infinipoint

SOLUTION BRIEF

Secure Your BYOD Initiative

Validate Unmanaged Devices and Improve User Experience

Infinipoint Device-Identity-as-a-Service (DIaaS) enables secure productivity from unmanaged workstations and mobile devices owned by employees or third-party contractors. Continuous device security posture assessment, self-service remediation, and risk-based security policies make it easy for users to work from unmanaged devices while adhering to corporate security and compliance standards.

Unmanaged device usage is an unavoidable reality

Use of unmanaged devices for business purposes is now a fact of life. According to a Gartner[1] survey, 55 percent of digital workers "are using personally owned devices for their work at least some of the time." Meanwhile, third-party contractors also frequently require access to sensitive applications from unmanaged devices.

This creates a complex set of security and compliance challenges for IT and security teams. Enrolling personal or third-party devices into legacy device management systems is highly impractical. Users often resist the idea, and support cost and complexity are also significant obstacles. At the same time, validating the security posture of unmanaged devices is critical for managing risk and ensuring compliance.

Benefits

Infinipoint enables you to:

- **Accelerate employee and contractor onboarding**
- **Increase user productivity and satisfaction**
- **Reduce security and compliance risk**
- **Avoid unnecessary cost and complexity**

Assess and secure unmanaged devices without IT or user friction

Infinipoint assesses the security posture of unmanaged devices attempting to access corporate resources, enforces a set of contextual security policies, and guides users through any self-service remediation steps required to achieve policy compliance. This gives employees and contractors the flexibility to use unmanaged devices securely with a simple and frictionless experience while reducing IT efforts and maintenance. Infinipoint maps devices to specific users, performs device security posture assessments during and after authentication, and governs access to corporate resources with risk-based security policies. Multiple device assessment and integration options provide deployment flexibility and extend coverage to all common workstation and mobile operating systems.

Infinipoint Highlights

Lightweight Integration

Client-based and clientless assessment options minimize device footprint and resource impact.

Self-Service Remediation

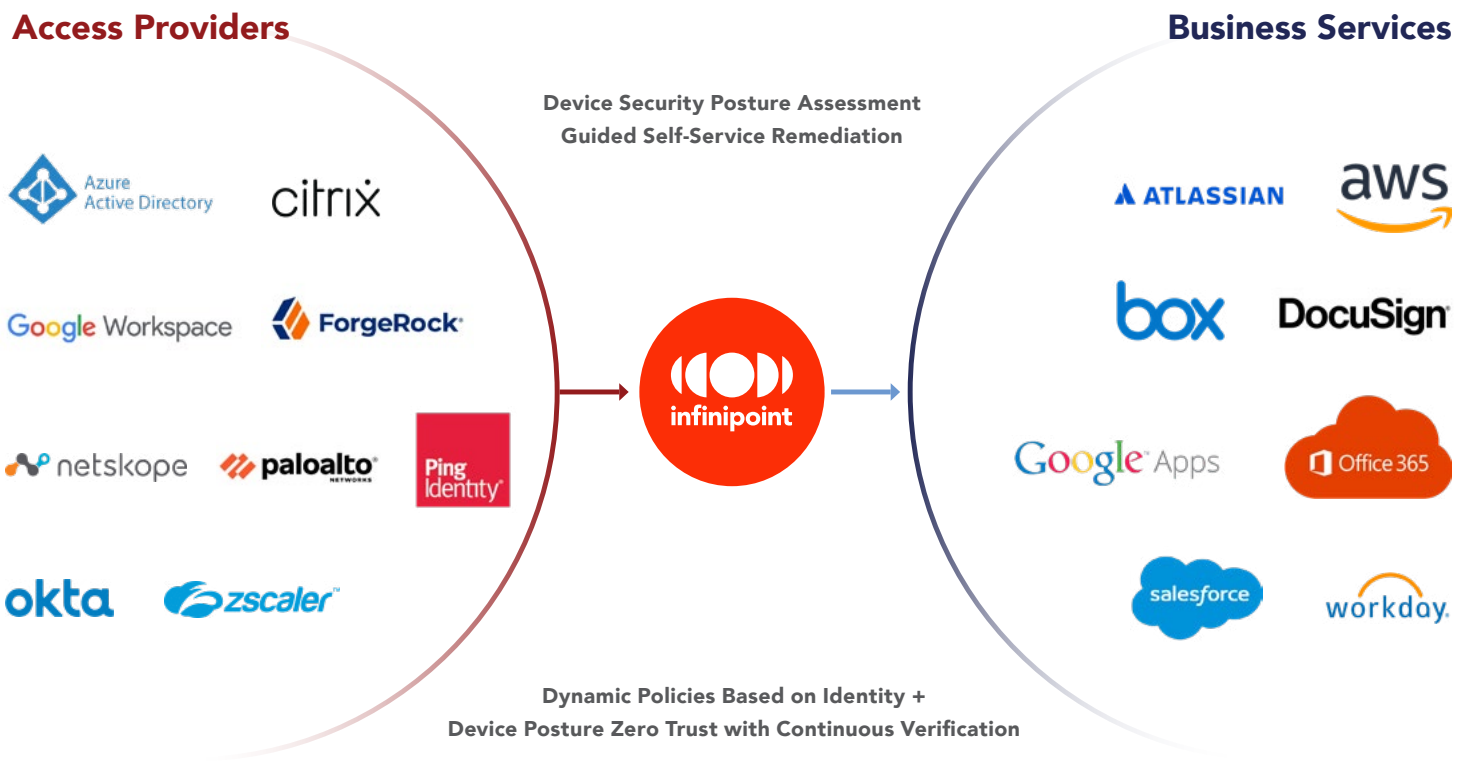
Clear and simple guidance helps users correct device compliance issues without IT dependence or productivity loss.

Continuous Assessment

Device risk is assessed during and after authentication, creating a true Zero Trust device posture.

[1] Gartner Press Release, "Gartner Survey Finds 1-in-5 Workers Consider Themselves Digital Technology Experts Since COVID-19," April 26, 2021.

infinipoint



Infinipoint combines insights about identity and entitlements with information about device security posture to manage access to sensitive business services dynamically.

Bring security and business productivity into balance

- **Continuous Conditional Access** -- Ensure only compliant devices access sensitive services, activities, and data. For example, create a device identity policy where only devices with the latest Windows security update are allowed access.
- **Accelerate employee and contractor onboarding** -- Simplify onboarding of new full-time hires and contractors by removing corporate workstation provisioning as a bottleneck to productivity. Empower users to work with personal or contractor-owned devices in a secure and compliant manner as an alternative or complement to company-managed devices.
- **Increase user productivity and satisfaction** -- Give users the flexibility to choose the best device for the job based on their device preferences, tasks, and work location. Increase productivity, satisfaction, and retention by avoiding productivity roadblocks and keeping device control in users' hands.
- **Reduce security and compliance risk** -- Mitigate device-based security and compliance risks while acknowledging the practical need for unmanaged device usage. Enforce device security standards and ensure compliance without assuming direct control over devices.
- **Avoid unnecessary cost and complexity** -- Limit use of enterprise device management and patching systems to select corporate devices. Provide easy-to-use self-service remediation capabilities that address device vulnerabilities and security risks without putting an unnecessary burden on IT teams or users.

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