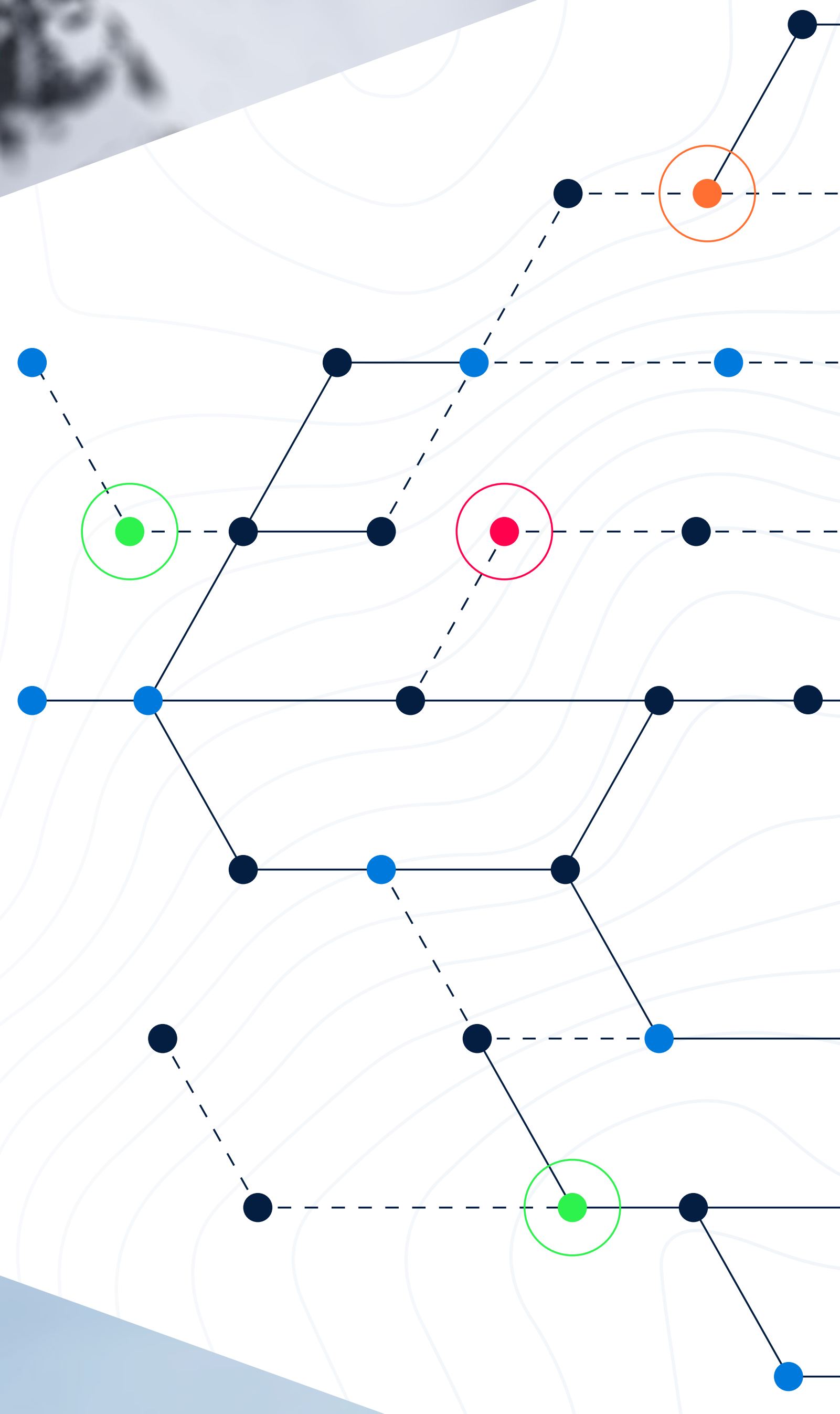
tenable one

FROM RISK-BASED VULNERABILITY MANAGEMENT TO

EXPOSURE MANAGEMENT

The Changing Definition
of Good Cyber Hygiene

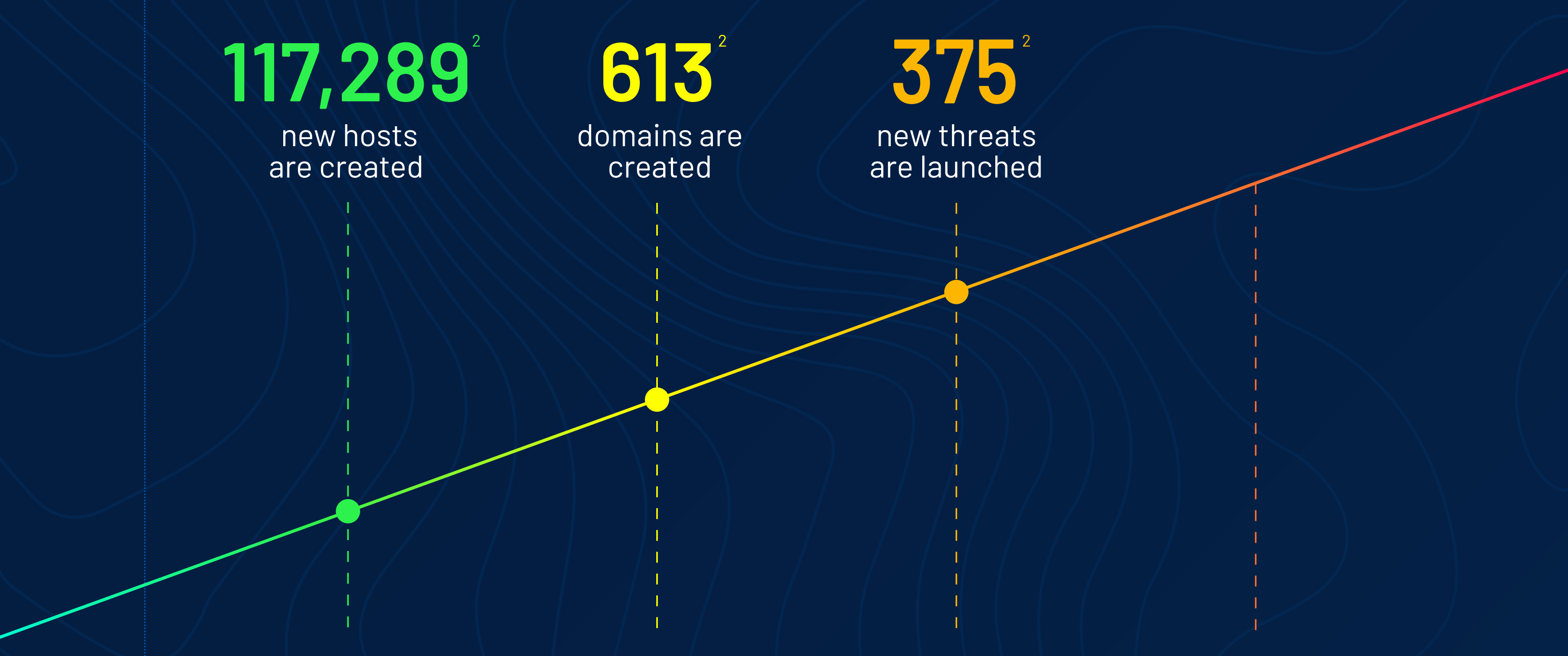


The adoption of modern technologies like cloud computing has made IT environments more **distributed, complex and dynamic,** and thus harder to protect.

As attackers aggressively seek to exploit security weaknesses, security teams face mounting challenges, including:

- **Limited visibility** into their expanded attack surface
- **Resource limitations** – both human and financial
- **Fragmented context** due to a siloed solution stack and "tool sprawl"
- Lack of **comprehensive metrics**
- Difficulty **assessing** & **communicating risk** status to leadership

