infinipoint

# Device Identity and Security Posture

How to Secure Your Business Services from Insecure Devices

WHITE PAPER

# Executive Summary

The surge of cyberattacks and exposures during the recent workforce transformation, turning all employees to road warriors in one day, has rendered the architecture we have relied on for years as almost irrelevant. To defend against today's threats a new approach is necessary to secure enterprise assets, applications and data. While it has been mostly clear that the underlying assumption that everything inside the organization's network can be trusted, it is becoming clear that relying on secure traffic, validating and ensuring the user is who he claims he is, and using secure applications is only a part of what is needed. An enterprise must also validate the integrity and security of the devices accessing corporate resources and using business applications to dramatically decrease their attack surface and reduce exposure of their strategic services and data to insecure devices.

First introduced by Forrester Research, Zero Trust is a security model that addresses the shortcomings of failing perimeter-centric strategies by removing the assumption of trust from the equation.

With Zero Trust, essential security capabilities are deployed in a way that provides policy enforcement and protection for all users, devices, applications, data resources, and the communications traffic between them, regardless of location.

This paper discusses the need for and the details of securing the device component as part of the Zero Trust model. It explains the requirements laid out by the industry required to employ the Zero Trust model focusing on the device factor and how Infinipoint's platform fits in to accelerate Zero Trust adoption in the enterprise.

Benefits to organizations that employ Infinipoint Device-Identity-as-a-Service (DIaaS) to implement a Zero Trust model include:

- Dramatically improved effectiveness in mitigating data loss via visibility and safe enablement of applications, and detection and prevention of advanced threats.
- Greater efficiency for achieving compliance with security and privacy mandates.
- Increased ability to efficiently secure devices seamlessly.
- Substantially reduced total cost of ownership (TCO) for IT security.

# The Traditional Approach to Device Security, Why Isn't It Sufficient?

Over the last few years noticeable data breaches have exposed the current device security model as no longer effective. In the Office of Personnel Management (OPM) data breach of 2015 an estimated 22.1 million records were exposed. It has been described as one of the largest breaches of U.S. government data in history. It exposed records of people who had undergone background checks, as well as information about their family, friends and acquaintances, many of whom weren't even government employees.

The OPM data breach was a big wake-up call for the U.S. government to secure its information systems and infrastructures. In its aftermath, several initiatives were launched to improve and modernize the U.S. government's security posture. The American Technology Council, formed in May 2017 under the direction of the president, promptly coordinated and produced a report for federal IT modernization later that year, leading NIST and The National Cybersecurity Center of Excellence (NCCoE) to release the general guidance document NIST SP 800-207 (a few years later), Zero Trust Architecture, for adoption of a Zero Trust architecture (ZTA) in the federal government. This is a document that provides conceptual-level insight for Zero Trust and Zero Trust architectures, including deployment models, use case scenarios and discovered gaps in technologies.

The primary issue with the current castle-and-moat security strategy where protection mechanisms sitting in the organization's data center are set between the enterprise premises and the outside world, protecting ingress egress traffic flows and data, is the assumption that the organization can trust anything on the inside network.

There are a few false assumptions hiding in the current strategy:

- Today, most of the workforce is working from various locations, outside of the company premises. What used to be a few road-warriors a few years ago, is now most employees.
- Many of the applications and services are no longer located on-premises and are quickly migrating to the cloud.
- Users using their own devices (BYOD), which the organization doesn't have visibility or control over, to access corporate resources.

# The Traditional Approach to Device Security, Why Isn't It Sufficient?

In the last few years, security companies have focused on providing solutions to support this digital transformation:

- User identity and authenticity has become a major security concern. It has become an industry common practice to use two factors (or more) to validate the authenticity of a user.

- Secure network traffic has also become a strong point of focus. Securing network traffic and ensuring no one is able to intercept or modify the traffic is becoming crucial.

- The organization's data is distributed across many different cloud services, and companies have to modify their security architecture to be distributed, as the world is shifting from central approach to distributed approach.

- Trust of 3rd party applications, which are no longer sitting in the data center, is also critical. These applications are much more exposed and store sensitive business data of most companies. Every business service provider must adhere to compliance policies and rigorous security validation before being trusted by any enterprise to store their crown-jewels and sensitive data.

While these focus areas provide better security and support the digital transformation process, there is still a major factor that must be secured properly to safely implement these modern practices – the device.

