

The background of the entire page is a dark, high-contrast image of a knight in full plate armor. The knight's right hand is raised, holding a sword hilt. The armor is highly detailed with rivets and plates. A yellow diagonal band cuts across the lower right portion of the image, partially obscuring the knight's armor and the text below.

DTS

INFINIPOINT DEVICE IDENTITY AS A SERVICE (DIAAS)

INFINIPOINT DEVICE IDENTITY AS A SERVICE

The shift from a centralized to a distributed way of working in companies is accompanied by a massive increase in the use of mobile devices. This in turn drastically increases the vulnerability to exploitation of security vulnerabilities, malware or configuration errors. To protect your enterprise and cloud infrastructure, it's critical that you have visibility into the current security posture of your organization's assets to maintain proper cyber hygiene and enforce compliance standards – for every asset, everywhere on the network, all the time.

Most solutions provide only partial visibility, are inaccurate, don't work in real time and can't handle the increased volume of assets from remote workers. With users accessing your corporate applications and data via VPNs, Zero Trust Network Access (ZTNA) and identity providers, even the strongest user identity authentication alone is not enough. A comprehensive endpoint security posture review is also required to ensure that the connecting endpoint has the right level of security. Device Identity as a Service (DlaaS), based on the solution from our strategic partner Infinipoint, provides this missing piece of the zero trust security model puzzle: the integrity of the device as the link between user identity and the application.

- Part of the zero trust model
- Continuous assessment of the device security situation
- Standardized SSO technology
- Access security integrated with IT security asset management
- Static & dynamic policies based on real risks
- Admin console for real-time visibility & control
- One-click remediation
- DTS managed service

Infinipoint's Next-Generation Asset Management Platform recognizes all assets and enables you to check and update them in real time. As IT environments become more complex, assets are everywhere: in the data center, at headquarters, in branch offices and at home. There are more types of endpoints, IoT devices, software components, etc. than ever before. At the same time, the risk situation of each asset changes depending on where, when and by whom it is used. Infinipoint uses cutting-edge technologies to provide a complete solution for visibility and control of thousands of IT assets for organizations of all sizes - instantly and wherever they are located.

INTERACTIVE ASSET MANAGEMENT

Infinipoint enables an end-to-end process for managing assets and improving their security posture in dynamic IT environments.

ASSET RECOGNITION & MANAGEMENT

Continuous real-time detection and management of all assets captures endpoints, VMs, IoT devices and cloud workloads, both inside and outside the corporate network. This happens very precisely, even in complex, rapidly changing environments.

VULNERABILITY & RISK MANAGEMENT

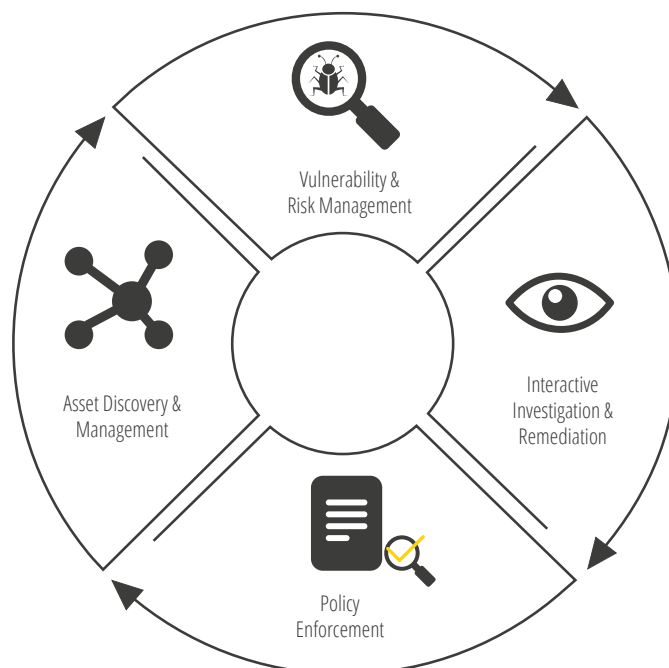
Identify and prioritize vulnerabilities through context-based assessments that include threat intelligence and network visibility. Configuration risks can also be identified and prioritized, e.g. user access, operating system configurations, hardening, hardware & removable media and unused software.

