CISCO SECURE | DUO

CISCO The bridge to possible

THE ESSENTIAL GUIDE TO

Device Trust in the Enterprise

IT networks have changed significantly in the last few years.

Businesses are leveraging cloud and mobile technologies to enable faster digital transformation. At the same time, IT teams need to optimize for cost and productivity. This paradigm shift in enterprise networks, from traditional on-premises presence to hybrid IT and multi-cloud environments, has necessitated a change in how organizations think about securing their **new perimeter**. This means moving from a network-centric security architecture to a user, device and application centric architecture.

Organizations need to enable secure and direct access to business applications for a diverse set of users (remote workers, vendors and contractors) and their devices that typically reside outside of the control of corporate EMM (enterprise mobility management) and MDM (mobile device management) solutions. Enforcing consistent security policies across managed devices, bring your own device (BYOD) and third-party (contractor or partner) devices poses a significant challenge. IT security teams lack the necessary insights and enforcement mechanisms when making an access decision on endpoints, particularly among unmanaged devices.

There are key posture checks organizations should perform before granting access to attest whether a device is trustworthy:

- Is the device managed?
- Are the operating system (OS) and browser versions, including patch levels up to date?
- Is the enterprise antivirus (AV) agent installed and running?
- Is the host firewall enabled?
- Is disk encryption turned on?
- Does the device have a password set?
- Is the mobile device rooted or jailbroken?

Challenges in Establishing Device Trust

Organizations of all sizes struggle with managing endpoints that need access to corporate applications and data. The multitude of unmanaged devices that reside outside of the control of corporate EMM and MDM solutions increases security risks.

A full 45% percent of companies surveyed in Verizon's 2022 Mobile Security Index said they had experienced a mobile device–based compromise in the last 12 months, and the majority reported the impact was major. Users are reluctant to enroll in an EMM or MDM because it can significantly impact their experience and privacy. At the same time, IT is unable to force users to enroll, but they can limit access to applications which can then turn into a loss in productivity. Instead, IT needs to set policies that make access decisions based on device security posture without impacting user experience and productivity.

Let's explore some current challenges to achieving device trust:

Limited Visibility

Organizations can deploy several solutions to manage and secure devices, but still find it challenging to gain visibility into all the devices that access their on-premises and cloud applications. This is especially true for devices that are outside the IT department's control, such as personal, contractor or partner laptops and mobile phones – items that are not enrolled in any device management solutions, but require access to cloud applications such as Microsoft 365 or Dropbox. IT teams often lack visibility into these devices and the ability to verify their health status before granting access to resources including data and applications. This can lead to increased risk of data breaches and non-compliance with IT regulations.

Complexity in Policy Enforcement

For managed devices, one way to ensure policy compliance is by forcing an update to gain access, which takes update installation control away from users. If updates are forced when a user is in the middle of working on a project, customer presentation or meeting, it hampers both business productivity and user experience.

For unmanaged user devices, the process to get them patched can be laborious for administrators, involving manual follow ups, which could take weeks, if not months. This is a significant exposure window.