## Existing Protection Mechanisms Lack the Necessary Capabilities to Secure Devices

Current solutions lack the ability to:

1. Uniquely identify the device to ensure they have control over all devices that access corporate services and applications, regardless of who owns the devices – the enterprise, the employee, a contractor or another 3rd party.

2. Verify device security posture against a fine-grained policy – the ability to specify dynamic, rapidly changing conditions, such as exposure to high-profile vulnerabilities, a specific process that is currently running, a specific certificate that is installed on device, any combination of these or many others.

3. Verify posture in real-time. User devices, today more than ever, are extremely dynamic. Users are installing new applications or removing existing applications, processes start up and terminate in seconds, new vulnerabilities are constantly being discovered. Only real-time verification of the current device state during access to an application ensures that the device indeed complies with enterprise requirements. Real-time posture verification is also crucial when allowing the user or administrator to quickly remediate the threat and get access back to what they were doing.

4. Efficiency remediate issues. When implementing a security solution there is always the balance between user efficiency and security. It is imperative that security solutions that continuously verify security posture are also able to allow the end user, regardless of his/her tech-savviness, to quickly remediate the issue and focus on what drives business.

## Device Trust and Access Control – Complementing the Zero Trust Model

The Zero Trust model was laid out in 2010 and has developed since, receiving great adoption from the industry. Implementing Zero Trust makes sure that no entity is inherently trusted based on ant sole principle, such as its origin, coming in from inside the network. In fact, a Zero Trust approach to security assumes that every user, device, system or connection is already compromised (by default) whether they are inside or outside of the network.

Looking at the device aspect of Zero Trust, which has been neglected compared to securing all other entities, it is becoming clear that least privilege should be applied to devices (i.e. they should only be allowed to do what is absolutely necessary) while they should always reassessed for their identity and posture.

The implications of these requirements are as follows:

1. There must be a unique device identity established by a trusted 3rd party. The identity cannot be forged or tampered with. This means that a known, trusted device is only that specific device. No other device can impersonate to look like another device and take advantage of the trust given to it.

2. Device Posture compliance must be assessed consistently, making sure that the device indeed complies with the policy assigned to it. User devices are rapidly changing, being exposed to additional risks by installing a new application or by changing endpoint protection configuration. In order to secure the data and applications, an organization must make sure that they only allow authorized devices, which are not exposed, to get access to sensitive information and applications.

