Solution Brief

netskope + CEQUENCE

Netskope customers now have access to Cequence Security's unique API-based threat intelligence. Cequence utilizes advanced artificial intelligence and machine learning to identify malicious actors across the globe, providing key security insights gained from evolving threats and attacks to ensure you have up-to-date protection for your mission-critical APIs and applications.

Quick Glance

- Greater visibility into threats with Cequence's real-world threat intelligence to block malicious IPs within Netskope
- Cequence's threat intelligence data is derived from anonymized, real-world attack data against customer production environments
- Integrates easily to get up and running quickly

> Over two years, Cequence reduced malicious traffic by 98% on our network, and shut down arbitrage markets scraping and reselling our inventory.
>
> Cequence Online Retail Industry Customer

The Challenge

Organizations need visibility and control over their API footprint as part of a robust security program. The rapid proliferation of APIs has exposed a broad range of security challenges that can lead to data loss, compliance violations, and fraud.

Digital transformation has induced extensive infrastructure changes throughout organizations. The proliferation of cloud environments and the deconstruction of monolithic web and mobile applications into microservices through APIs have created incredible infrastructure flexibility, but also changed and increased organizations' attack surface. Organizations need solutions designed to protect that attack surface as well as intelligence about attacks and where they are coming from. Bad actors are increasingly sophisticated and often use bulletproof proxies or launch their attacks from massive, rotating stables of residential IPs, so it is critical to have current data about the sources of attacks.

The Solution

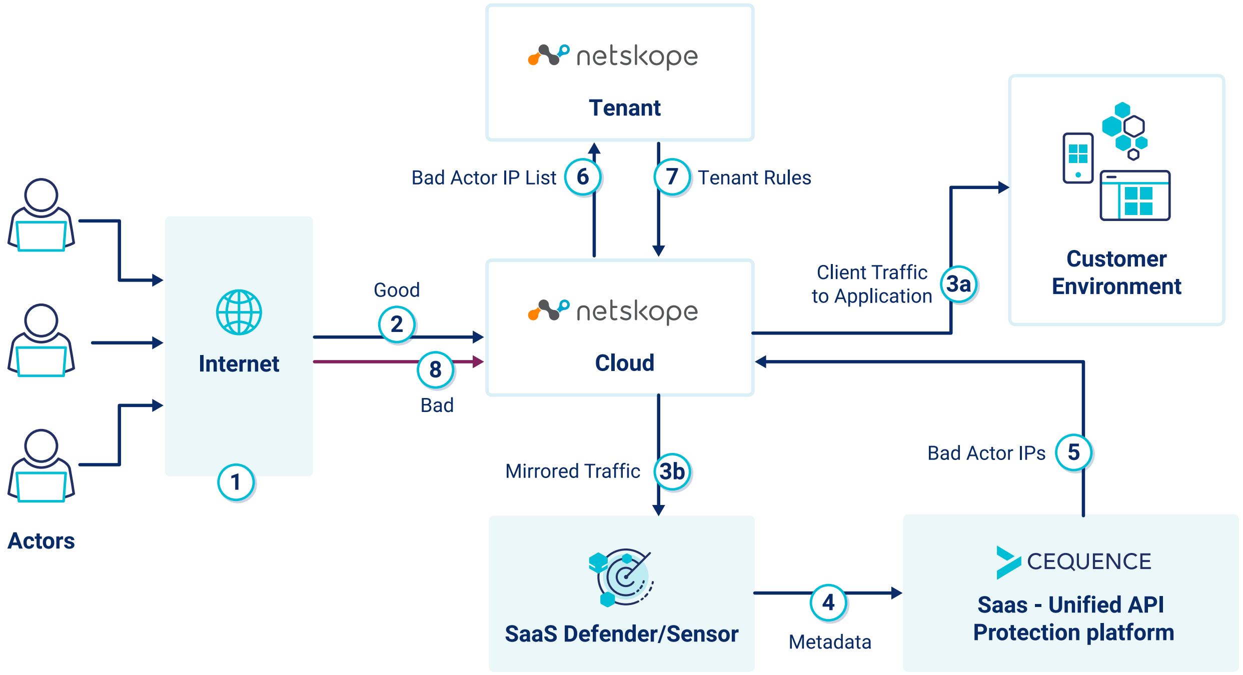
Cequence Security's unique threat intelligence integrated with Netskope enables customers to block known malicious IP addresses. Cequence's threat intelligence data is gathered from its own customer production environments – it's anonymized, real-world attack data that is both current and highly accurate. This ensures that Netskope customers can block IPs from which known attacks are originating.

Visibility and Control over API Footprint

Cequence uses multi-dimensional machine learning (ML) techniques to analyze and fingerprint good and bad traffic based on their behavioral traits. Cequence also identifies proxy IP addresses known to harbor malicious activities and incorporates other IP reputation information. This approach enables Cequence to accurately discern good traffic from bad traffic and identify attacks originating from multiple IPs. The data is shared through the integration with Netskope for the customer to take action.

Cequence Security's unique real-world threat intelligence enables accurate IP-based blocking of malicious traffic with Netskope.

An architectural overview of the Cequence and Netskope integration from initial user traffic to the Netskope customer environment with Cequence assessing risk and identifying bad actor IP addresses and returned to Netskope for appropriate action.



1. Clients send traffic through the internet
2. Traffic hits the Netskope architecture (first time)

3.a Traffic is sent to the Customer Environment/Application backend

3.b Traffic is mirrored to Cequence SaaS Defender/Sensor

4. Cequence Sensor sends metadata to Cequence SaaS Unified API Protection platform
5. Cequence sends Bad Actor IPs to Netskope
6. Netskope Sends Bad Actor IP lists to individual tenants based on their specific traffic
7. Tenants use policies/rules to take actions on Bad Actor IPs
8. Bad Traffic is blocked at Netskope/good traffic is allowed (per tenant)

BENEFITS	DESCRIPTION
Improved blocking of known bad IPs	Cequence threat intelligence of malicious IPs is unique and highly accurate
Up and running quickly	Simple integration between Netskope and Cequence

About Cequence

Cequence, a pioneer in API security and bot management, is the only solution that delivers Unified API Protection (UAP), uniting discovery, compliance, and protection across all internal and external APIs to defend against attacks, targeted abuse, and fraud. Requiring less than 15 minutes to onboard an API without requiring any app instrumentation, SDK, or JavaScript integration, the flexible deployment model supports SaaS, on-premises, and hybrid installations. Cequence solutions scale to handle the most demanding Fortune and Global 2000 organizations, securing more than 8 billion daily API calls and protecting more than 3 billion user accounts. To learn more, visit www.cequence.ai.

netskope

Interested in learning more? Request a demo

Netskope, a global SASE leader, uses zero trust principles and AI/ML innovations to protect data and defend against cyber threats, optimizing both security and performance without compromise. Thousands of customers trust the Netskope One platform and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity. Learn more at netskope.com.