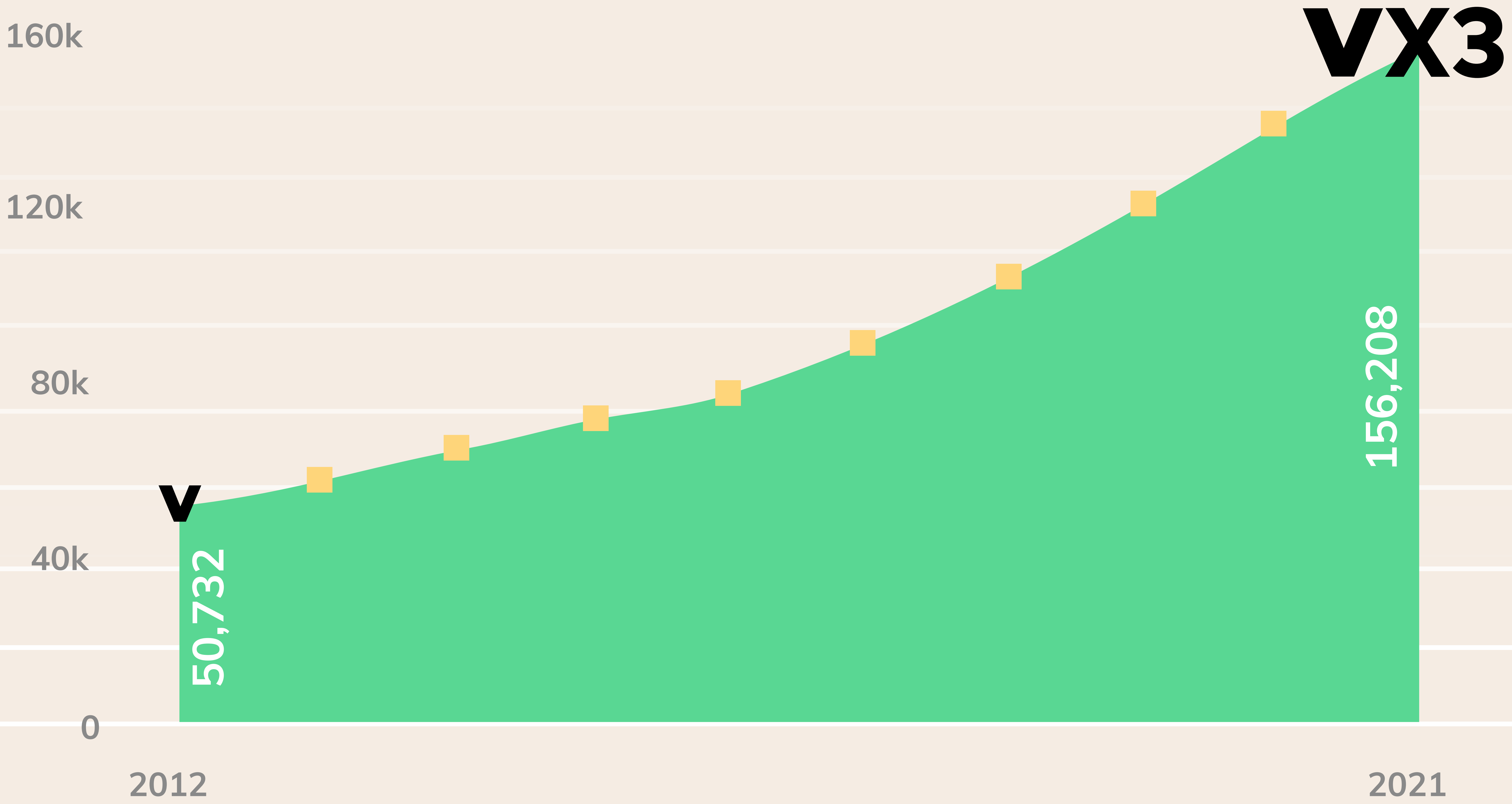
VULCAN.

The state of vulnerability management programs in 2021

As attack surfaces grow and become more complex, security teams must evolve their tools and processes to match the increasing complexity of their environments and those looking to attack them - or risk getting left behind. How are they coping?

