Duo for...

Duo Security is now part of Cisco.

Device Trust

Duo helps more than 20,000 organizations secure access to their critical business applications by providing insight into over 24 million endpoints.

THE CHALLENGE:

Lack of Visibility and Control

Thirty-three percent of companies surveyed in 2019 said they had experienced a device-based compromise, and the majority reported the impact was major (from Verizon's 2019 Mobile Security Index: https://enterprise.verizon.com/resources/reports/mobile-security-index/).

Organizations have deployed several solutions to manage and secure devices, but 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 which verifies the trustworthiness of all devices in addition to user authentication before granting access to business applications and data.

THE SOLUTION:

Duo's Device Trust

Duo's unique approach to gain visibility and assess device health status using a light-weight application and simple integrations with leading device management systems make it a compelling component of an organization's endpoint security program.

With Duo's device trust capabilities organizations get the following three key benefits:

01

Prevent Data Breaches

Duo's solution provides comprehensive insight into the types of devices accessing their 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, regardless of whether it's corporate owned or personal (BYOD). Administrators can easily restrict access to certain applications from devices that do not meet the required security criteria; or block access to devices that are identified by third party agents as compromised.

02

Achieve Compliance With Ease

Organizations operating in regulated verticals need to ensure that their modern IT environment complies with requirements such as 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 requirements on device security health and trust across these compliance and data privacy laws, such as implementing secure user and device authentication mechanismsand blocking access for unauthorized users and risky devices.

03

Balance Security and Productivity

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

"The Duo Device Health Application allows us to seamlessly enforce our company policy at the most important point in time: when users connect to our sensitive applications."

Jason Waits
Cyber Security Risk Officer, Inductive Automation

sales@duo.com

duo.com