infinipoint

Essential Elements of Device Trust

Apply Zero Trust to Devices and Fortify Your Enterprise Against Cyberattacks

WHITE PAPER

While it's difficult to say when the world will finally see the end of the global pandemic, many of the changes it wrought on enterprises will likely never revert to pre-pandemic form. For instance, 96 percent of business leaders say the pandemic accelerated their digital transformation journeys by an average of 5.3 years[i], largely to support remote and work-from-home (WFH) initiatives.

Employees want to continue working remotely, with 98 percent indicating they want to be remote at least part time[ii] for the remainder of their career and 30 percent saying they're likely to switch jobs[iii] if forced to return to fully on-site work.

Likewise, enterprises have increased dependence upon the cloud to support remote workers, with 61 percent of businesses migrating workloads to the cloud in 2020.[iv] In 2021, public cloud infrastructure is expected to continue growing by 35 percent.[v]

As enterprises have shifted more resources to the cloud and enabled remote workers to access enterprise resources, cyberattacks have increased, as well. Between Q1 and Q2 2021, ransomware attacks increased by 288 percent.[vi] Moreover, cybercrime costs are expected to reach $10.5 trillion by 2025[vii] – making cybercrime the third largest "economy" in the world, after the United States and China.

Not surprisingly, the massive uptick in cybercrime has ignited a firestorm of response from governments and regulators concerned with securing infrastructure and other high-value assets. In May, the Biden administration issued an executive order aimed at protecting the US from cyberattacks[viii], including the directive to move toward Zero Trust Architecture (ZTA).

As explained by Gartner, Zero Trust is a misnomer[x] that doesn't mean "no trust." Instead, Zero Trust replaces implicit trust with continuously assessed, explicitly calculated adaptive trust. Not only can Zero Trust reduce the risk of cyberattacks, enterprises can use it to securely support remote initiatives.

Zero Trust is a security paradigm that replaces implicit trust with continuously assessed explicit risk and trust levels based on identity and context supported by security infrastructure that adapts to risk-optimize the organization's security posture.[ix]

– From NIST Special Publication on Zero Trust Architecture

Why Zero Trust Is Needed at the Device Level

When enterprises moved resources to the cloud prior to the pandemic, security wasn't a significant concern because users typically accessed company data from inside the perimeter and behind a firewall. As such, on-premise devices were trusted, and security issues could be quickly remediated.

However, the pandemic vastly altered this strategy, as enterprises more rapidly moved resources to the cloud. Meanwhile, previously authenticated users moved from inside the perimeter to remote locations, using unknown devices to access the enterprise through virtual private networks (VPNs) and virtual desktop infrastructure (VDI).

This massive shift makes it paramount for enterprises to apply Zero Trust principles to devices in the right way. According to the National Institute of Standards and Technology (NIST)[xi] , such Zero Trust policies should ensure a number of factors, including:

- Every device must have its security posture evaluated before gaining access to enterprise resources
- Zero Trust should continuously perform diagnostics and mitigation to monitor the state of devices and applications
- Patches and fixes should be applied as needed on devices

Likewise, the Cybersecurity and Infrastructure Security Agency (CISA) has created a maturity model for Zero Trust, specifically breaking down the elements needed for device Zero Trust into three categories – traditional, advanced and optimal, as seen in **Figure 1.**[xii]

It's helpful to break down the requirements from these agencies to better understand how to ensure Zero Trust at the device level.

