DTS

Infinipoint Device Identity as a Service (DIaaS)

Infinipoint Device Identity as a Service

Der Wandel von einer zentralen zu einer verteilten Arbeitsweise in Unternehmen geht mit einer massiven Nutzungszunahme von mobilen Endgeräten einher. Dadurch erhöht sich wiederum die Anfälligkeit für die Ausnutzung von Sicherheitslücken, Malware oder Konfigurationsfehler drastisch. Um Ihre Unternehmens- und Cloud-Infrastruktur zu schützen, ist es von entscheidender Bedeutung, dass Sie Einblick in die aktuelle Sicherheitslage der Assets Ihres Unternehmens haben, um eine angemessene Cyber-Hygiene aufrechtzuerhalten und Compliance-Standards durchzusetzen – für jedes Asset, überall im Netzwerk, jederzeit.

Die meisten Lösungen bieten nur einen teilweisen Einblick, sind ungenau, arbeiten nicht in Echtzeit und können das erhöhte Asset-Volumen von Remote-Mitarbeitenden nicht bewältigen. Da Benutzer über VPNs, Zero-Trust Network Access (ZTNA) und Identitätsanbieter auf Ihre Unternehmensanwendungen und -daten zugreifen, reicht selbst die stärkste Benutzeridentitätsauthentifizierung allein nicht aus. Eine umfassende Überprüfung der Sicherheitslage des Endpunkts ist ebenfalls erforderlich, um sicherzustellen, dass der sich verbindende Endpunkt das richtige Sicherheitsniveau hat. Device Identity as a Service (DIaaS), basierend auf der Lösung unseres strategischen Partners Infinipoint, liefert dieses fehlende Puzzlestück des Zero-Trust-Sicherheitsmodells: Die Integrität des Devices als Bindeglied zwischen User Identity und der Applikation.

- Kontinuierliche Bewertung der Device-Sicherheitslage
- Einheitliche SSO-Technologie
- Zutrittssicherheit integriert mit IT-Security Asset Management
- Statische & dynamische, auf realen Risiken basierende Richtlinien
- Self-Service Portal für Endanwender
- Admin-Konsole für Visibilität & Kontrolle in Echtzeit
- One-Klick Remediation

Die Next-Generation Asset Management Platform von Infinipoint erkennt alle Assets und ermöglicht es Ihnen, diese in Echtzeit zu überprüfen und zu aktualisieren. Da IT-Umgebungen immer komplexer werden, befinden sich Assets überall: im Rechenzentrum, in der Zentrale, in den Filialen und zu Hause. Es gibt mehr Arten von Endpunkten, Workloads, IoT-Geräten und Softwarekomponenten als je zuvor. Gleichzeitig ändert sich die Risikolage jedes Assets je nachdem, wo, wann und von wem es genutzt wird. Infinipoint nutzt modernste Technologien, um eine Komplettlösung für die Sichtbarkeit und Kontrolle von tausenden von IT-Ressourcen für Unternehmen jeder Größe bereitzustellen – sofort und egal wo sie sich befinden: On- & Off-Premises, in Niederlassungen oder bei Mitarbeitenden in Homeoffice.

Interaktives Asset Management
Infinipoint ermöglicht einen durchgängigen Prozess für die Verwaltung von Assets und die Verbesserung ihrer Sicherheitslage in dynamischen IT-Umgebungen.

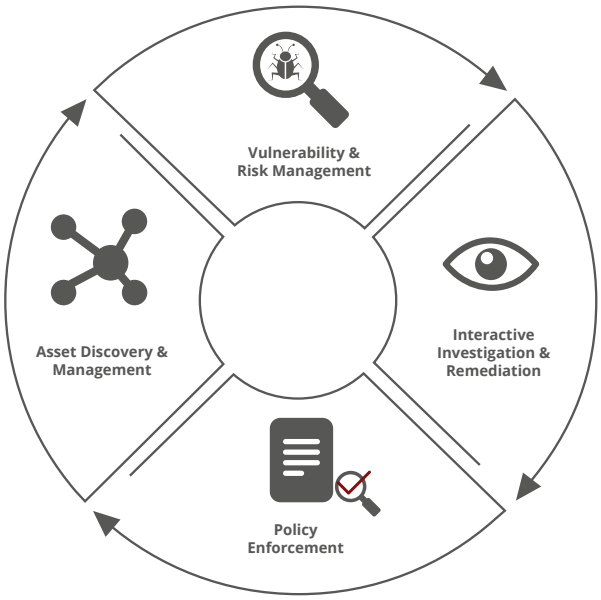
Asset-Erkennung & -Verwaltung
Durch die kontinuierliche Echtzeit-Erkennung und -Verwaltung aller Assets werden traditionelle Endpunkte, VMs, IoT-Geräte und Cloud-Workloads erfasst, sowohl innerhalb als auch außerhalb des Unternehmensnetzwerks. Das passiert auch in komplexen, sich schnell verändernden Umgebungen sehr präzise.