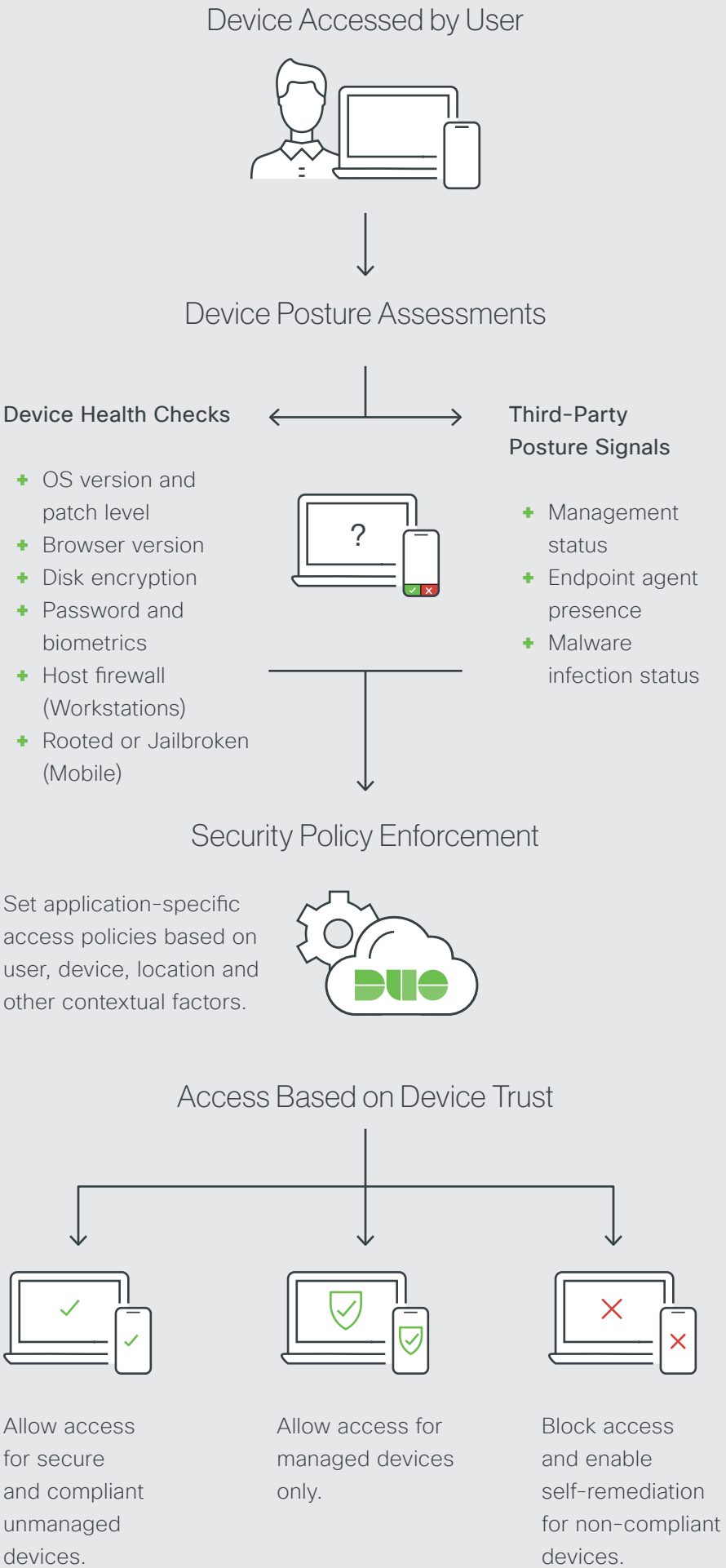
Without an enforcement point at the critical time of application access, administrators cannot assess device security posture. This could result in vulnerable devices gaining access into an organization's network.

Regulatory Compliance Headaches

Organizations operating in regulated markets need to ensure their modern IT environment complies with requirements such as HIPAA, PCI-DSS and NIST. Further, governments worldwide are introducing data privacy laws including GDPR and CCPA to hold organizations responsible for securing customer personally identifiable information (PII). These data security regulations and data privacy laws require adequate security controls to block risky devices and ensure that only the secure ones have access to data. And to prove compliance, administrators need access to detailed log information for audit trail and compliance reporting.

Duo's Device Trust Solution

As part of a Zero Trust for the Workforce approach, Duo has developed several novel tools to establish device trust. **Duo Device Trust** delivers three critical capabilities to help modern enterprises minimize their risk surface by verifying trust and enforcing security policy compliance across any device that requires access to corporate applications.



1 In-depth Device Visibility

Visibility is important to verify and enforce device trust policies. When organizations deploy **Duo**, device trust becomes part of the authentication workflow during the user login process for protected applications. This enables Duo to provide **in-depth visibility** across any device, irrespective of how and from where the users connect to these applications. Duo also helps administrators differentiate between corporate-managed devices and BYOD based on the enrollment status in device management systems.

Duo's **logging and reporting** capabilities enable organizations to maintain an inventory of all devices accessing corporate resources. The dashboard helps administrators understand the overall organizational security posture, and a quick drill-down with just a few clicks allows them to identify users with risky devices (e.g., running out-of-date operating systems including OS, browsers, Flash and Java versions).

All of this data can be easily exported to any log management and analysis tools. And administrators can schedule reports making it easy to prove compliance.

2 Device Security Posture Assessment

Building on endpoint visibility, Duo makes it easy for organizations to establish device trust before allowing access to corporate applications. Administrators can enforce corporate security policies to ensure compliance and block non-compliant devices at the time of authentication. For example: Duo can check OS patch level, password status, firewall status, AV agents enabled, disk encryption and device management status, before granting application access.

Duo's approach to assessing device health posture addresses the diverse population of managed and unmanaged devices that access enterprise applications. Duo helps administrators ensure their endpoint fleet is in compliance with corporate security policies and empowers end users with **self-remediation**, which reduces the number of IT tickets raised and calls to a support help desk.

Duo supports a broad range of leading Mobile Device Management (MDM) and Endpoint Detection and Response (EDR) solutions. Here are a few.

vmware

Symantec

Microsoft Active Directory

Cisco Secure Endpoint

jamf

Windows Defender

Microsoft Intune

CROWDSTRIKE

cisco Meraki

mobileiron

TREND MICRO

SOPHOS

3 Continuous Trusted Access

The core ethos of the zero trust security philosophy is “never trust, always verify.” It is the guiding principle for Duo’s solution. Duo continually assesses the context of user risk at the time of authentication and adjusts security requirements based on that context. Duo analyzes application access data and learns which devices users typically use to access applications and flags suspicious or unusual device access activity. Consider a scenario where a user who typically accesses an application from a personal device has their credentials compromised and now that account is being used to access the application from a different device for the first time. Duo can highlight the rarity or novelty of the device used in such security events by showing the recent devices used in access attempts and relative frequency of access.