Vulnerabilities have

tripled over the past 10 years



/www.skyboxsecurity.com

+30%

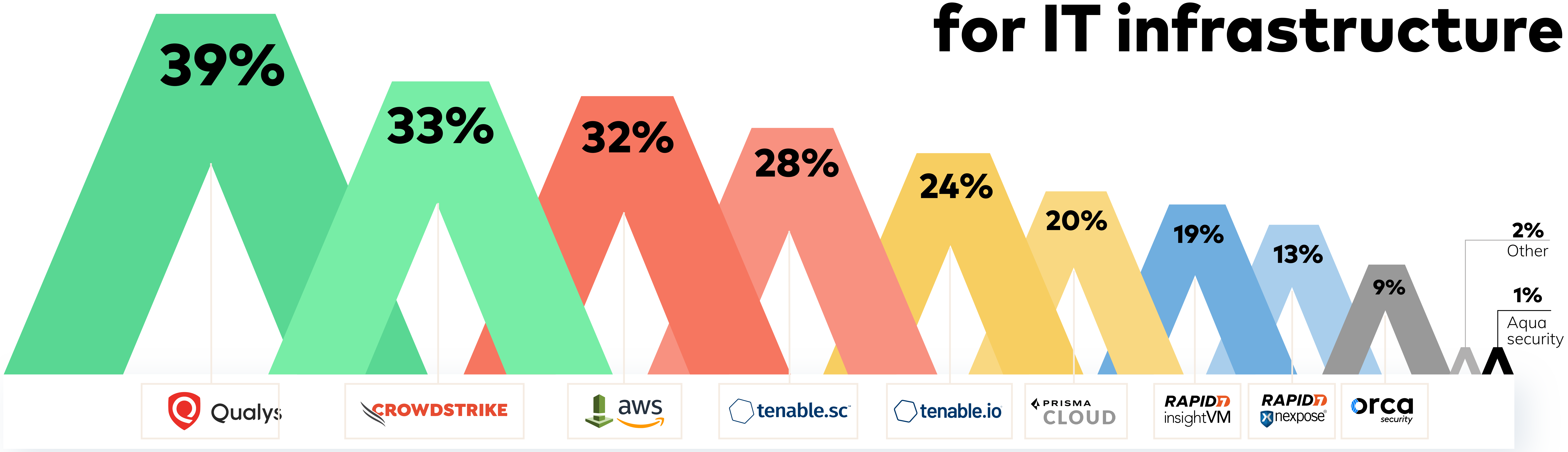
New vulnerabilties
exploited in the wild

