



infinipoint

Device Identity as a Service (DlaaS) *managed by DTS*

Das Arbeiten in Unternehmen hat sich während der letzten Monate und Jahre zunehmend von einer zentralisierten zu einer verteilten Arbeitsweise verändert. Dieser Wandel geht einher mit einer massiven Nutzungszunahme von mobilen Endgeräten, wodurch sich die Anfälligkeit für die Ausnutzung von Sicherheitslücken, Malware sowie Konfigurationsfehler drastisch erhöht hat.

Darüber hinaus werden immer mehr Applikationen aus der Cloud bereitgestellt und sind jederzeit von überall verfügbar. Obwohl dabei der Benutzer authentifiziert, der Netzwerkverkehr verschlüsselt und die SaaS-Anwendung geschützt ist, wird das zugreifende Endgerät und dessen Sicherheitszustand nicht beachtet. Aus diesem Grund wird das Endgerät zum schwächsten Glied der IT-Sicherheit des Unternehmens. Eine Authentifizierung des Benutzers hat dabei wenig Nutzen, wenn dieser von einem unsicheren, nicht vertrauenswürdigen Gerät auf die sensiblen Daten und Dienste zugreifen kann. Somit ist es von entscheidender Bedeutung, dass Sie Einblick in die aktuelle Sicherheitslage der Assets Ihres Unternehmens erhalten, um eine angemessene Cyber-Hygiene aufrechtzuerhalten sowie Compliance-Standards durchzusetzen - für jedes Asset, überall auf der Welt, jederzeit.

- Einheitliche Single Sign-On (SSO) Technologie
- Zutrittssicherheit kombiniert mit IT-Security Asset Management
- Statische und dynamische auf Risiken basierende Richtlinien
- Self-Service Portal für Endanwender
- Admin-Konsole für Visibilität und Kontrolle in Echtzeit
- Multi Faktor Authentication

Die Lösung

Device Identity as a Service (DlaaS), basierend auf der Lösung unseres strategischen Partners Infinipoint, liefert das fehlende Puzzlestück des Zero-Trust-Sicherheitsmodells, wie es von Gartner, NIST und Google (den Erfindern von BeyondCorp Zero-Trust) als Best Practice vorgegeben wird: Die Integrität des Devices. Es bietet somit das Bindeglied zwischen User Identity und der Applikation.

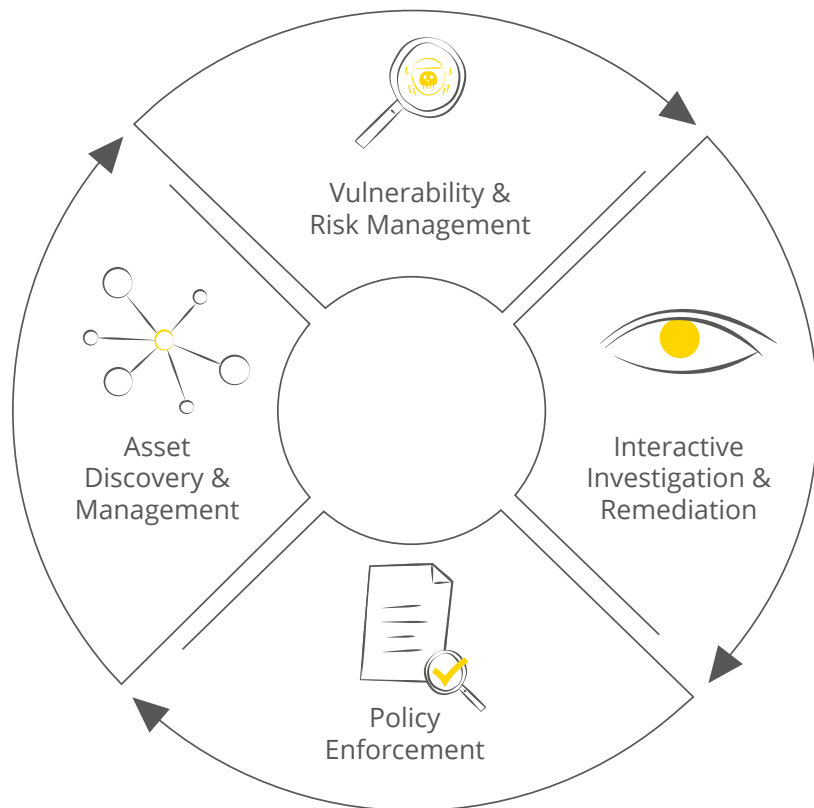
Die alleinige Authentifizierung von Benutzern für den Zugriff über VPNs, Zero-Trust Network Access (ZTNA) oder eines Identitätsanbieters auf Ihre Unternehmensressourcen und Anwendungen ist nicht ausreichend. Eine umfassende Überprüfung der Sicherheitslage des Endpunkts ist ebenfalls erforderlich, um sicherzustellen, dass der sich verbindende Endpunkt das richtige Sicherheitsniveau besitzt. Durch die permanente Einhaltung der Cyber-Hygiene verhindern Sie, dass böswillige Akteure erfolgreich in den Laptop eines Mitarbeitenden eindringen und die authentifizierte Identität nutzen, um böswillige Aktivitäten durchzuführen.

