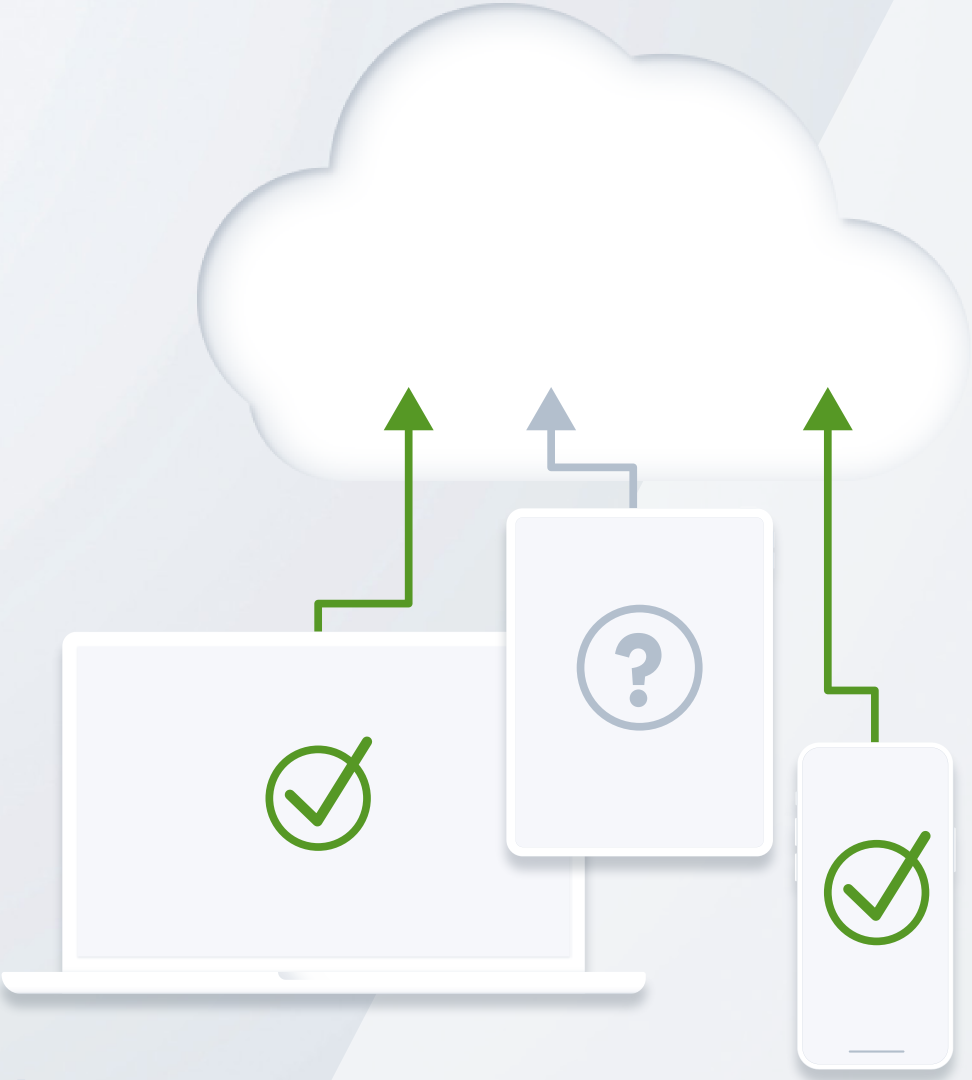
WHITE PAPER

HOW DEVICE TRUST IS KEY TO SECURING CLOUD ACCESS



BEYOND IDENTITY

CONTENTS

01

WHAT IS DEVICE TRUST?

It's critical that the devices accessing company data are trustworthy. Determining which devices should be trusted is a unique decision made by each organization depending on their risk tolerance and compliance requirements.

Different levels of trust are required for low-risk and high-risk resources. Furthermore, compliance requirements are dependent on industry regulations and types of company and customer data that the organization collects and needs to protect.

For example, healthcare professionals shouldn't be able to access sensitive patient medical records from unmanaged, personal machines with unencrypted disks, because that violates HIPAA requirements. However, it doesn't infringe on HIPAA requirements for healthcare professionals to access their HR benefits from their phone. Each organization has unique standards they need to enforce, but it's difficult to maintain these standards on some devices.

