Proactive Security - Principled Aspiration or Marketing Buzzword?

A Critical Look at a "Viral" Cyber Term, What it Means, and What's Really Actionable and Valuable to Today's Security Professionals

By Nathan Burke

Photo by Zach Savinar on Unsplash

Overview

Whenever a new cybersecurity acronym or term starts gaining momentum, it is usually met with two distinct and opposite reactions: vendors jump on the bandwagon and claim it while security professionals try to decipher whether there's substance and value or just a new buzzword. In this presentation, we will attempt to take an objective and critical look at a term that is quickly becoming today's "zero trust".

nagomi SECURITY

Table of Contents

nagomi SECURITY

What is Proactive Security?

Let's look at a few definitions of Proactive Security from different sources before we create our own working definition:

> Omdia formally defines Proactive Security as technologies (including those provided as services) that enable organizations to seek out and mitigate likely threats and threat conditions before they pose a danger to the extended IT environment."
>
> Eric Parizo, Principal Analyst, Omdia[1]

> "A proactive approach is not controversial. But it is a misunderstood objective. Security programs have entire teams and programs dedicated to proactive approaches such as posture management. But proactive teams, like vulnerability risk management, and reactive teams, like the security operations center, remain overwhelmed.....
>
> If you're wondering how or if a given security technology supports your proactive program, ask yourself these four questions:
>
> 1. Does it give me visibility into what I have in my organization that needs to be protected?
> 2. Does it help me prioritize my remediations?
> 3. Does it help me orchestrate remediations?
>
> Does it help me report on my proactive program?
>
> If you or the sales rep cannot provide coherent answers and examples to answer these questions, then the solution is not part of a proactive security solution suite (and it could be vaporware or snake oil)."
>
> Erik Nost, Senior Analyst, Forrester[2]

[1] Proactive Security: What It Means for Enterprise Security Strategy - DarkReading - 9/26/23

[2] It's Time That We Activate Proactive Security - Forrester - 9/11/23

Though definitions vary, the basic conceptual underpinning is the same:

1. Despite the efforts of cybersecurity professionals, vendors, researchers, and public sector guidance, organizations have not decreased their vulnerability to cyber-attacks.

2. The conventional wisdom of "assuming breach" shifts the onus onto incident response teams and technologies aimed at minimizing breaches as they happen rather than maximizing defenses to prevent incidents from succeeding.

3. Though many - if not most - organizations have implemented tools in the most popular and recognized defensive categories, security practitioners spend more time reacting to incidents than ensuring that their existing tools are as effective as they can be against threats.

4. Cybersecurity maturity and progress require objective metrics. Until organizations can tangibly quantify risk, understand baseline maturity, and calculate the cost of improvement, they will struggle to understand their risk/reward ratios in terms of business-level strategy.

5. Context is required for proactive security. For too long, security teams have relied on vulnerability criticality scores for prioritization regardless of context. A critical vulnerability on a development machine on a sequestered segment is fundamentally different from an internet-facing server with customer data with a medium CVSS.

6. Proactive security focuses on making the most of what organizations already have. This includes optimizing security stack coverage and using publicly available frameworks like MITRE ATT&CK.

7. Technologies that enable proactive security should seek out misconfigurations and coverage gaps, compare them to threats and in-the-wild campaigns, and provide prescriptive remediation and mitigation plans before they can pose a danger.

8. Any proactive security program should be able to provide objective, contextual, and understandable metrics to chart progress, rationalize investment, and show ROI at the board level while simultaneously providing overburdened defenders with plans to get ahead.

How is Proactive Security Different from Other Approaches?

Photo by Juha Lakaniemi on Unsplash

At a very high level, we can think of the move to proactive security as an evolution that started with prevention and moved to detection/response.