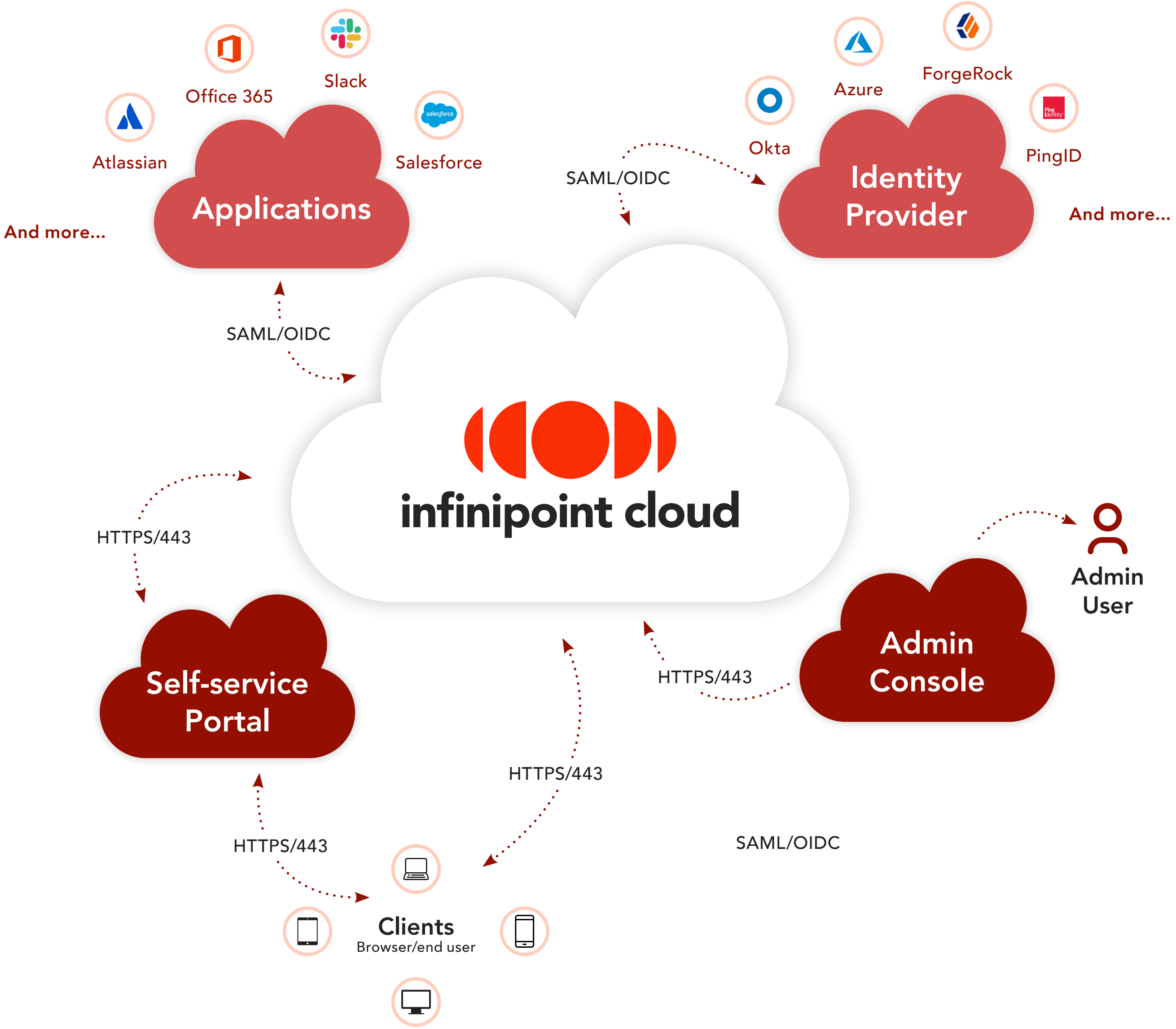

**Diagram 1 –** Infinipoint Solution Architecture

# Complementing Device-Focused Zero Trust with Infinipoint

This section identifies the key criteria for CISOs and IT security architects and managers to consider implementing a device-centric, Zero Trust architecture. For every such criterion, a brief description of the Infinipoint platform capabilities is provided to meet the corresponding requirements:

1. **One enforcement point for all services and applications.** Similarly to choosing one identity provider for user identity, it is inefficient to implement multiple solutions for different services when it comes to devices. It will require administrators to learn and adapt to multiple security solutions protecting different services, which will also likely have varying capabilities. The end users will become exhausted from having to handle and learn about multiple solutions in order to do their jobs. ***Infinipoint is a one enforcement solution for all business services and applications, supporting both SAML 2.0 and OpenID Connect.***

2. **Granular enforcement capabilities.** How security is implemented looks different from one organization to another. While there are common industry practices, like making sure a device has an endpoint protection product installed, an organization needs to have the ability to tailor their own policy and requirements, based on the risk and the specific device needs. ***Infinipoint provides a fine-grained policy mechanism allowing to fully-customize any policy and associate it with any device when access is requested to any application or service. It includes the ability to set policies based on dynamic attributes like real-live threats and outdated, vulnerable software installed.***

3. **Simple, efficient issue resolution.** Enforcing access control based on device posture must be simple and efficient. Otherwise, end users will spend their time chasing down the helpdesk, trying to resolve issues independently, finding workarounds, turning off security features. This can lead to users becoming frustrated and losing important time and focus instead of working on what they were hired to do. ***Infinipoint has an end user facing cloud-based portal, where the end user can resolve the issues he encounters with a click of a button (1-click remediation), including detailed guidance of what they need to achieve.***

4. **Real-time, always-on visibility and control.** When it comes to trusting user devices, which are dynamic and continuously changing, a daily check is not enough. That is because processes start and stop in seconds, new applications are being introduced into the system frequently, and new risks are being exposed. A secure organization must have the ability to enforce security decisions based on real-time data and not on past verifications. This means continuous assessment and validation of the device security posture. ***Infinipoint provides real-time identity and posture verification, ensuring trust is based on accurate, up-to-date data.***

5. **Scalability.** All of the above needs to be done in a way that supports substantial scale. In case the solution isn't scalable, it will not be able to address real-life requirements from a growing enterprise, damaging the end user experience, overall business continuity and the efficiency of the organization. ***Infinipoint is a cloud based platform that elastically scales to support any size of organization automatically without requiring specific or customized configurations to support even the largest environments.***

# How Does Infinipoint Device-Identity-as-a-Service Work?

The Infinipoint Console is a state-of-the-art asset management platform that provides visibility, access and control across all devices in real-time. Infinipoint discovers all assets that are associated with the organization using multiple methods: active scanning performed by its client, collection of data from 3rd party tools managing different assets, installation of its client using common deployment tools (SCCM, Jamf, and others) and by brokering identity authentication attempts to the organization's services and applications. It provides full coverage across all assets, regardless of their type, location, infrastructure or ownership.