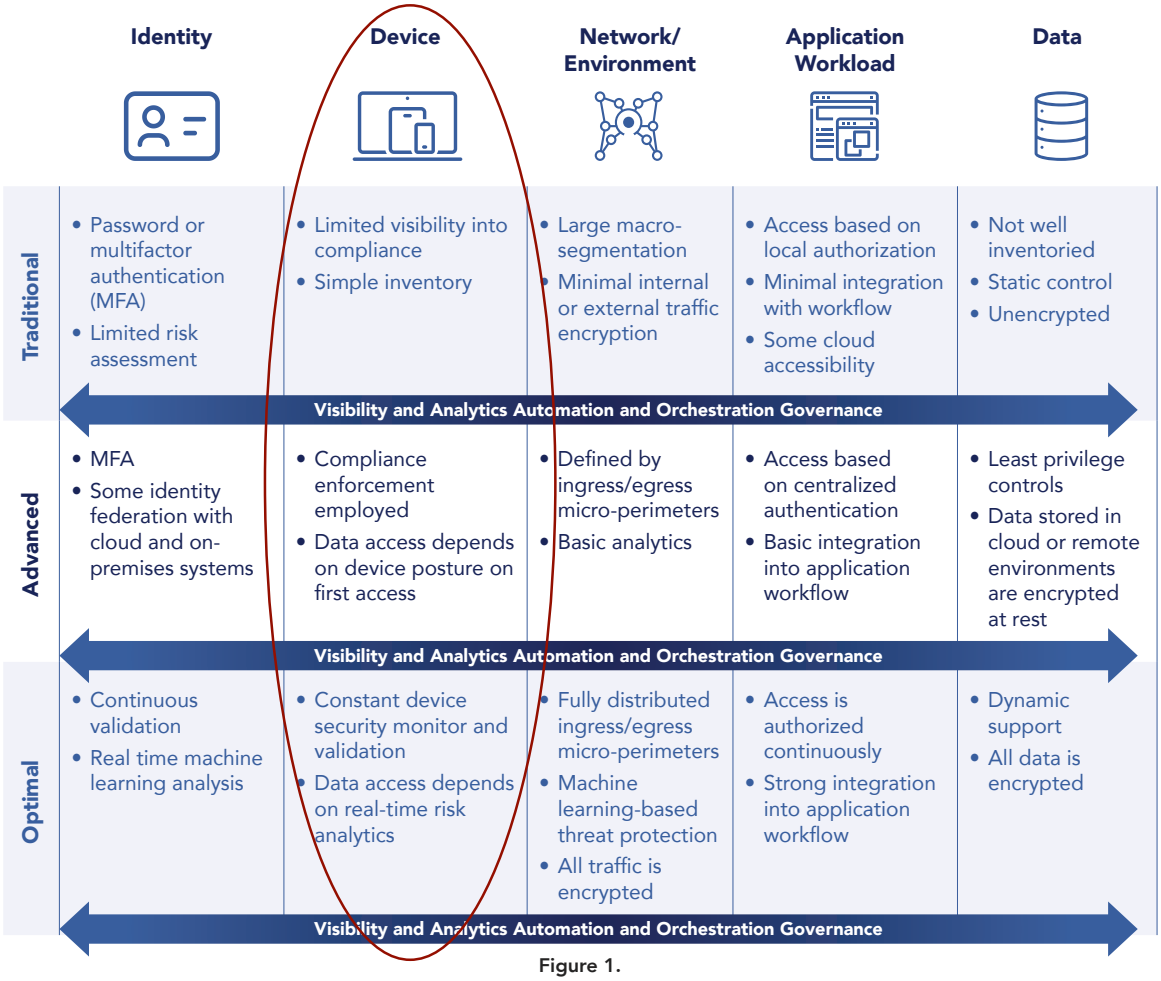

Figure 1.

Evaluating Security Posture

Many Zero Trust solutions on the market today authenticate and authorize users only at the "front door" when they first attempt to access enterprise resources. These device posture checks are used to ensure that devices are only allowed to connect to the network if they comply with predefined corporate security policies.

The problem with device posture checks is they typically only check against a small set of security parameters, and they don't have a way to continuously validate that the device is secure after the session is initiated and access is granted. Nor can such checks protect against legitimate users who authenticate from a new device that hasn't implemented adequate security controls.