	Prevention	Detection/Response	Proactive
Philosophy	Don't let anything known or expected penetrate the environment. Stop threats at the gates.	Assume breach and disrupt inevitable attacks before they create maximum damage.	Map threats to defenses, find and mitigate gaps, remediate threats from the inside.
Threat Lifecycle	Pre-exploit	Mid-attack	Continuous
Technologies	Signature-based (AV, NGFW, WAF)	Behavior-based (XDR, SOAR)	Threat-based (CTEM, CCM, ASM)

Each of these approaches have value and merit, and nothing replaces defense in depth. However, like color TV or remote car starters where it's cold.....it's hard to go back to dealing with only prevention and response when seeing that an additional option can add significant value (while removing manual work).

nagomi SECURITY

What Belongs Under the Proactive Security Umbrella?

In contrast to preventive and reactive/detection solutions that are focused solely on known and active threats, proactive security solutions add the dimension of understanding potential threat conditions that *could be* used in attacks. This is an important distinction with a real difference.

nagomi SECURITY

Hypothetical Example: The Casino

Scenario 1
Imagine you've been hired by a Las Vegas casino as a DFIR expert. The security team from the casino *knows* they're under attack, but the attackers are **great** at covering their tracks. Your job: find out where the attackers came in, the attack vector, what systems they had and still have access to, and what has been exfiltrated or compromised.

1. What would you need to answer those questions?
2. How confident would you be that - given access to any system and tool - you could answer questions about the type, impact, scope, and remediation plan for the attack?

Scenario 2
Imagine you've been hired by the same casino, but this time as a Cyber Risk and Defense Optimization expert tasked with identifying where attackers *might* get in.

Given this assignment, you would need more context than access. Just the word "might" implies probability, and leads to questions like:

1. What are the most critical/valuable assets that would be most attractive to attackers?
2. What defense capabilities are monitoring these assets?
3. Are these assets segmented?
4. How are they updated?
5. Who has access?
6. What known vulnerabilities are present? Are there patches/updates available? Are some of these systems EOL?
7. Is there an attack path from non-critical to critical assets?
8. What can I do with the security tools that are already implemented to reduce risk and optimize controls?

Instead of looking at this as a value judgment (which is more difficult?), this thought experiment shows the difference between uncovering facts and using data and context to provide an optimal and effective defense plan.

The following are examples of technologies that could be part of the proactive security umbrella.

Attack Surface Management

Whether looking at External Attack Surface Management (EASM) or Cyber Asset Attack Surface Management (CAASM), the two categories in concert can show both an outside-in and inside-out view of an organization's asset environment, identifying known vulnerabilities, providing asset inventories, and scoring risk.

Risk-based Vulnerability Management

RBVM or Vulnerability Prioritization tools are meant to add context to the broad-based CVSS scoring to help teams more effectively inform patch management. Faced with more vulnerabilities than people and tools to quickly remediate, adding a layer of threat-informed context is a valuable tool to decrease risk - especially given long patch timelines.

Posture Management

Posture Management tools including SaaS Security Posture Management (SSPM), Cloud Security Posture Management (CSPM), Application Security Posture Management (ASPM) and Data Security Posture Management (DSPM) are all based on discovery, assessment, and remediation within their specific domains, especially as related to configuration management, data flows, classification, and categorization.

Breach and Attack Simulation, Validation, and Testing

BAS tools and other automated testing solutions simulate probable attack paths given the actual conditions, defenses, and configuration details of an environment to understand the scope of an attack. Based on the results of a simulation, they can give remediation recommendations.

What is the Value and Impact of Proactive Security?

