



# The Nagomi Proactive Defense Platform

The Nagomi Proactive Defense Platform lets customers see how threats map to their defenses, and provides prescriptive remediation plans to decrease risk, improve defensive posture, and show tangible progress.



Maximize Security Coverage



Understand Exposure



Iteratively Optimize

## Objectively balance risk and defense.

### Blind to Tool Coverage and Effectiveness

Security teams often lack the confidence that their existing security tools are providing the expected level of protection. This lack of confidence leads to uncertainty about the overall threat tolerance.

### “Are we protected?”

Security teams struggle to answer critical questions about how well they are protected against specific threat scenarios, like phishing and ransomware. This leaves organizations vulnerable and unable to allocate resources effectively.

### Overloaded with manual tasks

Responding to evolving threats requires significant manual work analyzing, investigating, and responding to evolving threats. This causes misconfigurations, errors and fatigue

### Difficulty communicating cyber risk

Security teams need to provide concise and informative answers to the board in order to achieve alignment across the organization and get things done.



The Nagomi solution

Nagomi identifies redundancies, eliminates overlaps, and streamlines security operations, optimizing tool performance and effectiveness and maximizing ROI on security investments.



The Nagomi solution

Nagomi helps assess the impact of a potential cybersecurity threat to an organization's overall threat tolerance by understanding the relationship between assets, exposures, privileges, and threats across an attack path. This allows security teams to prioritize “next steps” and make better decisions.



The Nagomi solution

Nagomi automates security tool management allowing security teams to streamline processes, automate tasks, regain valuable time and prevent preventable threats



The Nagomi solution

Nagomi uses plain language, connecting threats to business impacts making it easier for security teams to report coverage gaps to the board and assess the value of each to the business.

## How it works

### Visualize

Holistic, unified view of threat exposure

Nagomi takes a holistic view of your stack and provides a unified, threat-centric view of your threat posture employing the renowned MITRE ATT&CK framework. Across endpoints, identity, email, network and more, you'll have a comprehensive overview of where you are exposed to risk.

### Prioritize

Threat-centric prioritization and ROI optimization

Nagomi understands the relationships between assets, exposures, privileges, and threats across an attack path. With this information, organizations can optimize the return on their security investments and ensure a strategic and comprehensive defense against evolving cyber threats.

### Remediate

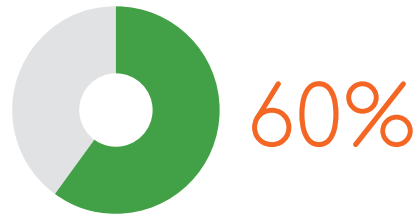
Actionable remediation recommendations

Nagomi stands out by offering actionable, step-by-step remediation recommendations, effectively streamlining processes and automating tasks. This not only enhances control effectiveness but also empowers security teams to reclaim valuable time, enabling them to focus on strategic aspects of cybersecurity and proactively address emerging threats.

### Communicate

Align all stakeholders on cybersecurity

Nagomi provides security executives and business leaders have a centralized and business-aligned view of cyber risk. It provides clear KPIs that show progress over time, benchmarking against external peers, and helping you effectively communicate cyber risk to stakeholders. This ensures that everyone in your organization is on the same page when it comes to cybersecurity.



Through 2028, more than 60% of security incidents will be traced to misconfigured security controls.

- Gartner.