Further, Duo enables IT security teams to monitor and respond to endpoint security events, especially when those devices are outside the network and can access cloud applications directly over the internet. By integrating Cisco Secure Endpoint with Duo, organizations can set a policy to automatically block malware-infected devices from accessing applications. Duo blocks only the device and the user can log in from any other device that is policy-compliant to stay productive.

Workers use their devices to access applications.

Cisco Secure Endpoint running on the device detects malware.

Secure Endpoint notifies Duo about the infected device.

Duo blocks that device from accessing apps.

Five Key Device Trust Use Cases

1

CHALLENGE

Protect corporate, manufacturing and retail employees against cybersecurity breaches through a zero trust framework and meet compliance regulations.

SOLUTION

Gain Visibility Across All Devices on the Network

"The level of detail Duo provided into what devices were connecting to our networks, managed or unmanaged, was helpful. We could see things we could never see before – like the number of attempts on a credential on O365 or someplace else, the number of lockouts that have happened. We have been able to use Duo's Device Trust to train our people and give them better avenues to resolve. Duo's Trusted Access platform gives us another deeper layer of insight on how our users are functioning out there."

Craig Vincent
Director of IT Infrastructure and Operations, La-Z-Boy

2

CHALLENGE

Ensure that only secured and corporate-managed devices could access the company's suite of cloud applications.

SOLUTION

Restrict Access to Sensitive Applications to Only Managed Devices

"Duo became the link we needed to make our security philosophy really work. We now know that if folks were downloading reports or manipulating data in a cloud application, that they were doing it from a safe device, and that their identity had been confirmed with MFA."

Richard Hall
Senior Director IT Infrastructure and Operations, FinancialForce

3

CHALLENGE

Assess the true status of managed and unmanaged devices before granting access.

SOLUTION

Improve User Experience While Managing Risk

"Duo very cleanly addresses our need for visibility and getting better insight into the true status of user devices. With Duo, we're both improving the user experience, but also better managing the risks in our environment."

Brad Arkin
SVP and Chief Security and Trust Officer, Cisco Systems

inductive automation

4

CHALLENGE

Protect sensitive applications containing valuable intellectual property. Inductive Automation needed to ensure all devices had a security agent installed and disk encryption enabled.

SOLUTION

Enforce Corporate Security Policies

"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. We're able to ensure that the devices connecting to our applications are company owned, up to date, encrypted, password protected, firewalled and running our company AV/EDR. Relying on the Device Health application as an enforcement point takes pressure off of the IT team to constantly chase down assets that may be out of compliance."

Jason Waits
Director of Cybersecurity, Inductive Automation

SENTARA®

5

CHALLENGE

Secure protected health information (PHI) and meet HIPAA and EPCS compliance requirements while enabling secure BYOD for physicians.

SOLUTION

Meet Compliance Requirements

"The only way we knew to get insights into mobile devices was to push a mobile device management (MDM) tool onto users' devices, but due to cost and complexity we didn't want to pursue this idea. Duo increased our security and was an easy tool to deploy. Every organization should consider them immediately."

Chad Spiers
Director of Information Security, Sentara

The Duo Advantage

Duo offers powerful security in an all-in-one solution that is platform agnostic, scalable, affordable and easy for end users and administrators to use. Below are three key reasons customers choose Duo:

Broadest Coverage

Duo offers the most comprehensive user and device trust capabilities in the market that cater to a wide variety of use cases and a diverse population of workforce devices (managed and unmanaged).

Ease of Use

Duo helps organizations improve security in a manner that is user friendly and enables productivity. Users can self-enroll and self-remediate their authentication and access devices, reducing IT overhead.

Lower Total Cost of Ownership

Duo is a stand-alone security solution that also integrates across the Cisco Secure portfolio so customers (big or small) can reduce their total cost of ownership (TCO) by consolidating security vendors, streamlining security operations and enabling automation.

Consistently applying policies for managed and unmanaged devices and having the capabilities to verify the trustworthiness of a device is essential for protecting data while providing seamless access across a diverse workforce. For organizations, this translates into enabling productivity, reducing risk, preventing threat scenarios and improving security hygiene.

Try Duo For Free

With your free 30-day trial you can see for yourself how easy it is to get started with Duo and secure your workforce, from anywhere and on any device.

Start a Free Trial

Duo Security, now part of Cisco, is the leading multi-factor authentication (MFA) and secure access provider. Duo is a trusted partner to more than 40,000 customers globally.

Try it for free at **duo.com**.

cisco SECURE

Cisco Secure delivers a streamlined, customer-centric approach to security that ensures it's easy to deploy, manage, and use. We help 100 percent of the Fortune 100 companies secure work – wherever it happens – with the broadest, most integrated platform.

Learn more at **cisco.com/go/secure**.