Discovered assets can be turned into managed assets by installing a lightweight, non-intrusive client. The Infinipoint client allows the administrator to collect all data from managed assets, in real-time, and at scale. It uses unique peer-to-peer communication, utilizing data-transmit optimizations and scalable elastic architecture to support substantial amounts of data, transmitted in seconds, to the cloud.

The ability to scale horizontally, and receive large amounts of data allows the Infinipoint platform administrator to have up-to-date visibility across his or her entire inventory - from managed devices, internal and external hardware components, applications, services, local users, emails, and more.

Infinipoint also provides unique vulnerability and threat intelligence data, including exposure to attacks, campaigns or in-the-wild exploits based on current inventory and mitigation information, allowing the administrator to make intelligence-based decisions and take remediation actions to reduce their risk and their potential attack surface.

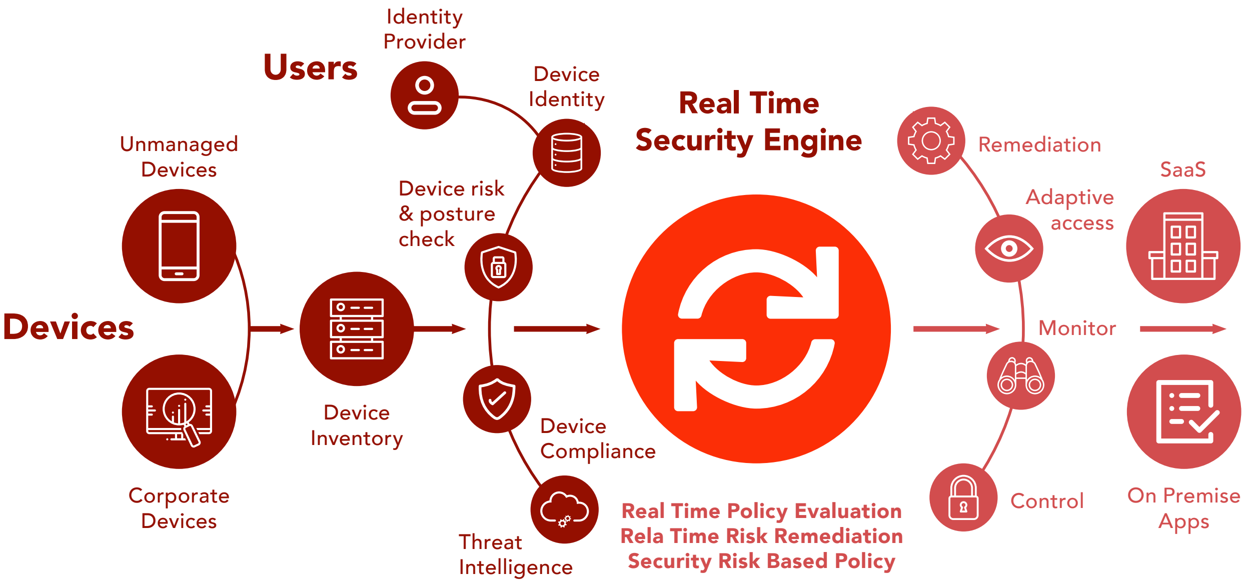

**Diagram 2 –** Access Control – coupling user authentication to device posture verification

# How Does Infinipoint Device-Identity-as-a-Service Work?

Infinipoint provides a unique one-stop solution for access control of all business applications and services, based on the device identity and security posture. The Infinipoint administrator can create tailor-made policies for different devices, define which users will have access to which services, and via which devices and under what circumstances. Enforcing these rules, while allowing the end user full transparency on the issues he currently has, how to fix them and automated, one-click remediation that can be initiated by the user. Remediation actions can also be initiated seamlessly, in the background, without the user involvement at all.

