DUO for...

Duo Security is now part of Cisco.

Bring Your Own Device

Duo helps more than 10,000 organizations secure access to their critical business applications by providing insight into over 300 million endpoints.

THE CHALLENGE:
Lack of Visibility

While Bring Your Own Device (BYOD) has allowed companies to increase employee productivity, it has also introduced a major security issue – the lack of visibility into the security health of personal devices.

Traditional mobile device management (MDM) solutions require the deployment of agents on endpoints to provide this visibility, but privacy concerns often stop users using these solutions on their personal devices. That leads to a significant lack of coverage and visibility.

There's a new way to get visibility into every device, both corporate and personal, to protect corporate networks and critical applications against vulnerable endpoints and potential data breaches.

Duo integrates with the most popular apps, including:

Cisco · Citrix · vmware · Juniper Networks · Outlook · Office 365

Duo for BYOD

THE SOLUTION:

Duo's Endpoint Visibility

Duo's Unified Access Security (UAS) solution provides three key benefits:

01

Enforce BYOD Security Policies

Gain visibility into the security health of all of your devices to monitor out-of-date operating systems, browsers and plugins that may put your company at risk of a security vulnerability.

Identify mobile devices that lack security features, such as screen lock and passcodes, or ones that may be jailbroken or rooted.

Then use this data to enforce security policies to block access to your corporate apps from outdated devices to reduce your risk of security vulnerabilities and malware infection.

02

Complete Device Inventory

Duo provides visibility into all user devices accessing any application. This includes laptops, desktops and mobile devices. Devices can be user-owned or corporate-owned.

Once admins have visibility into devices accessing their environment, they can determine the overall risk due to previously unseen or unknown devices, and enforce security policies based on application risk.

03

Insights into Device Posture

With Duo, admins can also gain deep insights into the security posture of all devices accessing applications. Admins can determine if a device has up-to-date software such as OS, browsers, Flash and Java running on the device. For mobile devices, admins can learn if a mobile device has a passcode lock enabled, encryption enabled and if it's jailbroken or not.

Based on these insights, admins can set policies to only allow secure and trusted devices to access applications

"

We have seen value in the data we get from Duo regarding authentication sources, as well as now having user device information that was largely opaque to us."

Thomas Siu
Chief Information Security Officer
Case Western Reserve University