Nanitor

WHITEPAPER

Active scanning versus passive discovery

In our view the real-time and continuous monitoring capabilities of the agent-based approach is crucial in today's fast paced cybersecurity environment. Swift detection of vulnerabilities and misconfigurations enable companies to quickly act on and mitigate threats before they are exploited. The Nanitor agent functions beyond potential network restrictions that ensures full and comprehensive coverage of the customers assets. Although there is a minor overhead to deploying/running an agent-based system the benefits of the swift feedback and in-depth analysis outweighs that overhead drastically.

Introduction

In the realm of modern cybersecurity, the Nanitor System stands out. It comprises of three key components:

01. The Nanitor Agent

02. The Nanitor Collector

03. The Nanitor Server, responsible for processing data gathered by the NDE

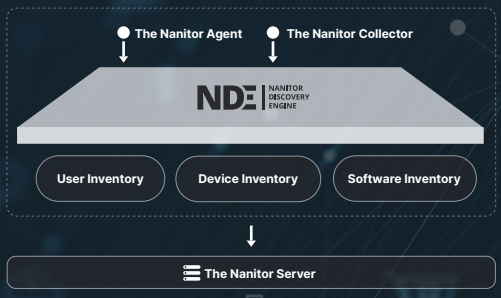
Nanitor's mission is to support small to medium size businesses (SMB's) with an enterprise grade Exposure Management solution, finding security and vulnerability issues within IT system, prioritizing these and reporting. Nanitor achieves these goals while placing minimal strain on IT Teams, network and system resources.

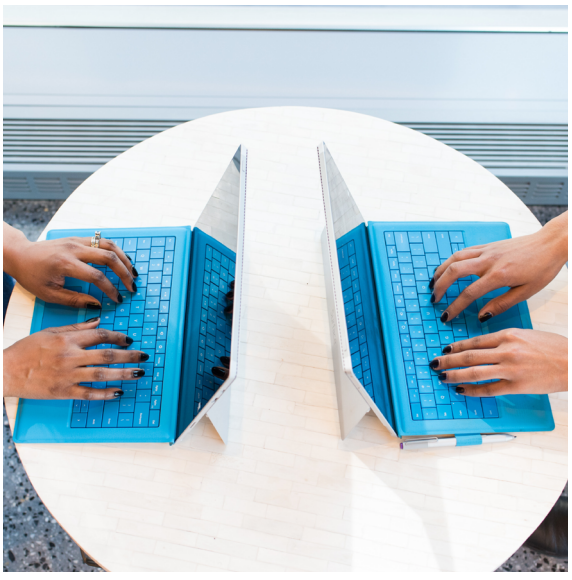
Guided by this philosophy, Nanitor exclusively employs passive discovery, or agent assessment. It deliberately avoids active network scanning due to its resource-intensive nature and potential risks for certain systems.

This discussion delves into a comparison of these two approaches, highlighting Nanitor's innovative role in the complex landscape of cybersecurity.

Our core technology: The Nanitor Discovery Engine™ (NDE)

The Nanitor Discovery Engine™ collects real-time asset information, including system details, user accounts, configurations, patch status, vulnerabilities, and software.





Active Scanning

This approach involves establishing connections to various IP addresses within your network environment. These IP addresses aren't necessarily the ones currently in use, as we can't accurately determine that. Instead, we target IP addresses that have been configured and designated for potential use. Depending on your organization's size and network configuration, this range can span from thousands to over 16 million IP addresses.

The active scanning method operates by checking if any of these potential IP addresses are hosting active services. These services encompass functions like Database, Web, File sharing, or even remote management services. This also encompasses a service called ICMP, which simply responds to queries like "Are you there?" through tools like ping.

To ensure thoroughness, you might choose to test a range of services, varying from a few dozen to a few thousand. However, given the immense number of possible service connections (65,536 ports), most efforts focus on the top few thousand ports.