## DIaaS Flow

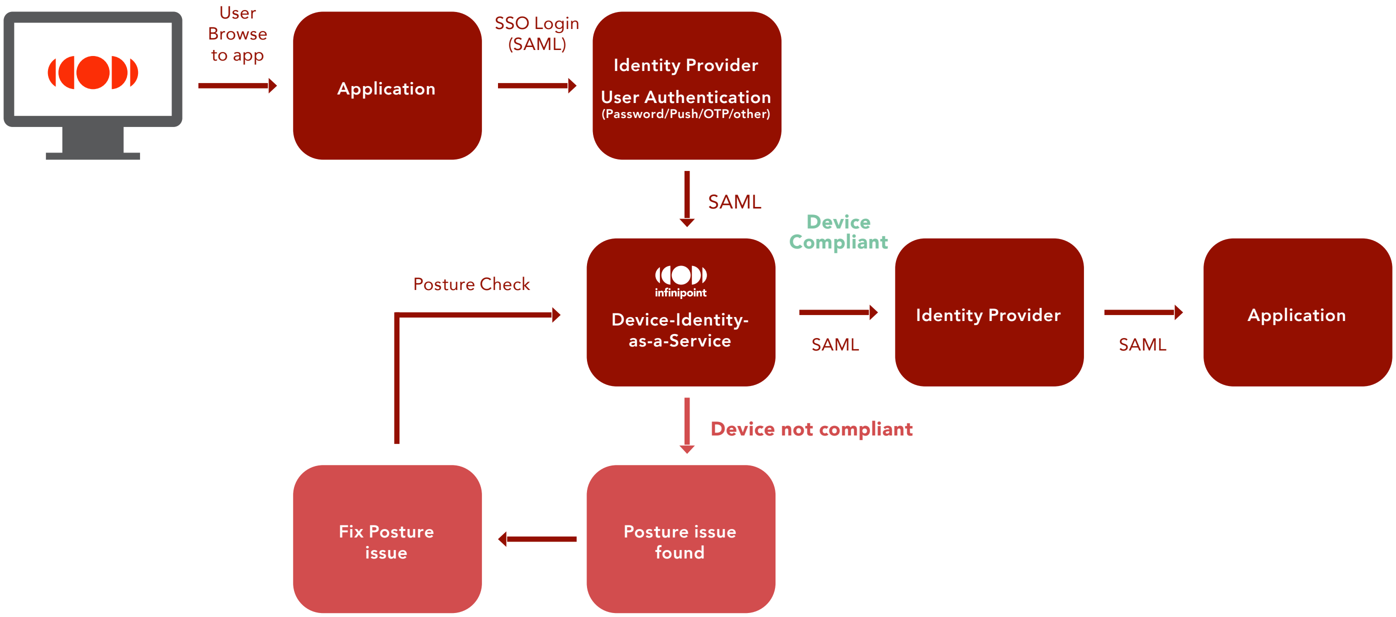

**Diagram 3** – End user login flow with Infinipoint Device-Identity-as-a-Service

## Benefits of Adopting Infinipoint Device Identity and Posture Verification

Using the Infinipoint platform has many associated business benefits. Here are a few of them:

1. **Reduce multiple platform and management overhead with a simple one-stop solution.** Get complete endpoint visibility and control, with granular enforcement policies across business applications. No need to set-up and maintain multiple security solutions for different applications or infrastructures.

2. **Dramatically reduce risk posture and the chances of being attacked.** Most attacks today are targeting known vulnerabilities or are caused by unintentional mistakes of not following security best practices. Enforcing access control will allow the users to become effective in their work, but not at the expense of security.

3. **Increase ROI by keeping users focused on the business.** When users can easily resolve issues without wasting time on doing their own investigating, or worse, they are denied access without an immediate resolution to the issue, they can spend more time on their productivity to support the business.

## Conclusion

The top security issue today is not just the surge of cyberattacks and exposures, but also the major changes to the technology and business landscape. There has been a massive workforce transformation where employees are now working outside of the corporate premises, whether as part of a hybrid work model or completely remote. This invalidates the assumption that the current security controls focused on securing the corporate premises are sufficient and effective in stopping today threats.

Organizations should strive to improve their current security posture, and apply Zero Trust principals to secure their devices and reduce the risk of a potential breach due to an insecure device.

Supporting digital transformation requires security to be a part of all involved entities - the device, the user, the service and the network. The Infinipoint platform is an ideal solution to implement device security effectively, and at scale, as it combines unparalleled visibility and control over all devices, regardless of their type, location or infrastructure.

# 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