INTERACTIVE INVESTIGATION & REMEDIATION

All assets can be easily queried to make changes in real time and assess the associated impact. Fix issues via patch or configuration, incrementally or all at once. Validate remedies on the spot and fix issues immediately.

ENFORCEMENT OF GUIDELINES

The solution also helps you ensure compliance with corporate security policies and industry best practices, both inside and outside the organization. Enforce security measures before connecting remotely from insecure locations.



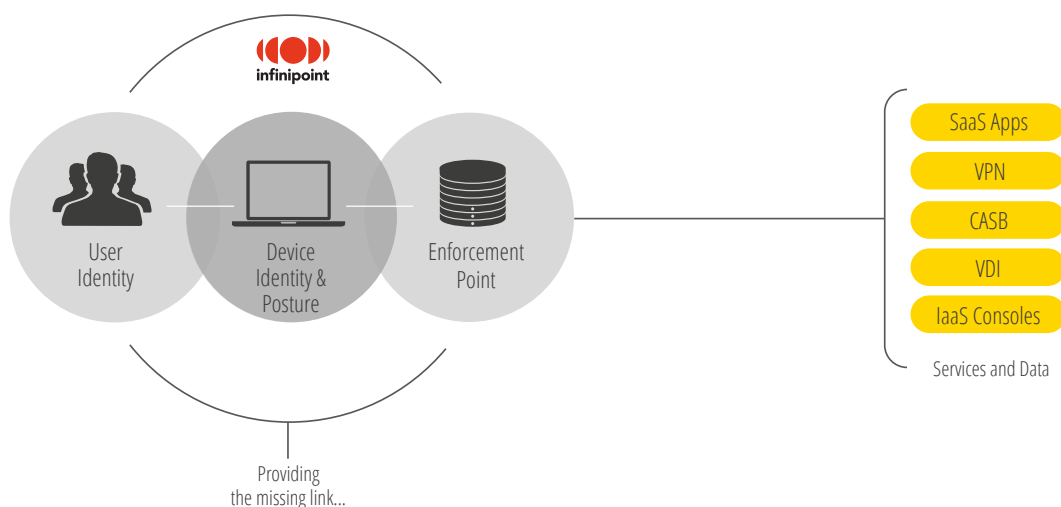
THE MISSING PIECE OF THE ZERO TRUST SECURITY MODEL PUZZLE

DlaaS is a comprehensive device identity and posture solution that integrates seamlessly with single sign-on authentication and acts as a central enforcement point for all enterprise services. It enables controlled access based on user, device and service and applies risk information to enforce static and dynamic access policies. The cloud-based service provides you with the necessary information on the status of your end devices and remediation options in a single interface.

The solution provides the missing piece of the puzzle of the zero trust security model as defined by Gartner, NIST and Google as best practice: the integrity of the device. The service provides you with high security added value by protecting access to your company's data and services and at the same time putting your end devices in a first-class secure state to prevent security breaches:

Introduces a risk-driven access process within the organization by detecting, managing and remediating threats in real time

Improves efficiency by optimizing security management through processes and automation, including one-click remediation for end users



DTS MANAGED SERVICES

Operating IT security solutions yourself always involves additional resources. As DTS, we support you across the entire scope of IT security. We provide you with the solution from our certified German data centers and take care of installation, 24/7 operation, updates, maintenance and support. Our experts reduce your workload to a minimum. Of course, we will work with you to customize the optimal deployment. Benefit from the unique combination of state-of-the-art IT security solutions and DTS managed services.