Device trust is also a key building block for a Zero Trust security architecture. With Zero trust, until an endpoint device has been proven to be trustworthy, it should not be given access to any data or resources. As some have noted, the endpoint has become the "new security perimeter", making it vitally important to establish device trust. With Zero Trust, don't trust until you verify. As organizations embark on, or continue their Zero Trust journey, they must consider how to establish trust in endpoint devices.

> "Device trust is the process of analyzing whether a device should be trusted and therefore is authorized to do something."

WHY IS DEVICE TRUST IMPORTANT TODAY?

Today, it's a nightmare to control which devices can access cloud resources like software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). These cloud services are great because they're turn-on-and-go, scalable, and easily accessible. Yet the bad news is that they're easily accessible — from any web browser on any device!

Making matters more complicated, COVID-19 sped up the use of cloud services and spawned the move to a permanent hybrid workplace. Now that more and more sensitive, confidential information and important intellectual property resides in cloud services, there's added complexity. Not to mention the workforce can log in from all types of devices, including personal computers, and shared computers, phones, and tablets.

> "If SaaS apps can be accessed from any web browser on any device, what's stopping employees, contractors, or partners from accessing company data using unmanaged, insecure personal machines, or worse?"

Without proper controls employees can access critical cloud resources from shared machines that are very likely compromised, like a computer in a library or hotel lobby.

It's the perfect storm and unmanaged devices are a huge blindspot.

Many CISOs know that employees are accessing sensitive company data on insecure personal machines and that they're powerless to stop it.

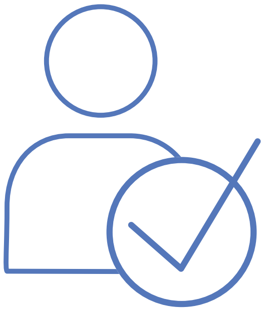
Why? It's easy for system admins to access critical infrastructure or for software engineers to access and commit code to Github from a personal machine, undetected and unmonitored. CISOs we've spoken to have asked these employees to stop, but they don't have confidence their employees are complying with this security measure.

Even if companies have taken steps to control which devices can access cloud resources, CISOs are not satisfied, because these security measures can often be bypassed by more technical users (e.g., engineers or attackers). For them, it's trivial to move a certificate issued by a centralized CA (and stored on the local hard drive) from one device to another device. Then a legitimate user can authenticate from an insecure, personal machine or an attacker can steal the certificate and use it.

Security teams spend a lot of energy and resources locking down company-issued machines because the workforce has access to important data. They're concerned by attackers potentially getting a foothold, installing malware on the endpoint, and gaining access to company data.

The accessibility of the cloud means company data can be moved onto personal machines. This opens up organizations to a lot of risk. Unmanaged personal machines could already be compromised and become an attack vector to company data and resources. Though this is a risk that a lot of CISOs have had to live with, it's very problematic.

MANAGED DEVICES ONLY TELL HALF THE STORY



Historically, organizations have turned to managing devices to control access to company data. By managing devices, we mean the process of identifying, purchasing, configuring, and rolling out mobile device management (MDM) software.

In some circles, MDM has been re-named unified endpoint management (UEM) to incorporate all types of devices, including computers and tablets. Endpoint detection and response (EDR) solutions are also an important part of endpoint security, as they're helpful in detecting threats after attackers get access.

Common orthodoxy suggests that "if the device is managed, then it is secure and can be trusted." Device management tools are great at maintaining "golden images", recording what is accessed to prevent malware from being downloaded, and remotely wiping devices when they are lost or stolen.

The downside of device management tools is they're difficult to roll out and manage over time. Most importantly, MDMs also only tell half the story. What about devices that aren't managed?

MODERN COMPANIES CAN'T LIMIT ACCESS TO ONLY MANAGED DEVICES

While device management tools are highly recommended for company-issued machines, MDM strategies fall apart when not all devices that the workforce uses are company-issued and not all devices can be managed.

In fact, most employees (especially temporary workers, third party contractors, and partners) don't want their personal devices to be managed at all. Most organizations do not want to purchase and issue phones for employees as this can become quite expensive.

Instead, employers have to accommodate employees who are using their personal phones or other mobile devices. Besides, employees don't want their employer to infringe on their privacy and see or accidentally wipe their personal devices.