Schwachstellen- & Risikomanagement
Identifizieren und priorisieren Sie Schwachstellen durch kontextbasierte Bewertungen, die Bedrohungsdaten und Netzwerksichtbarkeit umfassen. Auch Konfigurationsrisiken können identifiziert und priorisiert werden, z. B. Benutzerzugriffe, Betriebssystemkonfigurationen, Hardening, Hardware & Wechselmedien sowie nicht verwendete Software.

Interaktive Untersuchung & Behebung
Sämtliche Assets können problemlos abgefragt werden, um in Echtzeit Änderungen vorzunehmen und die damit verbundenen Auswirkungen zu bewerten. Beheben Sie Probleme per Patch oder Konfiguration, schrittweise oder auf einmal. Validieren Sie Abhilfemaßnahmen an Ort und Stelle und beheben beheben Sie die Probleme sofort.

Durchsetzung von Richtlinien
Die Lösung hilft Ihnen zudem die Einhaltung der Sicherheitsrichtlinien des Unternehmens und der branchenüblichen Best Practices zu gewährleisten, sowohl innerhalb als auch außerhalb des Unternehmens. Erzwingen Sie Sicherheitsmaßnahmen, bevor Sie eine Remote-Verbindung von unsicheren Standorten aus herstellen.

Das fehlende Puzzlestück des Zero-Trust-Sicherheitsmodells
DIaaS ist eine umfassende Device Identity & Posture Lösung die sich nahtlos in die Single-Sign-On-Authentifizierung einfügt und als eine zentrale Enforcement-Stelle für sämtliche Unternehmensdienste fungiert. Sie ermöglicht einen kontrollierten Zugriff auf Grundlage von Benutzer, Endgerät sowie Dienst und wendet Risikoinformationen an, um statische und dynamische Zugriffs-Richtlinien durchzusetzen. Der Cloud-basierte Service bietet Ihnen so die notwendigen Informationen zum Zustand Ihrer Endgeräte und Möglichkeiten zur Remediation in nur einer Oberfläche.

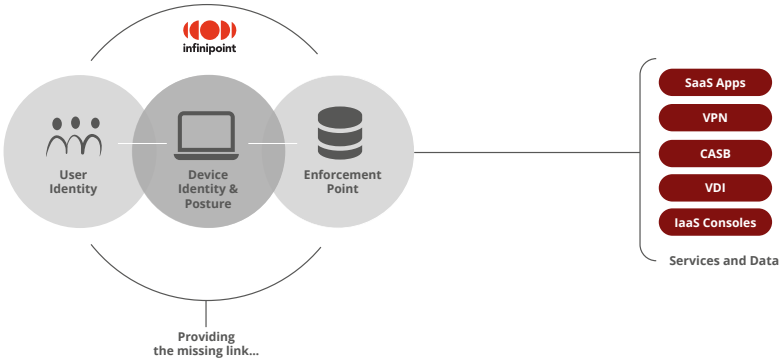


Das fehlende Puzzlestück des Zero-Trust-Sicherheitsmodells

DIaaS ist eine umfassende Device Identity & Posture Lösung die sich nahtlos in die Single-Sign-On-Authentifizierung einfügt und als eine zentrale Enforcement-Stelle für sämtliche Unternehmensdienste fungiert. Sie ermöglicht einen kontrollierten Zugriff auf Grundlage von Benutzer, Endgerät sowie Dienst und wendet Risikoinformationen an, um statische und dynamische Zugriffs-Richtlinien durchzusetzen. Der Cloud-basierte Service bietet Ihnen so die notwendigen Informationen zum Zustand Ihrer Endgeräte und Möglichkeiten zur Remediation in nur einer Oberfläche.

Die Lösung liefert das fehlende Puzzlestück des Zero-Trust-Sicherheitsmodells, wie es von Gartner, NIST und Google als Best Practice vorgegeben wird: die Integrität des Devices. Der Service liefert Ihnen hohe Sicherheits-Mehrwerte, indem sie den Zugang zu den Daten und Diensten Ihres Unternehmens schützen und gleichzeitig Ihre Endgeräte in einen erstklassig sicheren Zustand versetzen, um Sicherheitsverletzungen zu verhindern:

- Einführung eines risikogesteuerten Zugriffs-Prozesses innerhalb der Organisation durch Erkennung, Verwaltung und Beseitigung von Bedrohungen in Echtzeit
- Verbessert die Effizienz, indem das Sicherheitsmanagement durch Prozesse und Automatisierung optimiert wird, einschließlich der One-Klick-Remediation für Endnutzer



DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de