Instead, security posture should determine where the device has been and how it's operating to determine whether it's given access, including:

- **Is the operating system (OS) current?** Attackers can compromise devices that run outdated or misconfigured firmware.
- **Are there any malicious or malware-infected apps?** Even legitimate apps can be poorly coded and leak information unintentionally.
- **What websites, servers and domains have been accessed?** Malware can be installed and data exfiltrated when a device accesses compromised content.
- **What network is the device using to connect?** Unencrypted connections and spoofed access points could result in confidential information being intercepted or altered.

> Building an architecture that **"never trusts, always verifies"** connections and that assumes a bad actor is active at all times leads to **highly resilient, highly flexible environments** that are much better suited to the demands of the modern workplace.
>
> – Gartner: How To Explain Zero Trust To Business Executives

Conditional vs. Adaptive Access

Conditional access gives users access to corporate applications and data based on the fulfillment of certain conditions, including multifactor authentication (MFA). Many enterprises have implemented MFA as part of a Zero Trust approach to users, which improves the overall security posture through strong user identity authentication.

However, this step alone doesn't accomplish true Zero Trust. Adaptive access control is defined by Gartner as an instance of context-aware access control that acts to balance the level of trust against risk. It enables organizations to better address access-related risks, while improving user experience.

By combining the rich context of device identity with adaptive access control, access permissions can be done in real time based on the user and device context. Adaptive access control balances Zero Trust risk reduction with end-user productivity. Moreover, it provides remediation options for non-compliant devices, including self-service or automated options to mitigate issues without disrupting access to critical services.

So, for instance, if a device is found to be non-compliant, users might be limited to read-only access for documents. Or a non-compliant device might be blocked from downloading files. The goal is to provide users with an adaptive Zero Trust approach that maintains business continuity without disrupting access.

Continuous Monitoring and Remediation

Another key facet to ensuring Zero Trust on devices is the ability to continuously monitor the device in real time. Many solutions on the market today only perform policy checks every 8 hours. During that 8-hour period, a device might become non-compliant for any number of reasons. However, if the non-compliance occurs in the first hour of the cycle, the device is non-compliant for the next seven hours without any way to remediate the issue or determine whether it's being used by bad actors.

Additional complications ensue when these products recognize that a device is non-compliant. When that happens, users are immediately blocked from accessing the system for a full eight hours until the next cycle runs. This happens regardless of the compliance issue – even if it could be remediated within seconds.

The solution is for Zero Trust to be applied to devices continuously in real time to ensure that non-compliant devices are identified as soon as they become non-compliant. When that happens, users should be given a range of remediation options that enable them to continue working.

For example, a user that has an outdated extension might be given a 1-click option to immediately bring the device into compliance. Or a user who needs to completely update the OS on a device might be given a grace period for addressing the issue, with the caveat that he has read-only access to documents until the OS is compliant.

How DIaaS Ensures Device-Level Zero Trust

As enterprises recognize the importance of establishing Zero Trust principles at the device level, several questions should be considered, including:

- What devices are accessing my applications and services?
- When is it OK to trust a device to access enterprise services, applications and resources?
- How can I control access by user and device rather than only by user?
- How can I ensure that devices are trusted before they are allowed to access apps and services?
- How can I ensure a strong device security posture without compromising business continuity?
- Is there a way to improve device security by enabling end user self-service security updates?