03

HOW TO VERIFY AND TRUST (SOME) DEVICES

Device trust has fundamentally changed; it's no longer a simple binary question asking if this device is managed or not. Instead, it requires security teams to establish if each endpoint is trustworthy enough "right now" as users are attempting to log into a resource.

In device trust, the first step is to verify the user behind the device, and the second step is to establish if the device is secure before allowing access.

STEP 1: VERIFY THE USER BEHIND THE DEVICE

Today, managed devices are registered with a user. Some of the techniques used to do this are less than optimal and can be easily subverted .

Worse, unmanaged devices are a black box. They're not registered and it's difficult to know who's device it is. With unmanaged devices, it's a free-for-all. Managing the risks of unmanaged devices isn't new, it's just becoming more prevalent and important.

The only way to validate a user behind an unmanaged device is to attach some type of identification to that device and to store it in a safe, unclonable way. That way, these registered devices are tied to a known identity that can be picked out from the rest of the bunch, separating the dogs from the wolves: the authorized users from the attackers.

Some organizations have turned to behavioral analysis to evaluate who is behind every device. This field is in the early stages and interesting in theory, but impractical for solving all problems around positively identifying users behind every device. Just because someone acts like a duck, doesn't mean they're actually a duck. Correlation is not causation.

For example, take the popular option of checking geolocation and IP addresses. There are two problems with this approach.

1. First, geolocation can be easily spoofed by an attacker. And with a hybrid workplace, everyone is logging in from everywhere. Employees could be traveling halfway across the world, so it's not as simple as banning access based on a singular location. What if the behavior is legitimate? If they get locked out, then they can't do work. (A reasonable exception to this rule is banning all access from a known bad geography like North Korea).
2. Second, IP addresses are unreliable because it's so easy to mask location with VPN and other encrypted tunnels.

While behavioral analysis provides additional context around the level of risk of the situation, it doesn't provide positive proof that it's actually a registered user on an approved device.

STEP 2: VALIDATE THAT THE DEVICE IS SECURE

In the past, checking the security posture of a device was typically a binary, basic check if the device was managed or not. However, just because a device is managed doesn't mean the device is still securely configured or that the security software is running properly on the device as expected. Mistakes happen (oops).

Because things can and do change, the security posture of a device is only valid for a given point in time. Security settings can change, software can break or be uninstalled, etc.

A device needs to be continuously checked to determine if it is still secure. Device security checks could include:

- Is the expected security software installed and running on the device (EDR, MDM, etc.)?
- Are there any current security alerts for the device?
- Are device security settings properly configured?
- Is the local firewall enabled?
- Is device access protected by a biometric?
- Is this the disc encrypted?
- Is the device jailbroken?

These are just a few of the questions security teams might want to answer to help them understand if the device is secure. These checks are crucial across all machines accessing company resources, whether the device is managed or unmanaged. The only way to get the whole picture is to conduct these checks automatically at scale on every device continuously over time.

DEVICE TRUST SHOULD BE ON A CONTINUUM AND CONTINUOUS

The answer to the question "is this device secure enough" is not a binary decision. Rather, it is based on a continuum that needs to account for the criticality of the resource being accessed. An important financial system does not have the same security requirements as the company vacation schedule. This decision also needs to include the risk tolerance of the organization and regulatory compliance requirements.

Deciding to trust a device is also a continuous process, where fresh, up-to-date data is necessary to understand the level of risk at the time of the access request. Again, it requires security teams to ensure that the endpoint is trustworthy right now, not that it was set up securely at some point in the past. The ability to assess the security posture of the device and enforce device trust policies on a continuous basis is an important requirement.

The security posture of the device changes over time. Security teams will want to ensure that native device security settings are turned on and that security software is installed, configured, and running on the device when the request for access is made.

> "Deciding to trust a device is also a continuous process, where fresh, up-to-date data is necessary to understand the level of risk at the time of the access request."

HOW BEYOND IDENTITY PROVIDES DEVICE TRUST

Beyond Identity solves the two important components of device trust: verify the user behind the device and find out if the device is secure.

Our cloud-native system positively validates that each device is registered to a known, authorized user and assesses whether the security posture of the device meets the security and compliance requirements necessary for accessing the application or resource being requested. The security posture of each device is assessed continuously, with new security checks conducted during every authentication transaction.

> "Beyond Identity is the only option in the market where security teams can create and securely store credentials on each endpoint, including phones, tablets, and desktops."