DlaaS liefert eine kontinuierliche Bewertung der Device-Sicherheitslage und unterstützt Sie somit bei der Einführung eines risikogesteuerten Zugriffsprozesses. Zudem bewahren Sie durch die Erkennung, Verwaltung und Beseitigung von Bedrohungen in Echtzeit, jederzeit die Kontrolle Ihrer weltweiten Assets. Durch Automatisierung, standardisierte Prozesse und einen einfachen Enduser Self-Service zur Herstellung der Geräte-Compliance (mit nur einem Klick) entstehen keine zusätzlichen Aufwände für die enorme Erhöhung der Sicherheit. Hierbei setzen wir die stetige Befolgung von Unternehmensrichtlinien und Industriestandards durch, bevor der Zugriff auf Ihre Cloud und Unternehmensnetzwerke gewährleistet wird.



Einzigartige Sichtbarkeit und Kontrolle aus einer Hand

Teil des effizienten und unendlich skalierbaren Managed Services ist zudem eine vollumfassende Plattform, die den kompletten Prozess des Asset- und Risk-Managements abdeckt.



Asset Discovery & Management

- Kontinuierliche Echtzeit-Erkennung und Verwaltung von Assets, einschließlich klassischer Endpunkte von VMs, IoT bis hin zu Cloud Workloads
- Präzise Erkennung für komplexe, sich verändernde Umgebungen
- Unabhängige Erkennung von Geräten, egal ob On-Premises oder Remote

Vulnerability & Risk Management

- Erkennung von IT-Konfigurationsproblemen, hochentwickelten Bedrohungen und Missbrauch von Sicherheitspraktiken in Echtzeit
- Überblick von Schwachstellen in Betriebssystemen und Anwendungen in Echtzeit unter Windows, Mac und Linux
- Priorisierung von Schwachstellen durch kontextbasierte Bewertungen

Policy & Compliance

- Überprüfung von IT-Richtlinien des Unternehmens (aktivierter Endpunktschutz, Firewall und vieles mehr)
- Verifizierung gängiger Standards
- Kontrolle der benutzerdefinierten Richtlinien mithilfe eines beliebigen Skripts oder eines „Osquery“

Remediation

- Remote-Behebung von Schwachstellen und Konfigurationen für Administratoren
- Self-Service Problembhebung für Endbenutzer
- Empfehlungen für manuelle Abhilfemaßnahmen

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

DTS Systeme Wien GmbH
+43 1 3614414-10

www.dts.de
info@dts.de