infinipoint

SOLUTION BRIEF

Enable Continuous Adaptive Trust

Manage Secure Access Dynamically Using Device Risk Signals

While most organizations now employ best practices like multi-factor authentication (MFA), controlling access to sensitive systems based on binary, one-time identity checks is no longer sufficient. User-related risks may vary based on the device they are connecting from, different systems have varying levels of security and compliance sensitivity, and device security posture may change significantly during an active user session. Infinipoint makes it possible to assess device risk and govern system access continuously without adding unnecessary user friction.

Trusted access can't be a 'yes or no' decision

Many organizations make user identity and MFA the cornerstones of their access management strategy. But user identity alone doesn't provide a complete picture of your risk posture. The risks posed by the same user may vary greatly depending on the device they are connecting from and other contextual factors. Risk exposure may also escalate after the initial point of authentication. For example, sophisticated attackers increasingly use techniques like social engineering, coercion, and even bribery to gain access to insiders' authenticated systems. At the same time, blindly stepping up the frequency of MFA challenges or enforcing policies when there isn't a true threat is frustrating to legitimate users and disruptive to overall business productivity.

Benefits

Infinipoint enables you to:

- **Reduce overall security and compliance risk**
- **Minimize security-related productivity disruptions**
- **Unlock new capabilities from your SASE platform**
- **Improve IT and security team efficiency**

Mitigate ongoing risk without frustrating users

Infinipoint assesses the security posture of user's devices both during and after the initial point of authentication. But unlike legacy device security approaches, our device checks don't lead to user productivity dead ends or new IT trouble tickets. Users connecting from insecure or non-compliant devices are presented with simple, self-service remediation options that allow them to address issues immediately. They can also be granted compliance grace periods or limited access when threat intelligence feeds indicate that the risk of exploit is low, striking an optimal balance between risk mitigation and business productivity. Ongoing device assessments after initial authentication ensure that protection is continuous, and optional integration with leading secure access service edge (SASE) enables granular conditional access policies.

Infinipoint Highlights

Continuous Assessment

Device checks after initial authentication detect new risks and adapt access policies as necessary

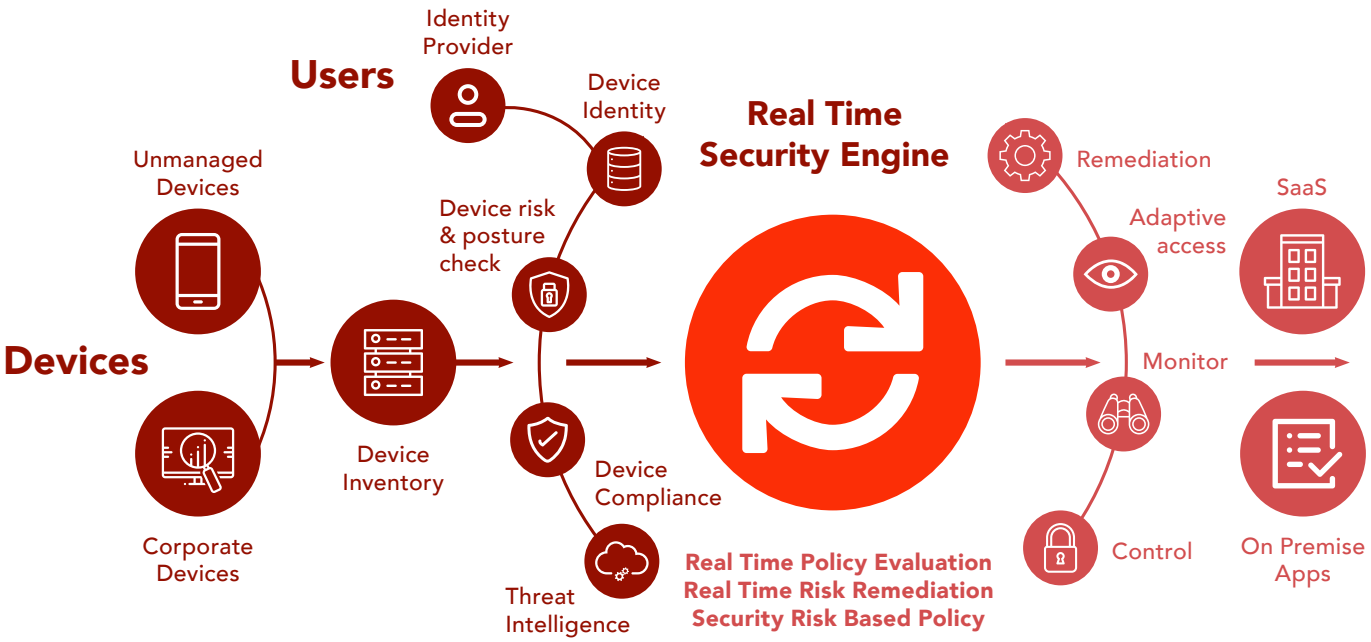
User Empowerment

Self-service remediation and intelligent policies based on threat intelligence minimize disruptions.

SASE Integration

Optional SASE integration provides granular control over resource access based on device security posture

infinipoint



Infinipoint assesses device security posture continuously while avoiding user disruption by assessing threat severity based on threat intelligence and providing self-service remediation capabilities to users.

Bring security and business productivity into balance

- **Reduce overall security and compliance risk** -- Limit exposure to ransomware, malicious insider activity, and many other device security risks by extending risk assessment beyond initial authentication. Combine continuous visibility into device security posture, timely threat intelligence, and granular policy controls to mitigate risks with precision.
- **Minimize security-related productivity disruptions** -- Enforce security policies based on threat intelligence and device security posture signals while limiting user disruptions to those situations that present clear and immediate risk. Empower users to self-remediate device compliance issues, and provide limited access options on an interim basis based on threat intelligence and your organization's risk tolerances
- **Unlock new capabilities from your SASE platform** -- Enforce precise conditional and limited access policies based on device identity and security posture in addition to user identity. Adapt SASE policies dynamically when device risk assessments change after initial authentication.
- **Improve IT and security team efficiency** -- Minimize support burden by providing intuitive self-service capabilities to users and replacing "all or nothing" access options with a more pragmatic risk-based model. Enable secure use of unmanaged employee or contractor-owned devices without compromising security and compliance standards.

infinipoint

About Infinipoint

Infinipoint is the pioneer of Device-Identity-as-a-Service (DIaaS), addressing Zero Trust device access and enabling enterprises of all sizes to manage access to corporate services and data based on the security posture of end user 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.

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