Active Scanning

Sigurður Gísli Bjarnason
Cybersecurity Technical Specialist

Now, let's illustrate a scalability challenge with some calculations, using certain assumptions:

- *Consider a reasonably sized network with an 18-bit mask, offering 16,382 potential IP addresses*
- *To be moderately comprehensive, you decide to test for five hundred services, including ICMP*
- *This requires 8,191,000 connection attempts*
- *Assuming each connection takes about 1 second on average (factoring in successful and failed attempts)*
- *Conducting one connection attempt at a time would take over 94 days to complete*

You can reduce this time by attempting multiple connections concurrently. For instance, with twenty simultaneous connections, you could finish in 4-5 days. Even with an ambitious scenario of 100 simultaneous connections, the process would still take about 23 hours.

This timeframe scales linearly, so doubling the network's size would double the time needed.

Upon completing this effort, you'll have a record of IP addresses and the services that responded on each one. This data enables educated guesses about the corresponding IP and service. However, such estimates are around 80% accurate. The subsequent challenge lies in determining the identity, location, ownership, etc., of these IP addresses, which can pose considerable difficulties for many organizations and even be insurmountable in some cases.

Active scanning disadvantages

Despite the method's potential benefits, there are drawbacks:

- Configuration and management of these scans require time and effort, which grows with network size
- Certain devices are vulnerable to crashes when probed for non-existent services, revealing a Denial of Service (DoS) vulnerability
- Devices, even well-designed ones, must handle or block numerous invalid connection attempts, incurring a cost that is neither cost-free nor resource-light
- These connection attempts add extra load to your network, potentially posing capacity-related issues
- Secure workstations designed to communicate outwards without offering services won't respond to such connection attempts, remaining hidden from probing

An offensive DoS attack resembles an intensified active network scan, performed at an accelerated pace.

After expending considerable effort and assuming associated risks, achieving 100% assurance of complete discovery remains elusive, this method averages about 90% completeness. This is the approach both Qualys VMDR and all Tenable products employ during their standard discovery phase.

Passive Discovery

Nanitor adopts this approach and uses various methods to uncover network information. To understand this, let's take a quick look at networking basics for a moment.

All devices connected via network cables link up to something called a network switch. If you're using a wireless connection, you're connecting through an access point that's linked to a network switch. All these switches are connected through a device called a router. This router, in turn, connects to other routers, enabling access to internal company services and the broader internet.

For these switches and routers to facilitate communication between computers and the internet, they maintain something called a connection table. This table keeps track of who's communicating with whom and the specific port they're using. Think of it as a directory in a university that tells you where to find the biology department – in this case, it's in room 404 of the science building on the fourth floor, third corridor, fourth door.

The passive discovery method essentially involves requesting these connection tables from routers and switches and then piecing the information together. The agent also monitors whom it's communicating with, relaying this data to the NDE. The system then cross-references this with other data to identify unfamiliar devices, their locations, etc. It can even create a report about potentially unauthorized devices, which is called a rogue asset report, to alert the user.

Sigurður Gísli Bjarnason
Cybersecurity Technical Specialist

Passive discovery disadvantages

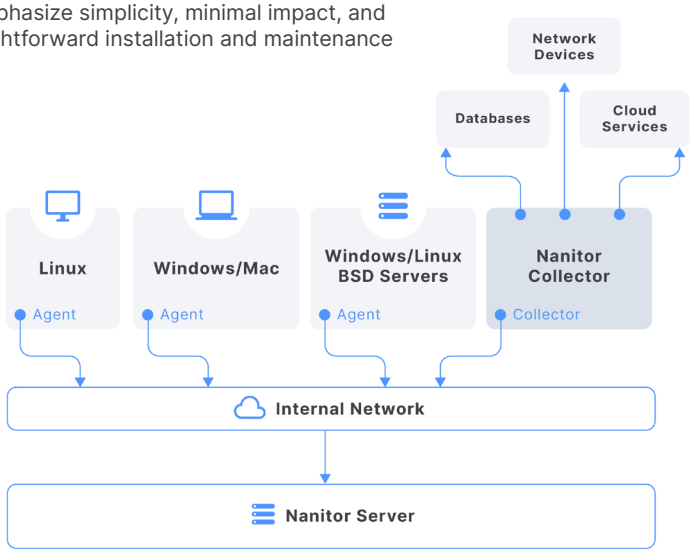
However, there are drawbacks to this method:

- You need a comprehensive list of all the network devices in your setup. Missing even one could lead to it being flagged as a rogue system.
- Convincing the network team to share their roster of network devices is necessary.
- Gaining permission from the network team to connect to their devices and access the connection table is essential.

Care and feeding

Nanitor guiding design principles emphasize simplicity, minimal impact, and user-friendliness, resulting in a straightforward installation and maintenance process.

Conceptual Diagram



Deploying the Nanitor SaaS System involves installing the Nanitor Agent and configuring the Nanitor Collector. Here's the breakdown:

Nanitor Agent Deployment:

- Installing the Nanitor Agent is akin to any other software in your organization
- It's a matter of running an application installer
- Applying a license key to the application
- For most organizations, distributing this is effortless through software distribution or remote management solutions like Microsoft Intune, Puppet, Chef, Ansible, Automate, etc

Nightly Updates:

- Each night, both the agent and the collector download information about the latest vulnerabilities
- If an updated version is available, the agents and collectors detect it and upgrade themselves automatically

Daily Collection:

- The collector tests connectivity with each collected asset throughout the day
- However, actual data collection only happens once a day, during the night
- Users can manually initiate collection if required

Agent Monitoring:

- The agent continually monitors the asset and sends reports whenever changes occur
- It also contacts the NDE every five minutes, serving as a health check and update trigger

Nanitor Collector Configuration:

If you wish to gather and analyze data from network devices, databases, or cloud services, you employ the Nanitor Collector. Given that these cannot host an agent, we utilize a collector to establish a targeted remote connection to their management interfaces for the required tasks. The setup involves these steps:

- Designating an agent as a collector in each network segment, a simple process via the system's main UI
- Providing credentials for the collector's remote connections
- Specifying connection details for each asset or service you want to collect from, along with the designated collector for each

For an on-prem Nanitor system, the setup additionally involves creating and maintaining the Nanitor server, treating it much like any other server in your environment.

The ongoing system maintenance requires minimal effort; you primarily add new systems as they come online. The rest is automated.

Heartbeat Mechanism:

The collector maintains a connection with the asset via a heartbeat mechanism, regularly checking in to report its status and inquire about updates