## Why Nagomi?



Easy, 1-hour agentless onboarding



Read Only APIs



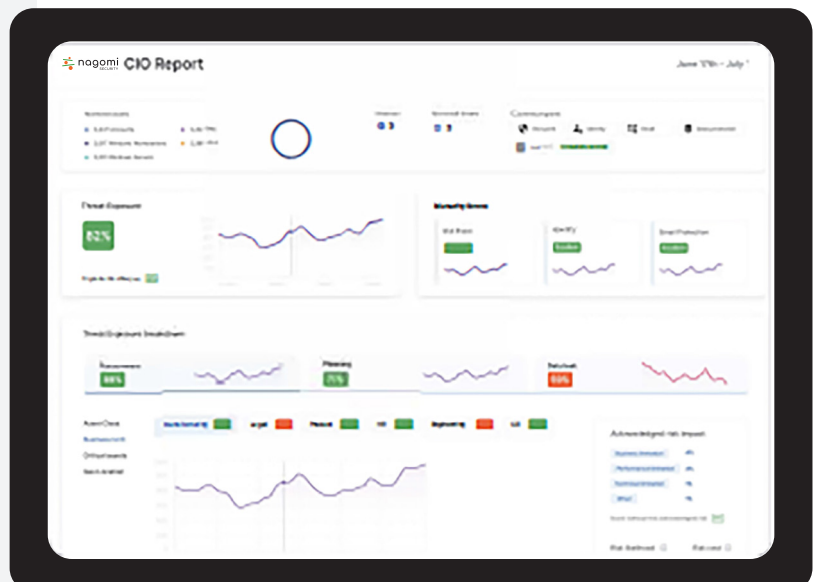
Threat assurance



Deep visibility into control effectiveness

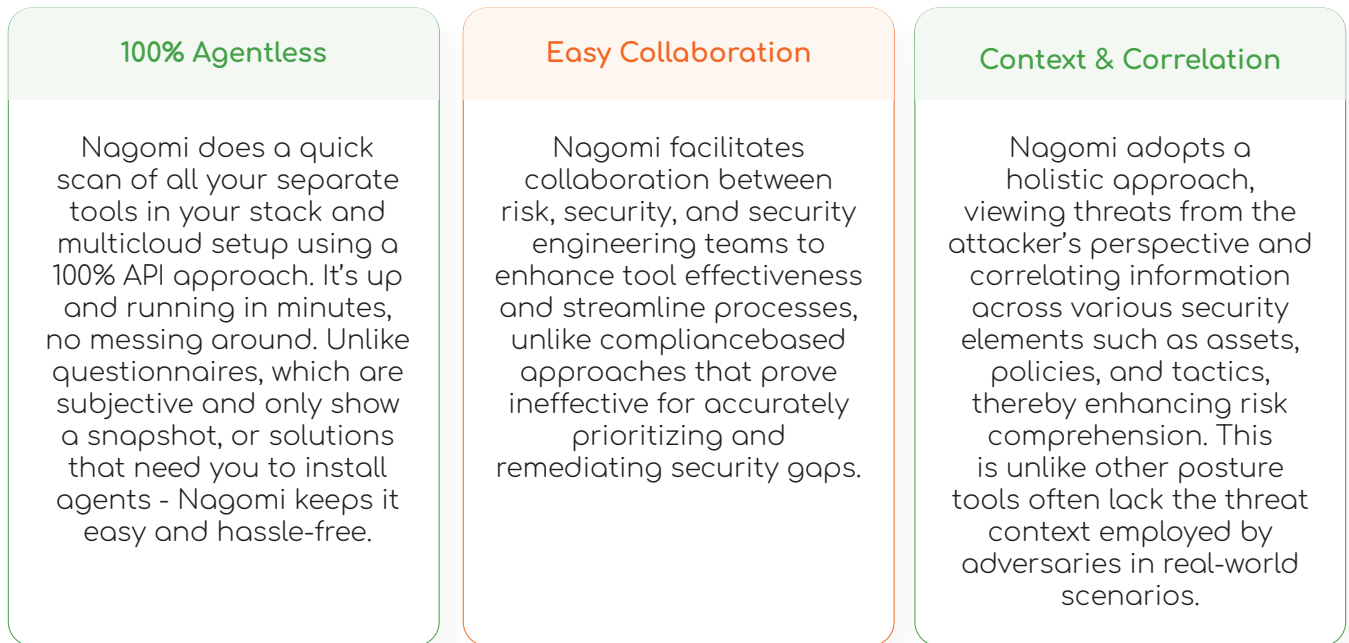


Improve your defensive posture against MITRE ATT&CK techniques

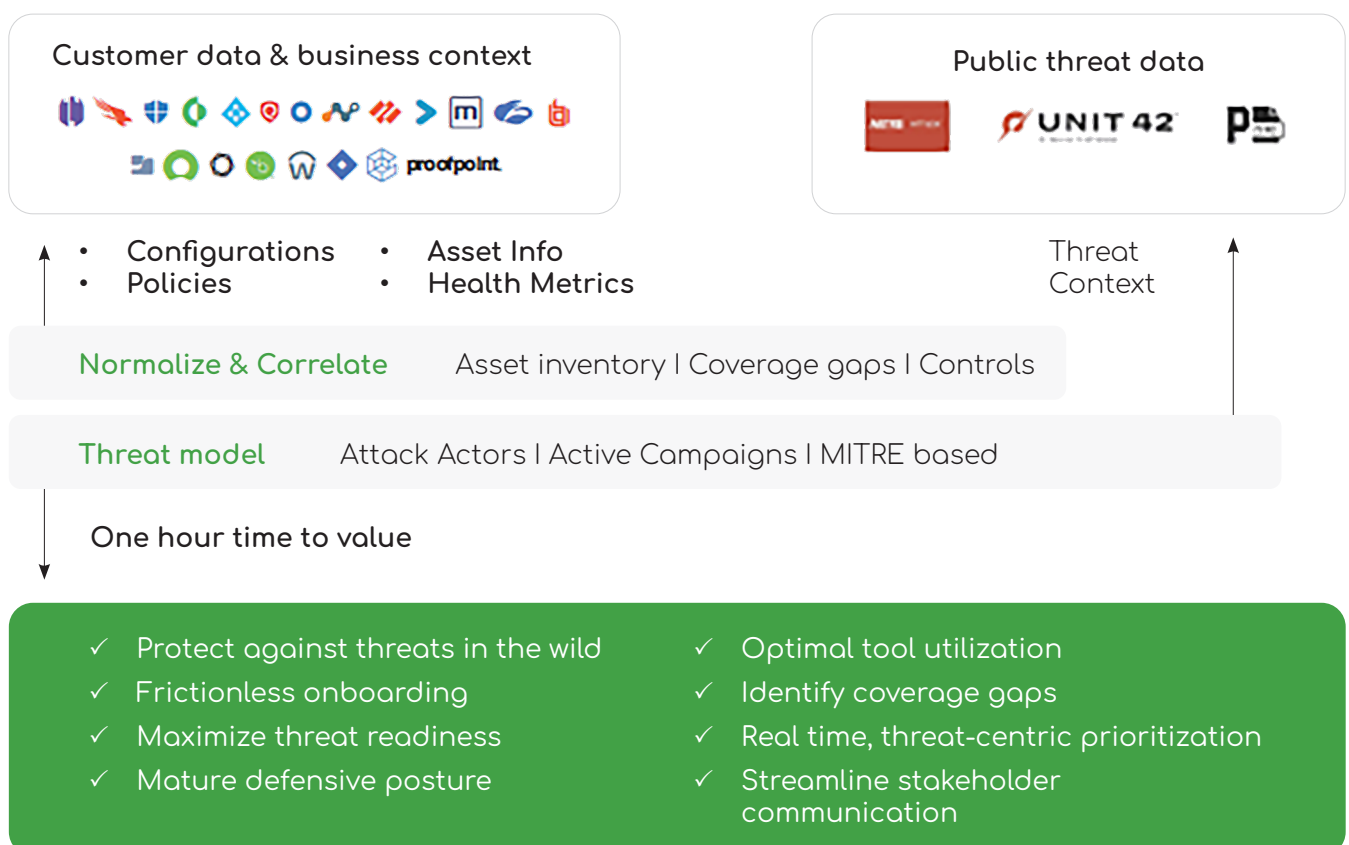


## What makes Nagomi different?

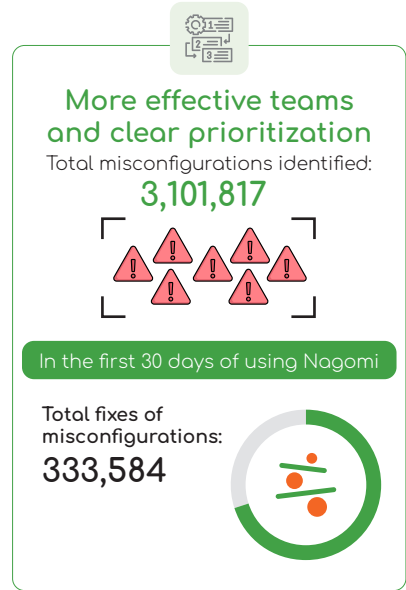
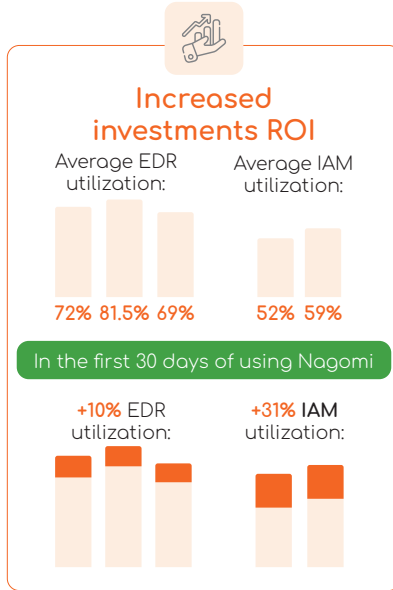
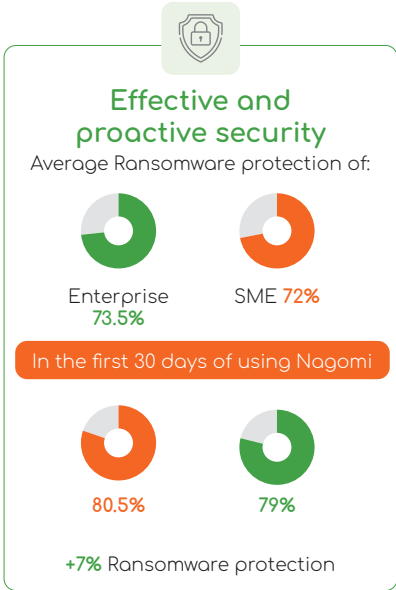
Nagomi Security helps organizations increase their cybersecurity maturity, optimize their defenses, be more proactive, and make the most of their technology investments. Armed with tangible measurement, prescriptive remediation plans, and threat context, security teams can confidently balance risk, defense, and make better business decisions.



