infinipoint netskope

Infinipoint for Netskope

Applying Device Identity to Zero Trust Access Verification

Solution Brief

Infinipoint Device-Identity-as-a-Service (DIaaS) works with Netskope to deliver a comprehensive security solution for Zero Trust device access. Infinipoint complements Netskope by integrating device state, risk-based policies, and one-click remediation for non-compliant devices. Verify device security posture, extend adaptive access, and enable auto-remediation as part of user authentication.

The Challenge

The increase in remote workers coupled with an increase in cyber attacks has elevated urgency around a Zero Trust security approach for secure device access. Zero Trust reference architectures from U.S. DOD, NIST and others are prioritizing more granular security controls for user devices to protect critical data and services.

With users accessing IT resources via new access solutions such as Zero Trust Network Access (ZTNA) and Secure Access Service Edge (SASE) even the strongest user authentication is insufficient on its own. A comprehensive device security posture is now required to ensure devices connecting to IT services have the right level of security and have been verified as compliant with security policy. This includes context-aware policies that can identify devices that are compromised, have known vulnerabilities, or are not managed by the enterprise.

Infinipoint for Netskope

Infinipoint ensures endpoint devices are secure and continuously compliant when connecting to services via Netskope. Infinipoint performs a device identity and security posture check as part of the Netskope user access flow. This includes validating the Netskope device classification by identifying endpoints where the Netskope client is not installed.

Infinipoint extends Netskope adaptive access controls, enabling conditional, granular policies for access based on device identity policies, for example, providing full cloud resource access to compliant and read-only access to cloud services and data for non-compliant devices. Device identity policies managed by Infinipoint are based on rich context such as critical vulnerabilities, OS firewall settings, browser extensions, certificates, installed software, and more.

Infinipoint also enables 1-click remediation for unmanaged and non-compliant devices, including installation of the Netskope client. The result is an adaptive Zero Trust approach to device access while maintaining business continuity with no disruption to the workforce.

Benefits

Together, Infinipoint and Netskope enable you to:

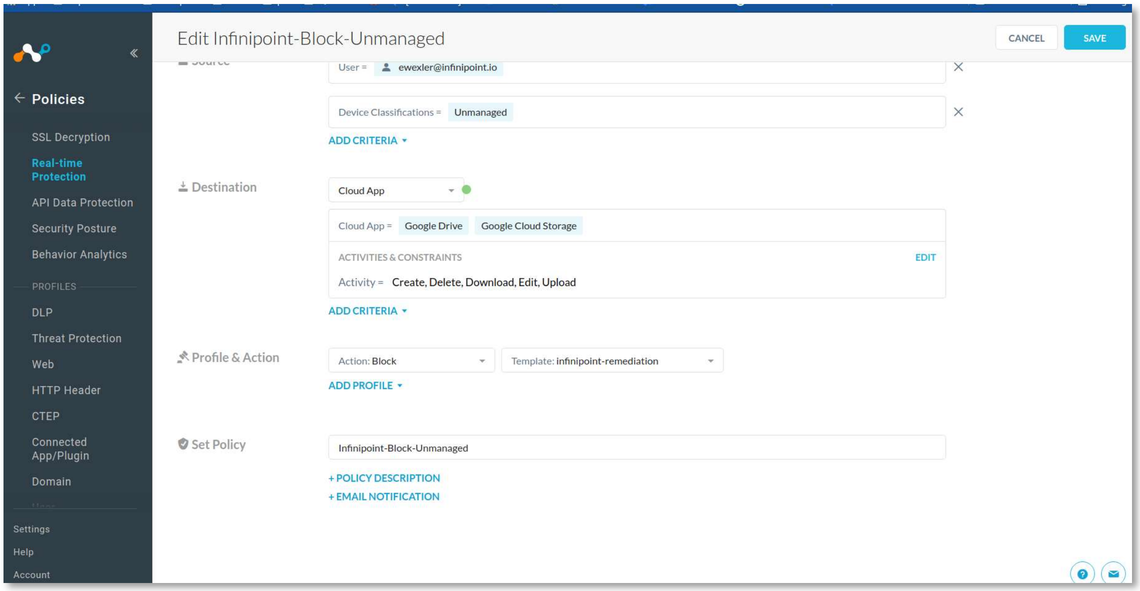
- Enforce a true Zero Trust user and device access policy
- Control access to sensitive data and applications for non-compliant devices
- Enable continuous adaptive access control based on granular device context
- Automate remediation for non-compliant devices

Integration Features

Device identity compliance check based on rich context

Adaptive access control for compliant and non-compliant devices

1-click remediation for unmanaged Netskope devices



Edit Infinipoint-Block-Unmanaged

User = ewexler@infinipoint.io

Device Classifications = Unmanaged

Destination

Cloud App

Cloud App = Google Drive Google Cloud Storage

ACTIVITIES & CONSTRAINTS

Activity = Create, Delete, Download, Edit, Upload

Profile & Action

Action: Block

Template: infinipoint-remediation

Set Policy

Infinipoint-Block-Unmanaged

Infinipoint integration with Netskope includes controls such as reducing cloud access for unmanaged devices where a Netskope agent is not installed.

Use Cases

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.

Adaptive Access -- Govern access permissions based on device context. For example, allow access but prevent files from being downloaded or restrict access to specific assets for non-compliant devices.

Auto-Remediation -- Easily bring user devices to a secure, compliant state by enabling self-service remediation. For example, enable 1-click installation of Netskope client for unmanaged devices.

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.

About Netskope

Netskope, the SASE leader, safely and quickly connects users directly to the internet, any application, and their infrastructure from any device, on or off the network. With CASB, SWG, and ZTNA built natively in a single platform, the Netskope Security Cloud provides the most granular context, via patented technology, to enable conditional access and user awareness while enforcing zero trust principles across data protection and threat prevention everywhere.