcement Point, providing access to your data only to trusted mobile devices.

The Trustd app monitors the security risks of every mobile device in your workforce, and whether they should be allowed access to your business data.



The Trustd app acts as a trust broker on each device to validate the device is safe before granting access to company data, such as email, Teams, Office docs, OneDrive etc. If at any point the device's trustworthiness changes (e.g. if it connects to a network with man-in-the-middle, or if the user installs a malware Android app), then access to company resources is restricted and your organisations' data remains safe. And if any of your users don't have the Trustd app installed, they simply can't access company data on their mobile devices.

How is this different from other MTDs?

Trustd's unique approach to Zero-Trust means that it is the only single- solution MTD that enables your Zero-trust strategy for all of your mobile devices, whether they're managed by an MDM/MAM or not.

Most MTDs feed a device's threat status into mobility management software like Microsoft InTune to restrict access to company data. Trustd uses the device health status to restrict access to company resources from mobile platforms ***at a user-level***, meaning that devices are protected even if they aren't known or managed.

Here's an example of how this works in practice.

The Big Manufacturing Co. has 1000 employees. The business demands a BYOD strategy for the important flexibility, productivity and cost-saving benefits it brings. However, what the security team discovered was that many employees refused to use the company's management software, Microsoft Intune, on their personal mobile phones and tablets. Staff were worried about the lack of privacy, as the IT team would be able to see things about their location, browsing behaviour, and the apps installed on their devices.

One option would be to buy corporate-owned devices for employees. There were several issues with this, not least of which was the huge cost, and the problem remained that employees still owned personal devices. The continuous merging of business and personal life meant that shadow devices that access business data were still a constant threat.

The solution that worked best for all stakeholders was that the company would provide mobile phones to the senior management team only, managing them with their MDM.

The rest of the workforce continued to access company data from their personal devices if they wished, but were instructed to install the Trustd app - which puts employee privacy first, returning nothing but the security health status of the device.

Because the Trustd console (that communicates with the Trustd app on all devices) talks directly to Azure Active Directory, without relying on Microsoft Intune, it means that all those unmanaged personal devices can be given conditional access to company data, just like those corporate-owned ones that are managed by Intune.

Not all MTD vendors provide integration with Mobile Application Management (MAM) and Mobile Device Management (MDM), and those that do often only offer it as part of their premium licence tier. No other MTD enables a Zero-Trust security model for unmanaged devices in a single solution - preventing access to business resources from devices that aren't enrolled in a management platform. This makes Trustd the ideal choice for organisations that want to provide a secure BYOD environment.

"The power of a zero trust architecture comes from the access policies you define."

Zero trust architecture design principles, National Cyber Security Centre

HOW TRUSTD PROTECTS YOUR DATA

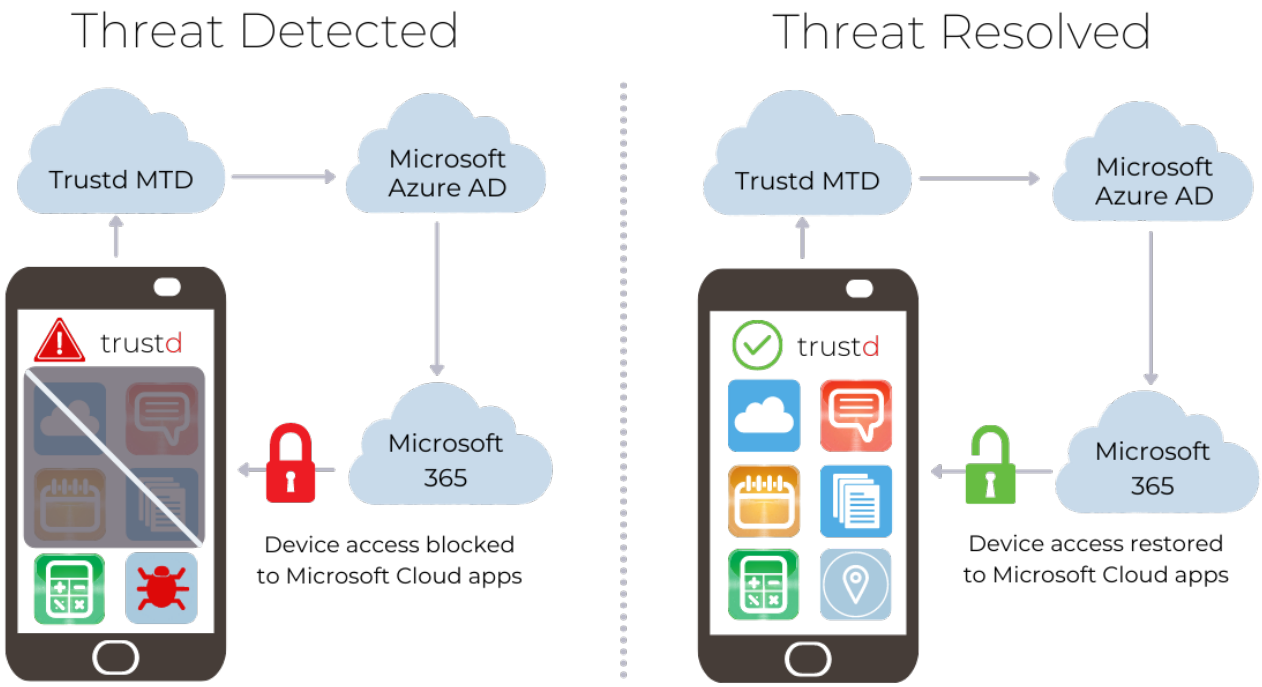
Network threats (Android & iOS)
- Man-in-the-Middle attacks
- Phishing
- Malicious web scripts
- Malicious proxies
- Unsecured WiFi
- Weak WiFi security

Device threats (Android & iOS)
- OS exploits
- Out of date devices
- Vulnerable configuration

App threats (Android)
- Malware apps
- Known and unknown threats
- Screen recording
- Leaky apps
- Camera/Microphone access
- App permission abuse

With Trustd you can trust your mobile devices to mitigate data breaches

In monitoring each mobile device for these threats, the Trustd app returns a security health status to the Trustd console, which in turn talks to Microsoft Azure Active Directory to grant or deny access to your company data and Microsoft Cloud apps. If the device is untrusted, the user simply needs to follow the straightforward guidance in the Trustd app to resolve the threat on the device, then access is automatically restored.



CommSec Sensible Cyber Security

Web: https://commsec.ie/
Email: sales@commsec.ie
Tel: +353 1 536 7320

traced AUTHORISED PARTNER