The global attack surface is growing. **Every minute...**



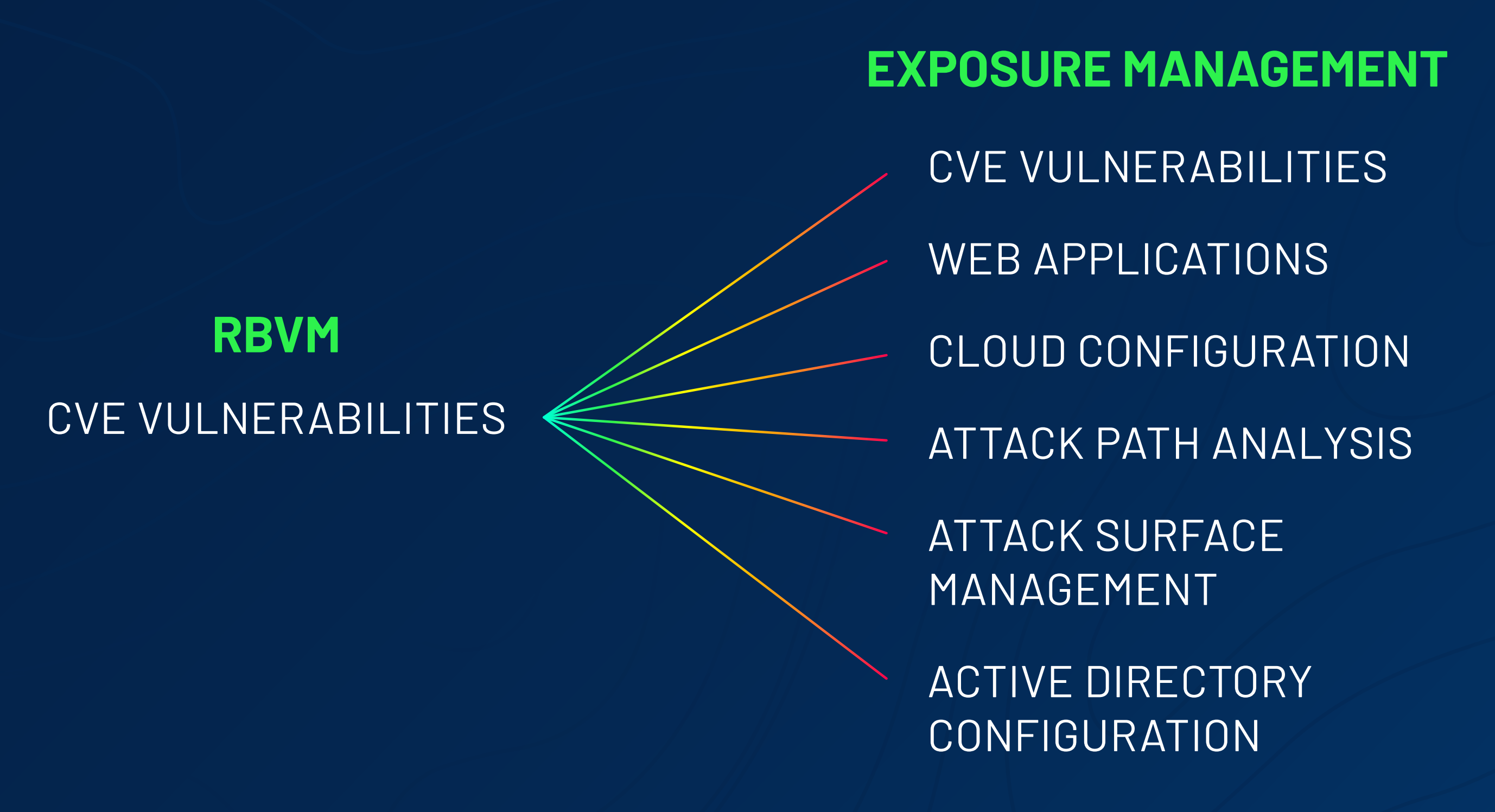
This new reality requires you to **transform your VM program** into a much broader exposure management strategy.

What An Exposure Management Platform Provides

Comprehensive Visibility
A unified view of all assets and software vulnerabilities, configuration vulnerabilities and entitlement vulnerabilities, whether on-prem or in the cloud.

Prediction and Prioritization
The ability to anticipate the consequence of a cyber attack and understand relationships between assets, exposures, privileges and threats across an attack path.

Effective Communication of Cyber Risk
A centralized and business-aligned view of cyber risk with clear KPIs, benchmarks to compare against external peers and actionable insights into your overall cyber risk.



RBVM
CVE VULNERABILITIES

EXPOSURE MANAGEMENT
CVE VULNERABILITIES
WEB APPLICATIONS
CLOUD CONFIGURATION
ATTACK PATH ANALYSIS
ATTACK SURFACE MANAGEMENT
ACTIVE DIRECTORY CONFIGURATION

> "By 2026, organizations prioritizing their security investments based on a continuous **exposure management** programme will be three times less likely to suffer from a breach."
>
> Gartner®, Implement a Continuous Threat Exposure Management (CTEM) Program, July 2022[1]

