CASE STUDY


# Cloud Security Leader Netskope Trusts Tenable to Secure Its Own Modern Attack Surface

tenable

CASE STUDY

netskope

As Gupta points out, a unified solution with flexible reporting "makes my life easier by delivering custom dashboards for the different teams and making them accountable to remediate and validate their respective issues."

*Rahul Gupta, Senior Security Engineer, Netskope*

# NETSKOPE

Netskope has assembled a world-class team of security professionals, who grew to realize that successfully managing cyber risk in the company's dynamic, cloud native infrastructure requires more than just traditional vulnerability management tools. They also sought to better engage all facets of the organization in the risk management process. As Rahul Gupta, senior security engineer, says, "it is no longer enough to have a handful of diligent security and compliance professionals managing the organization's risk strategies and controls." The team needed to augment its expertise and existing technology with a new class of services that moves cyber risk management beyond legacy vulnerability management that serves just the InfoSec team, to strategic management of Cyber Exposure benefiting the broader organization.

Netskope is a cloud access security broker (CASB) vendor. As a CASB, Netskope leverages its patented Cloud XD technology to provide its clients "360-degree" cloud visibility and data protection on a global scale. Delivering a unified control point for all cloud service security architectures, Netskope has built a cloud native infrastructure, heavily leveraging DevOps processes. For Netskope's information security team, this means safeguarding both standard business IT infrastructure (servers, storage, desktops, laptops, networks) and cloud native technologies.

## GROWING FROM VULNERABILITY MANAGEMENT TO CYBER EXPOSURE

### Environment Before Implementing Tenable

When Netskope's information security team started looking to mature their vulnerability management (VM) practices, the team was up against the reality that "building and preserving a company's reputation has become a massive task in any industry, and a single breach can bring down the whole reputation and business," says Gupta. Netskope's information security team was following VM best practices including comprehensive scanning, patch management, and advanced detection technologies, but Gupta and his team still faced a significant challenge.

They needed to elevate cyber risk management to a higher level. As Gupta describes, the team's goal was to "embrace the business professional's knowledge of risk" and provide the metrics and control points to evaluate how vulnerabilities and threats impact their cyber risk. The team needed to expand cyber risk management to be a more holistic and inclusive process.

This challenge underscored the significant gap between what they required to manage cyber risk successfully and what their previous VM tools offered. For example, relying purely on active scanning technologies gave the information security team point-in-time snapshots, leaving substantial exposure for the cloud instances that spin-up and -down between scans. In today's cloud native development environment, assets are no longer just laptops, servers, and storage LUNs. They are often ephemeral, coming and going – continually.

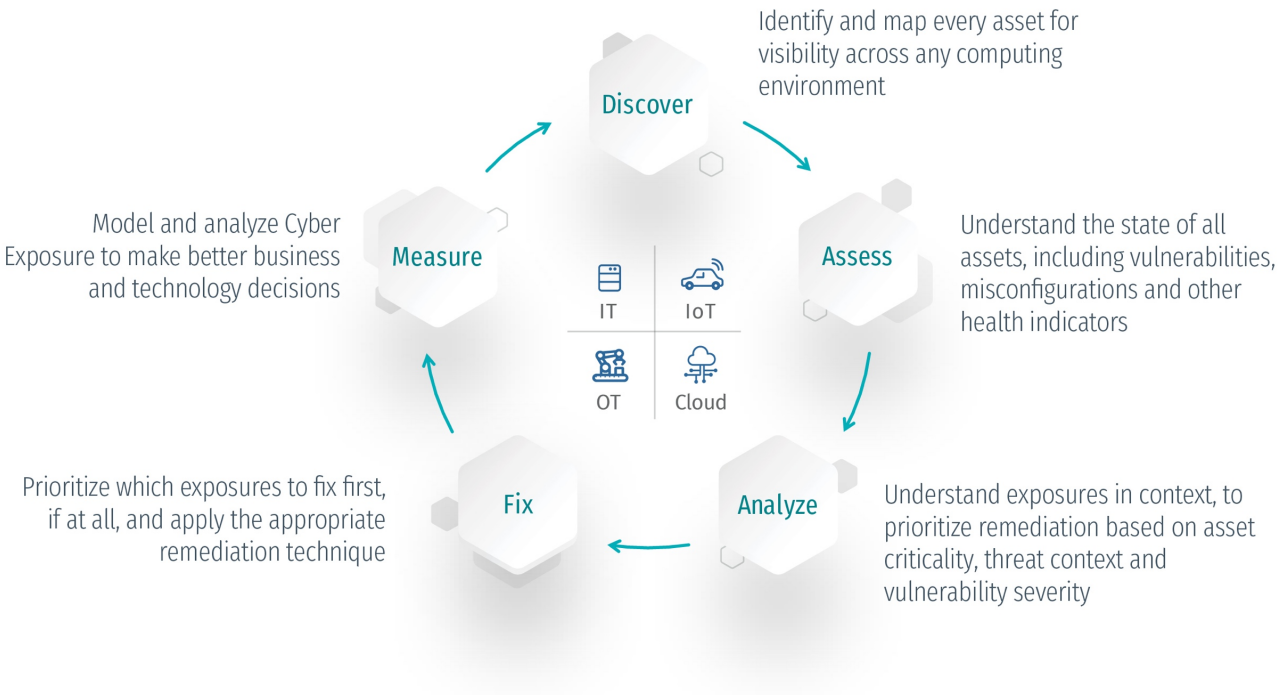
The team was also becoming overloaded with volumes of vulnerability data: data lacking the context and insight necessary to prioritize asset vulnerability, risk, and response, quickly. Although information security organizations often try to power through such volumes of data, Gupta and his team recognized this was a losing proposition. They didn't want to become so mired in data that they would not have the insights and perspective to make effective cyber risk management decisions.

