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 loopholes, malware and configuration errors. In order to protect your company and cloud infrastructure, it is essential to be able to assess the current security status of your company assets so that you can maintain proper cyber hygiene and enforce compliance standards - for any asset, anywhere on the network, at any time.

Most solutions provide only partial insight, are inaccurate, do not operate in real time and cannot handle the increased asset volume of employees working remotely. As users access your business applications and data through VPNs, Zero-Trust Network Access (ZTNA) and identity providers, even the strongest user identity authentication is not enough on its own. A comprehensive review of the security status of the endpoint is also required to ensure that the connecting endpoint has the proper level of security. Device Identity as a Service (DIaaS), based on the solution from our strategic partner Infinipoint, provides this missing piece of the zero trust security model: The integrity of the device as a link between the user identity and the application.

- Continuous assessment of the device security status
- Unified SSO technology
- Access security integrated with IT security asset management
- Static & dynamic policies based on real risks
- Self-service portal for end users
- Admin console for real-time visibility & control
- One-click remediation

Infinipoint's next generation asset management platform recognizes all assets and allows you to review 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, workloads, IoT devices and software components than ever before. At the same time, the risk status of each asset changes depending on where, when and by whom it is being 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, no matter where they are located: on & off-premises, in branch offices or with employees working from home.

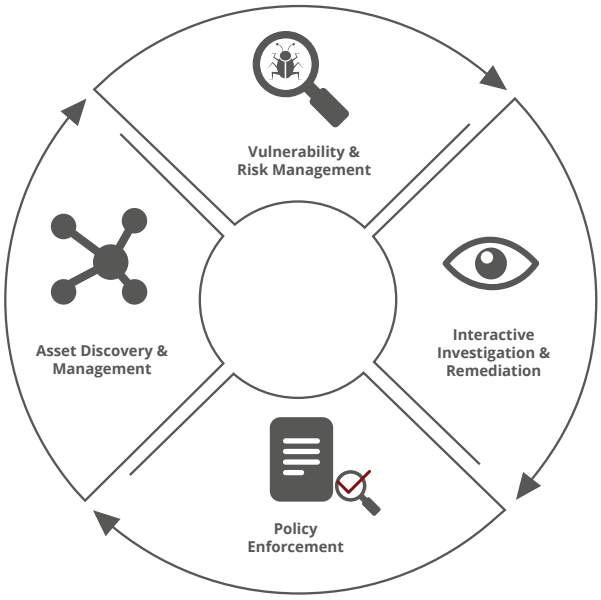
Interactive asset management
Infinipoint provides an end-to-end process for managing assets and improving their security status in dynamic IT environments.

Asset discovery & management
Continuous, real-time discovery and management of all assets captures traditional endpoints, VMs, IoT devices and cloud workloads, both inside and outside the company network. This happens very precisely even in complex, fast-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, such as user access, operating system configurations, hardening, hardware & removable media and unused software.

Interactive investigation & remediation
All assets can be checked easily to make real-time changes and evaluate the associated impact. Fix problems by patch or configuration, incrementally or all at once. Validate remedies and fix issues immediately.

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

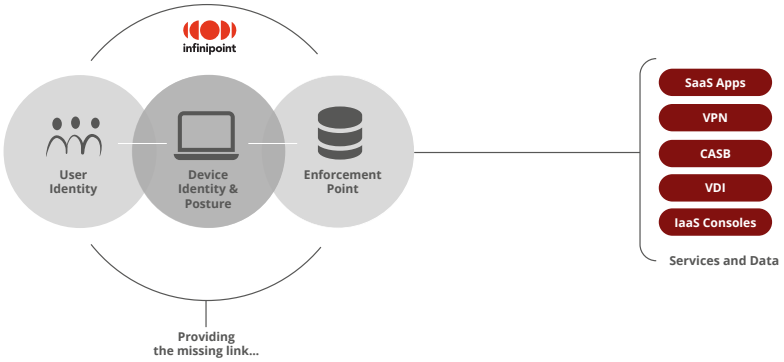


The missing piece of the puzzle in the zero-trust security model

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

The solution provides the missing piece of the puzzle in the zero-trust security model as specified by Gartner, NIST and Google as best practice: the integrity of the device. The service delivers high security value by protecting access to your organization's data and services while putting your endpoints in a first-class, secure state to prevent security breaches:

- Implement a risk-managed access process within your organization by detecting, managing and resolving threats in real time
- Improves efficiency by streamlining security management through processes and automation, including one-click remediation for end users



DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de