Beyond Identity provides an unmatched level of device trust.

Each device is cryptographically bound to a specific identity. Beyond Identity works in conjunction with technology built into modern endpoints to eliminate the password entirely and authenticate users with proven, secure asymmetric cryptography and X.509 certificates. This is the same technology ubiquitously deployed across the internet in the form of Transport Layer Security (TLS, the "lock" in the browser window), and trusted to safeguard trillions of dollars of transactions every day.

Beyond Identity is the only option in the market where security teams can create and securely store credentials on each endpoint, including phones, tablets, and desktops. Unlike other solutions, there is no centralized certificate (CA) authority. So there is no need to set up a PKI infrastructure, deploy a CA, or manage certificates.

Beyond Identity created a new type of authenticator that runs on each device. Beyond Identity's authenticator enables security teams to cryptographically validate the user and device identity and to assess the security posture of the actual authenticating machine. The Beyond Identity authenticator app is lightweight, can be downloaded and installed by users on a wide range of devices.

SO HOW DOES IT WORK?

Beyond Identity leverages the TPM (or secure enclave on Apple devices) present on modern devices to create a public/private key pair. This is the same hardware chip that's used to secure local device pins and biometrics. The private key remains securely stored in the TPM on the device and it can't be moved; neither Beyond Identity nor the user can access the private key.

During initial registration, the public key is stored in the Beyond Identity cloud. This cryptographically binds the user's identity to a specific device in a way that cannot be copied and moved by the user or digitally subverted by an adversary — a major advantage of the novel architecture. During each login request the Beyond Identity authenticator "asks" the device's TPM to generate an X.509 certificate which is forwarded to our cloud and validated using the public key.

Additionally, during each login request, Beyond Identity gathers up to 25+ device security posture attributes. Beyond Identity packages the data and cryptographically signs the package before forwarding it to the cloud. After the cloud backend confirms the data has not been tampered with in transit, the data is presented to the Beyond Identity risk-policy engine. Attributes — such as whether device biometrics are enabled, the status of the local firewall, and others — are evaluated against policy and a decision on whether to grant access is made.

Each time an authentication request is made a new risk-policy decision is made using the most current and validated data available. The data is stored in the data lake to provide an immutable record of every request and the security posture of the device at the time of request. This immutable record is important for proving compliance and very helpful for threat hunting teams.

The system does not require any third party endpoint security software and will incorporate additional security posture if these tools are present on the device. In addition to the attributes that Beyond Identity can analyze natively, our team has developed out of the box integrations with multiple MDMs. It can also be customized to look for any user-specific attributes, like if a certain software package is installed, running, and configured properly at the time of authentication.

?
Gatekeeper Enabled
Biometric Enabled
Disk Encryption Active
Jailbroken Status
Firewall Enabled
Filevault Active

06

CONCLUSION

The rise of cloud applications and remote work has made device trust an even more important part of your security story. The only way to verify trust of all your endpoints is to evaluate every single machine that accesses company resources, including unmanaged and BYOD, in real-time.

Beyond Identity delivers a cryptographic, tamper-proof method that binds a validated identity to a user's device. It gathers device security signals in real-time for every authentication so that security teams can enforce adaptive, risk-based controls and enable the right people to access resources from wherever they are.

With strong device trust in place, you can confidently control access to increasingly critical cloud applications and resources. Furthermore, you have laid down a foundational building block for your Zero Trust security architecture. Now that the endpoint has become the new security perimeter, securing company resources requires confidence that every endpoint is safe.

About Beyond Identity

Beyond Identity provides the most secure authentication platform in the world. Breaking down barriers between cybersecurity, identity, and device management, Beyond Identity fundamentally changes the way the world logs in–eliminating passwords and providing users with a frictionless multi-factor login experience. Beyond passwordless, the company provides the zero-trust access needed to secure hybrid work environments, where tightly controlling which users and which devices are accessing critical cloud resources has become essential. The advanced platform collects dozens of user and device risk signals during each login - enabling customers to enforce continuous, risk-based access control. The innovative architecture replaces passwords with the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily. Customers turn to Beyond Identity to stop cyberattacks, protect their most critical data, and meet compliance requirements.

Ready to Explore Passwordless Workforce Solutions?

GET A DEMO

beyondidentity.com | info@beyondidentity.com

BEYOND
IDENTITY