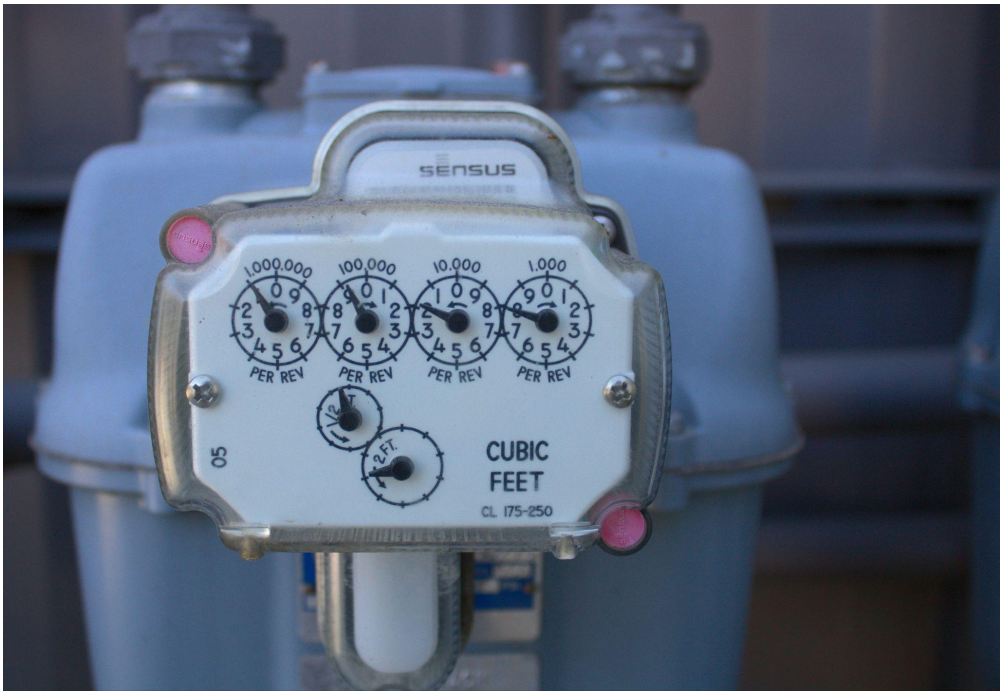


Photo by Doris Morgan on Unsplash

There are several quantifiable as well as soft benefits resulting from implementing proactive security measures. We'll focus on three here:

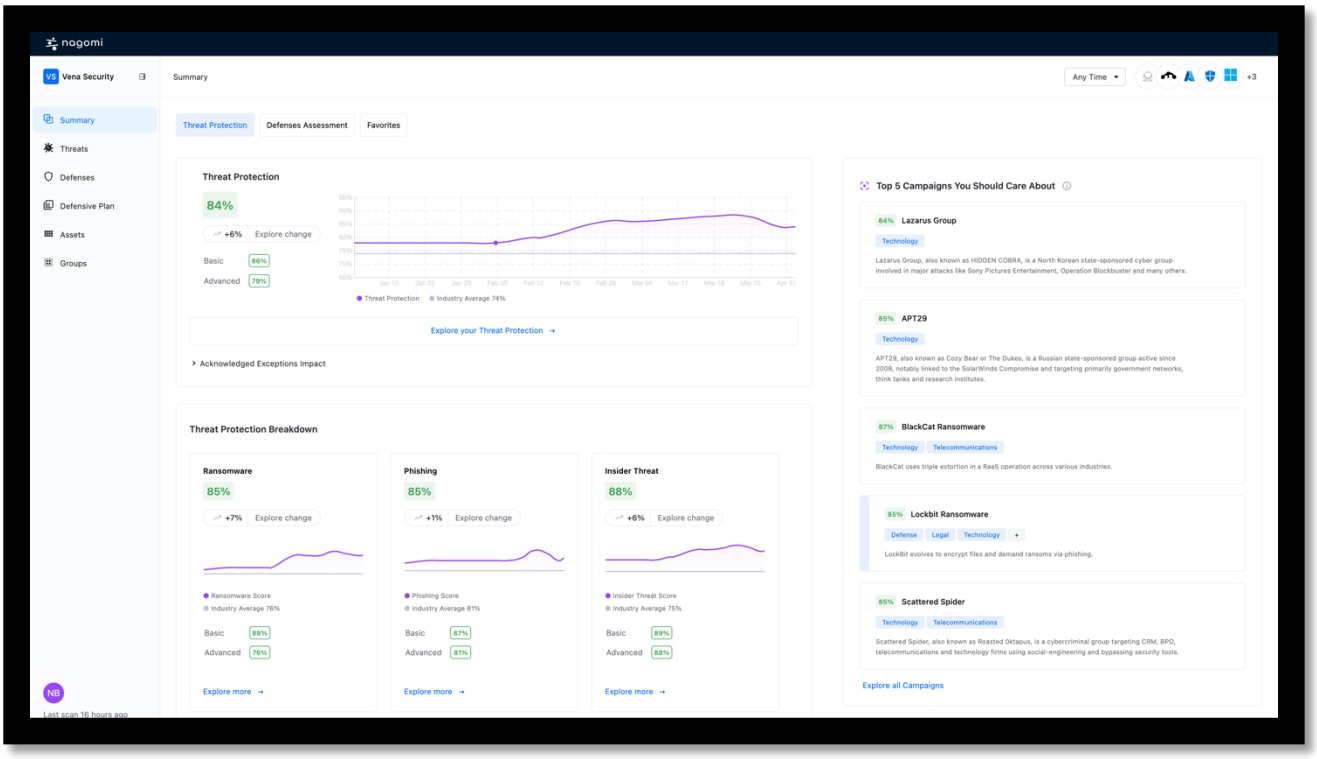
1. **Increased Security Investment ROI** - With most security teams already having preventive and response tools implemented and under contract, using proactive security tools to ensure full deployment and threat-based optimization helps security teams get the most out of their existing tools. Rather than simply adding more point solutions, they can see more value from what they already have.
2. **Decreased Risk** - We've seen reports that as high as 80% of breaches happened in organizations that already had a tool in place that could have prevented it. By taking advantage and optimizing their current security stack coupled with proactively seeking to minimize threats before they can be exploited, security teams can see a significant decrease in risk.
3. **Focus on Strategic, High Value Initiatives** - When security teams can focus on what increases cybersecurity maturity rather than simply reacting to alerts, they are able to do more high value, satisfying work that matters. The soft benefit: they stay longer.

What are Examples of Initiatives that Security Teams Can Get Value from Today?

Rather than advising the reader to buy more tools, there's a more effective way to be more proactive starting today. And while there's no such thing as 100% security or a magic bullet, the following will provide value immediately.

1. Decide which threats are the most important for your organization to protect against. This may sound like an oversimplification.
2. Map those threats with the campaigns and techniques that can actively exploit organizations like yours.
3. Understand how your defenses - your security controls and associated tool stack - map to those campaigns, techniques, and threats. For example: ransomware is not a one tool threat. It has several entrance vectors, exploit techniques, evasion methods, exfiltration paths....looking at the tools and their configuration and deployment in the context of attacks is the first step in understanding what can be done to decrease risk and maximize your investments.
4. Analyze business context - There will be exceptions, and there will be differences between units and groups. The finance team has different critical assets and attack paths than the Marketing team, and the development team will have assets that won't be covered by all the same tools as HR.
5. Build a baseline - The only way to improve is to know where you are and where you want to go. Understand your strengths and weaknesses, analyze the amount of effort and investment it will take to make progress, and then build your plan to make incremental progress over time.

About Nagomi Security



Nagomi is changing the way security teams balance risk and defense, empowering customers to focus on what matters now. By mapping customers' existing security tools to the threats that matter and providing prescriptive remediation plans, the Nagomi Proactive Defense Platform finally makes it possible to optimize, measure, and maximize the ROI of security investments. By taking a threat-centered, data-driven, and actionable approach to risk and cybersecurity, customers can provide high-level cybersecurity maturity metrics to executives while simultaneously showing security practitioners exactly what to do to reduce risk, fix misconfigurations, and make strategic decisions with business context. Learn more at nagomi.security.

nagomi SECURITY