5 Steps to Creating an Exposure Management Program

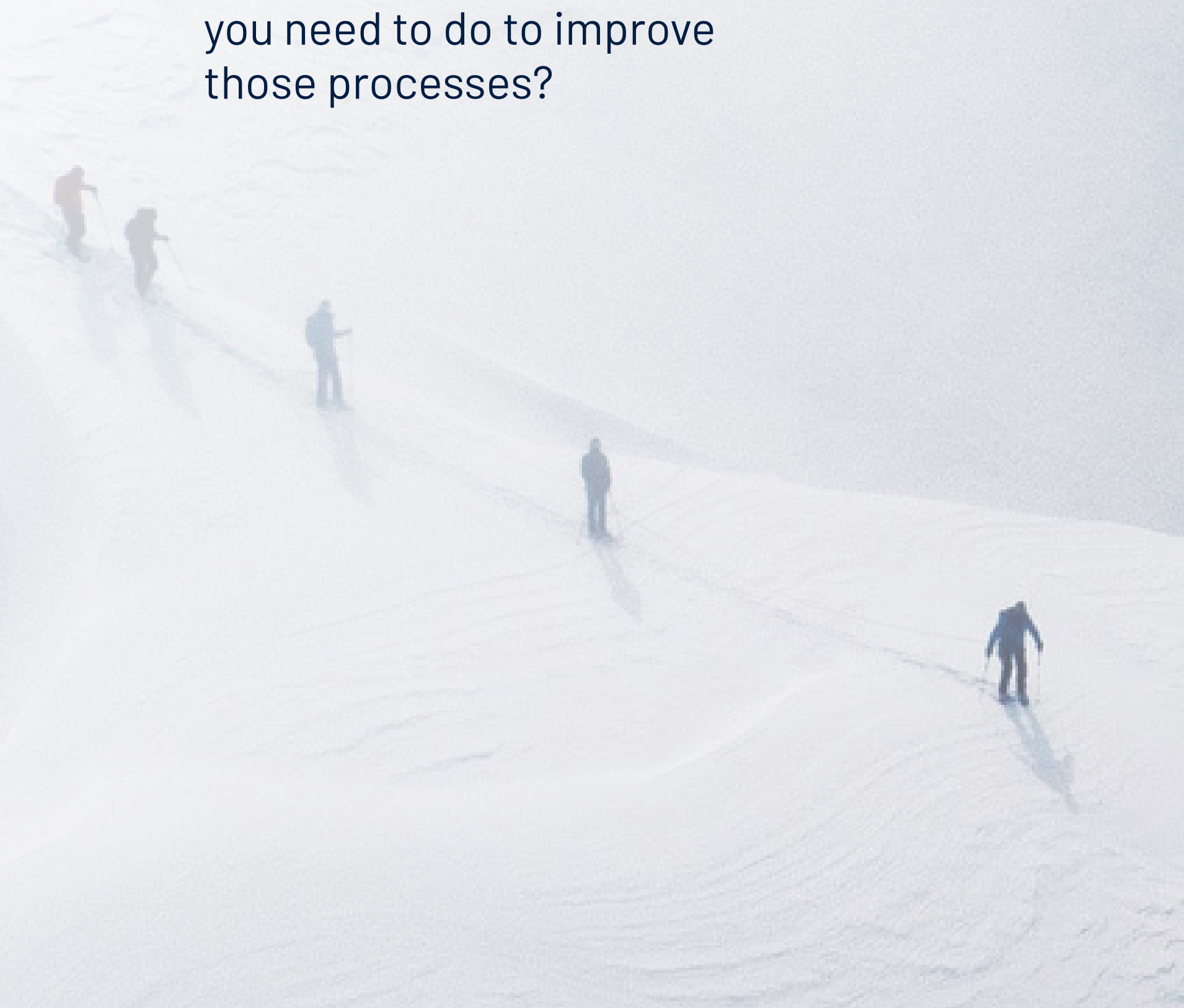
1 **Assess your security technologies**
Do they interoperate to offer you comprehensive insights into your **exposure** or are they information silos?

2 **Evaluate your attack-surface visibility from endpoints to the cloud**
Do you have blind spots?

3 **Prioritize your efforts**
What do you need to do first? How can you best prioritize your preventative efforts?

4 **Measure your remediation processes**
How well are you doing at fixing the things you find right now? What do you need to do to improve those processes?

5 **Assess your ability to communicate risks and take action**
Can you answer: **'How secure are we?'** How well can you communicate that status to both executive business management and your security teams?



GARTNER® is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

[1] Source: https://www.tenable.com/analyst-research/2022-gartner-exposure-management-report
[2] Source: Anatomy Of An External Attack Surface: Microsoft, April 2022

tenable