

Device Trust

Duo helps more than 100,000 organizations secure access to their critical business applications by providing insight into over 26 million endpoints.



The Challenge:

Lack of Visibility and Control

In its 2022 Mobile Security Index, Verizon reported that close to half of the companies surveyed had experienced a device-based compromise in the past 12 months. Almost three-quarters stated that the impact of the attack was major, including data loss, downtime or some other negative outcome.

Over time, organizations have deployed a variety of solutions to manage and secure devices. However many still find it challenging to gain visibility into all devices used to access their on-premises and cloud applications. They also struggle to enforce access controls based

on the health and security status of managed (corporate-owned) and unmanaged (BYOD) devices.

Even when an end user is properly authenticated and granted access based on their role and privilege, the organization may still be at risk if the device in use is vulnerable to compromises due to malware downloaded from email or websites, or through the use of malicious apps. Therefore, to implement an effective mitigation, organizations need to consider a zero trust security strategy that verifies the trustworthiness of all devices in addition to user authentication before granting access to business applications and data.

The Solution:

Duo Device Trust

Duo's unique approach to gain visibility and assess device health status using a lightweight application plus simple integrations with leading device management solutions make it a compelling component of any organization's endpoint security strategy. **With Duo's device trust capabilities organizations get these three key benefits:**

01. Prevent Data Breaches

Duo's solution provides comprehensive insight into the types of devices accessing corporate networks and applications, helping security teams monitor and flag risky devices to further secure their environment.

Further, Duo's device trust policies enable organizations to enforce device verification policies across any device, whether corporate-owned or personal (BYOD). Administrators can easily restrict access to sensitive applications from devices that do not meet the required security criteria; or block access from those identified by third-party agents as compromised.

02. Achieve Compliance with Ease

Organizations operating in regulated verticals need to ensure their modern IT environment complies with requirements – for example HIPAA, PCI-DSS and NIST. Further, governments all over the globe are introducing data privacy laws such as GDPR and CCPA to hold organizations responsible for securing customer personally identifiable information (PII).

Duo can help organizations meet certain zero trust security requirements for device health and trust across these compliance and data privacy laws. This includes implementing secure user and device authentication mechanisms and blocking access for unauthorized users and risky devices.

03. Balance Security and Productivity

It is critical to balance security and user productivity by verifying device trust in a manner that is easy for IT to manage and not disruptive to employee workflows. Duo has taken a unique approach that simplifies integration with leading device management systems. This makes it easy for organizations of all sizes to incorporate Duo seamlessly into their IT security strategy while delivering the best possible user experience with minimal administrative overhead and a low total cost of ownership.

“**Duo Desktop allows us to seamlessly enforce our company policy at the most important point in time: when users connect to our sensitive applications.**”

Jason Waits
CISO, Inductive Automation

Start your free 30-day trial at duo.com/trial.