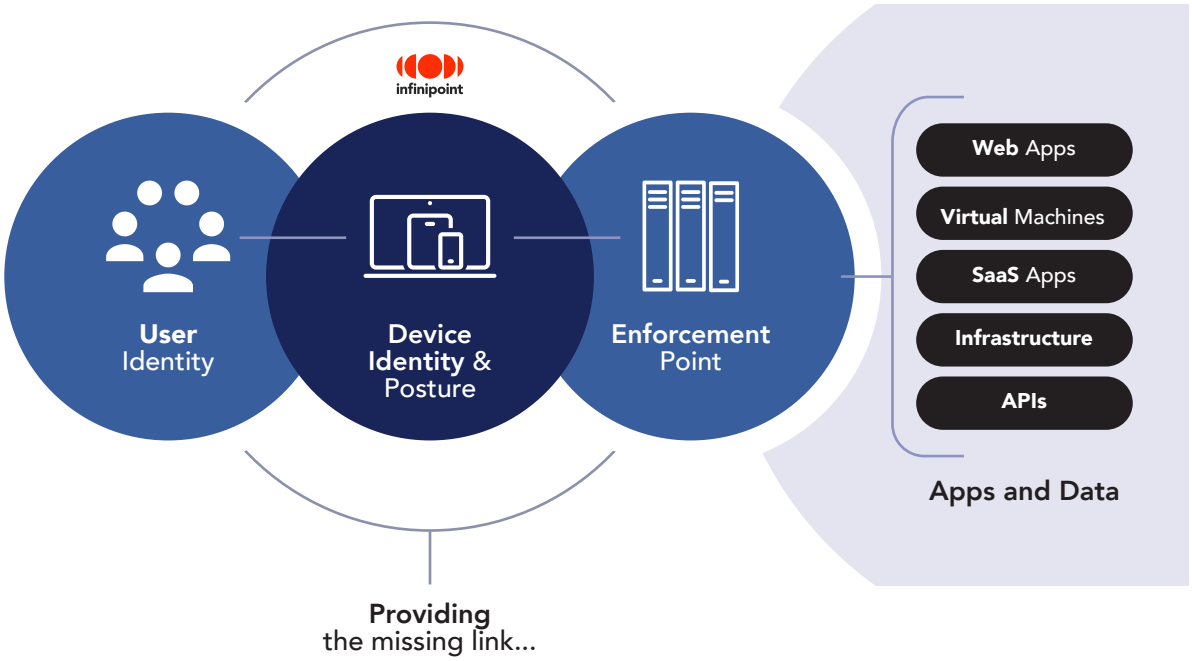

Figure 2: Device-Identity-as-a-Service enforces true Zero Trust security policies as part of the user authentication flow – before vulnerable devices can access business services and data.

Device-Identity-as-a-Service (DIaaS) enables enterprises to address all these questions and authenticate devices without disrupting user experience or business continuity. DIaaS is integrated as part of the user authentication flow and acts as a single enforcement point for every enterprise service, using any access method, whether on-premises or in the cloud. In short, DIaaS is a new security approach that enables "advanced" and "optimal" Zero Trust postures for devices.

Want to see how DIaaS can improve your Zero Trust device security?

BOOK A DEMO TODAY!

go.infinipoint.io/demo

Infinipoint is the pioneer in the Device-Identity-as-as-Service security category to extend a true Zero Trust security posture to devices. Infinipoint is the only solution that provides Single Sign-On (SSO) authorization integrated with risk-based policies and one-click remediation for non-compliant and vulnerable devices. This reduces risk by protecting access to an organization's data and services while transforming devices to support a world-class security posture.

To Learn More Visit, **infinipoint.io,** or Contact us at **Info@Infinipoint.io**

infinipoint

©2022 Infinipoint, Ltd. All rights reserved.

References

[i] IBM, Digital transformation at work

[ii] Buffer, The 2021 State of Remote Work

[iii] McKinsey & Company, The Great Attrition: The power of adaptability

[iv] Techjury (Source: Flexera), How Many Companies Use Cloud Computing in 2021

[v] Hosting Tribunal, Cloud Adoption Statistics for 2021

[vi] Helpnet Security (Source: NCC Group), Ransomware attacks increased by 288%

[vii] The Conversation, The increase in ransomware attacks during the COVID-19

[viii] Whitehouse.gov, Executive Order on Improving the Nation's Cybersecurity

[ix] NIST, Special Publication 800-207 Zero Trust Architecture

[x] Gartner, How to Explain Zero Trust to Technology Executives

[xi] NIST, Special Publication 800-207 Zero Trust Architecture

[xii] CISA, Zero Trust Maturity Model