## Raising the Bar from Vulnerability Management to Cyber Exposure

Netskope's team sought a new approach, shifting from traditional vulnerability management best practices and tools to a more modern and comprehensive plan. With their previous tools, Gupta and his team had faced continual challenges with vulnerability prioritization for remediation, given the diverse and dynamic asset portfolio Netskope maintains. They required a unified solution for tracking vulnerabilities and remediation – for assets communicating both north-south and east-west within their cloud infrastructure. They also required a means to provide actionable risk information in the context of the business, up and down the organization. As Gupta defines it, the team needed "360-degree protection for the whole vulnerability management lifecycle." To achieve this goal, they raised the bar on their VM practices and technology by moving from a legacy VM approach to a more comprehensive Cyber Exposure approach.

Their Cyber Exposure strategy now includes:

1. **Live discovery** of every Netskope asset, providing dynamic and holistic visibility across the modern attack surface (cloud, data center, IoT, etc.). This includes automating asset discovery, particularly assets in their cloud infrastructure, including containers. This live visibility now covers the entire software development lifecycle – spanning build, test, deploy and run. In a DevOps world, this typically includes embedding security controls into continuous integration/continuous deployment (CI/CD) systems.
2. **Continuous assessment** that indicates where – and when – an asset is secure or exposed. This assessment includes the state of all assets in the environment including vulnerabilities and misconfigurations.
3. **Prioritizing analysis and response**, based on enriching continuous vulnerability results with context. This approach includes putting assessment and discovery information in context to facilitate prioritization of exposures and the best remediation approach for each.
4. **Strategic decision support**, by using Cyber Exposure data as a critical risk metric that helps the organization define its security strategy and make key technology decisions.



## DEPLOYING TENABLE.IO AND SECURITYCENTER

Netskope deployed Tenable to continuously visualize and analyze the overall Cyber Exposure of the organization. A primary benefit of Tenable for Netskope is the advanced reporting capabilities, giving Gupta and his team the ability to more closely align security operations to business operations, bringing all functions of the Netskope organization into the Cyber Exposure lifecycle. Delivering these advanced reports helps Gupta enable all areas of the business to participate in decision-making to meet their risk posture goals.

Central to Netskope's Tenable deployment is Tenable.io, providing live information about vulnerabilities, malware, misconfigurations, and policy violations across its cloud native infrastructure. Netskope uses Tenable.io for its enterprise network to discover and monitor these issues, prioritize cyber risk decisions based on context, and enforce policy across its exceedingly dynamic IT environment.

Netskope also uses SecurityCenter from Tenable to monitor and protect the assets that comprise its customer-facing Netskope Security Cloud. Netskope's patented Cloud XD technology eliminates blind spots by going deeper than any other security provider to quickly target and control activities across thousands of cloud services and millions of websites.

Given a dynamic environment consisting of thousands of Linux and Windows assets, Gupta relies on Tenable to provide the "visibility across the environment necessary to confidently prioritize issues." To achieve this visibility, Gupta leverages the industry's broadest set of data collection capabilities, including active scanning, passive monitoring (Nessus Network Monitor), cloud connectors, and agents. As a result, the organization can see all vulnerabilities and prioritize remediation to address the most critical and highly exploitable vulnerabilities first.

## CONCLUSION – EMPOWERING THE SECURITY TEAM

Tenable empowers Netskope's security team to get out in front of risk by proactively managing comprehensive Cyber Exposure: east-west, north-south, and up and down the organization. By deploying SecurityCenter and Tenable.io, Netskope's information security team now has continuous monitoring and visibility into its entire product and IT infrastructure, providing confidence that it is actively managing risk at the speed of the company's DevOps environment.

An added benefit of Tenable.io is that the security team has gained the breathing room necessary to make informed decisions based on timely information about cyber risk, and thus manage its risk posture in line with Netskope's risk appetite. As Gupta points out, a unified solution with flexible reporting "makes my life easier by delivering custom dashboards for the different teams and making them accountable to remediate and validate their respective issues."

With the help of Tenable, Gupta and his team now see and manage their complete Cyber Exposure, directly enabling Netskope's mission of providing its clients with 360-degree cloud visibility and data protection.

**To learn more, visit: tenable.com and netskope.com | Contact Us: marketing@tenable.com**