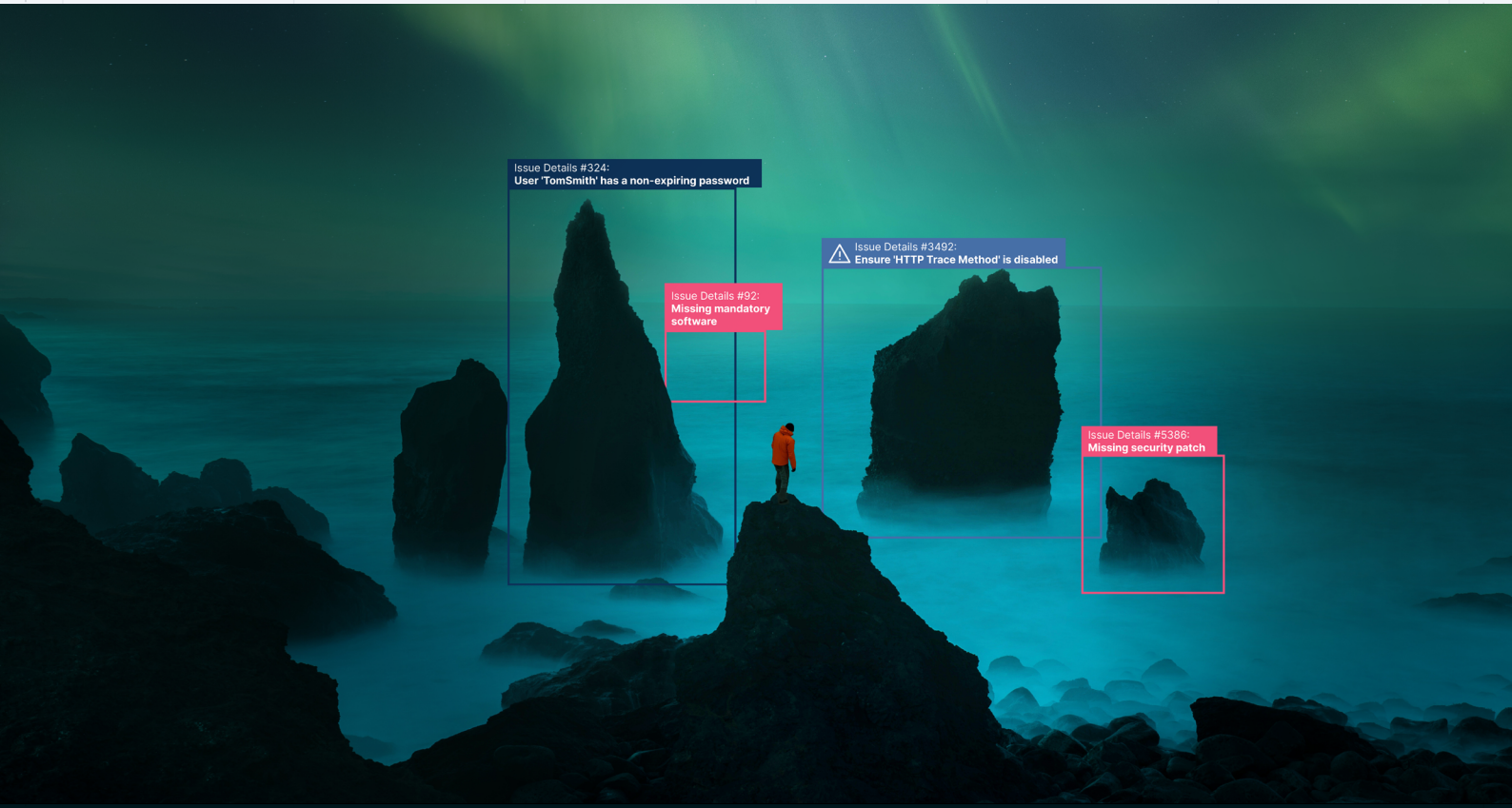
Agent-Initiated Communication:

- For security reasons, the NDE cannot initiate connections to agents
- It waits to receive communication from an agent before providing instructions, like notifying agents about new vulnerability definitions available for download

Summary

Nanitor offers a convenient solution to monitor your assets and their vulnerabilities, ensuring streamlined management without sacrificing visibility. It's an excellent fit for organizations seeking a straightforward approach to vulnerability tracking, especially Small and Medium Businesses (SMBs) without extensive in-house cybersecurity knowledge.

Sigurður Gísli Bjarnason
Cybersecurity Technical Specialist



Want to learn more about the Nanitor platform?

Nanitor is a powerful cybersecurity management platform focusing on hardening security fundamentals across your global IT infrastructure. The platform provides unique visibility and control of your security challenges that stakeholders can trust, at a fraction of the cost and time of alternatives.

Nanitor

Sales locations

Sudurlandsbraut 6, 7th floor
108 Reykjavik, Iceland

100 Bishopsgate, 18th floor
EC2N 4AG London, UK

North Andover, 01845,
Massachusetts, USA

Visit our website
www.nanitor.com

Get in touch with us
sales@nanitor.com