## Where Nagomi fits in the security stack







## The Benefits



## Customer Case Study

Single platform to manage, monitor and assess security effectiveness

 Single platform to manage, monitor and assess security effectiveness

-  CISO
-  Chief Trust Officer
-  Executive Leadership
-  Board

Core Enterprise IT tools Connected

Acknowledged Exceptions

Custom Business Context (BU, Geo, Crown Jewels)



-  Security Operations
-  Program Directors
-  Risk Manager
-  Security Engineering

## Customer Details

25,000  
Employees

FORTUNE  
**500**

Manufacturing

## Last 90 days Results

<div style="background-color: #f44336; color: white; padding: 5px; border-radius: 5px; display: inline-block; margin-bottom: 5px;">01</div> CrowdStrike Utilization +9% improvement	<div style="background-color: #f44336; color: white; padding: 5px; border-radius: 5px; display: inline-block; margin-bottom: 5px;">02</div> 10% Reduction in Threat Exposure
<div style="background-color: #f44336; color: white; padding: 5px; border-radius: 5px; display: inline-block; margin-bottom: 5px;">03</div> Okta Utilization +10% improvement	<div style="background-color: #f44336; color: white; padding: 5px; border-radius: 5px; display: inline-block; margin-bottom: 5px;">04</div> +250k misconfigurations fixed



Honestly, because Nagomi is both data driven and actionable, it allows me to using one set of data -present the high level to my board to give them comfort and confidence, and then go back to my team and tell them here's exactly what we need to do to move the needle.

- IFF CISO