And, in the first half of 2021 alone,

the number of exploits rose by 30%

Qualys, Crowdstrike, AWS Inspector and Tenable were amongst the

most used vulnerability scanners for IT infrastructure

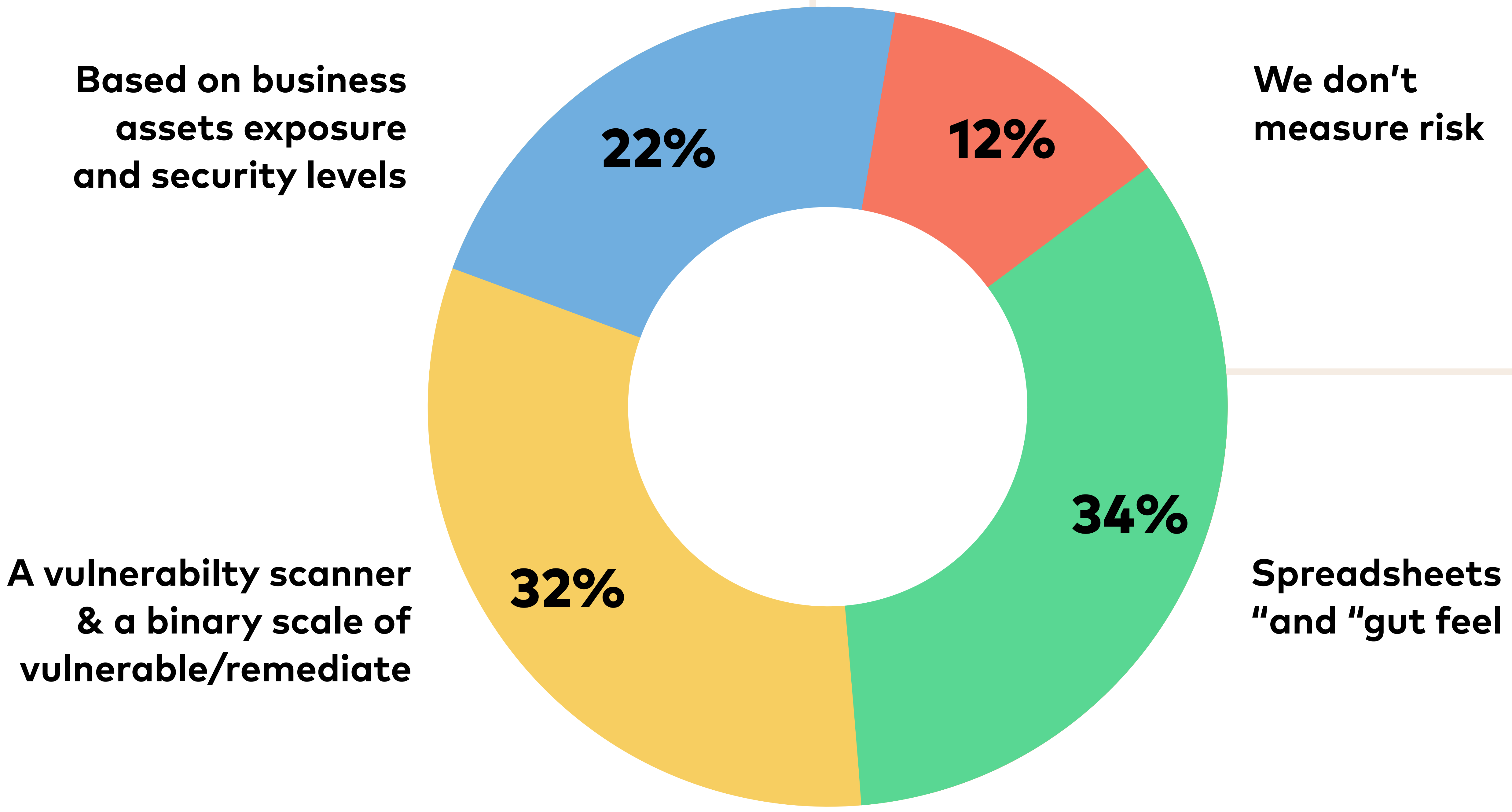


Vulcan/Pulse Research July 2021 - "How are businesses mitigating cyber risk?"

But when it comes to measuring risk many cybersecurity pros are still using

"gut feel" and outdated technology

How does your company measure risk to the business stemming from unsolved vulnerabilities?

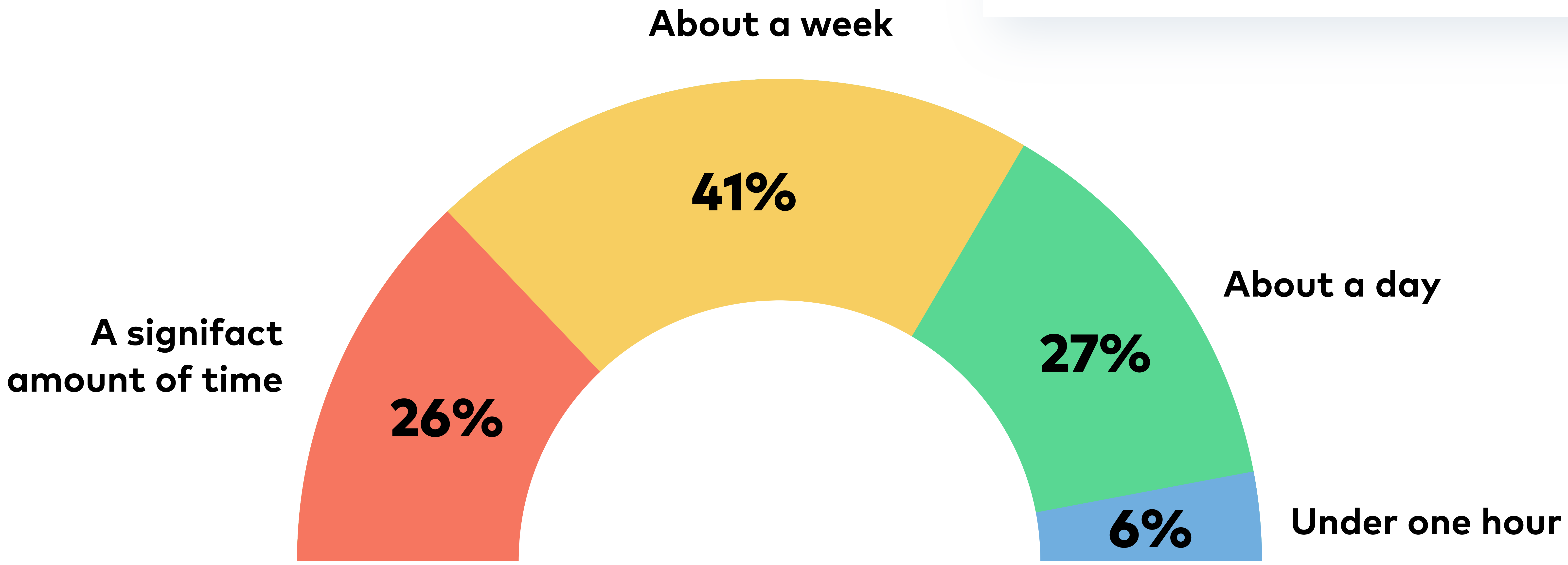


Almost a third of executives admit it takes their team

a significant amount of time to solve a vulnerability

?

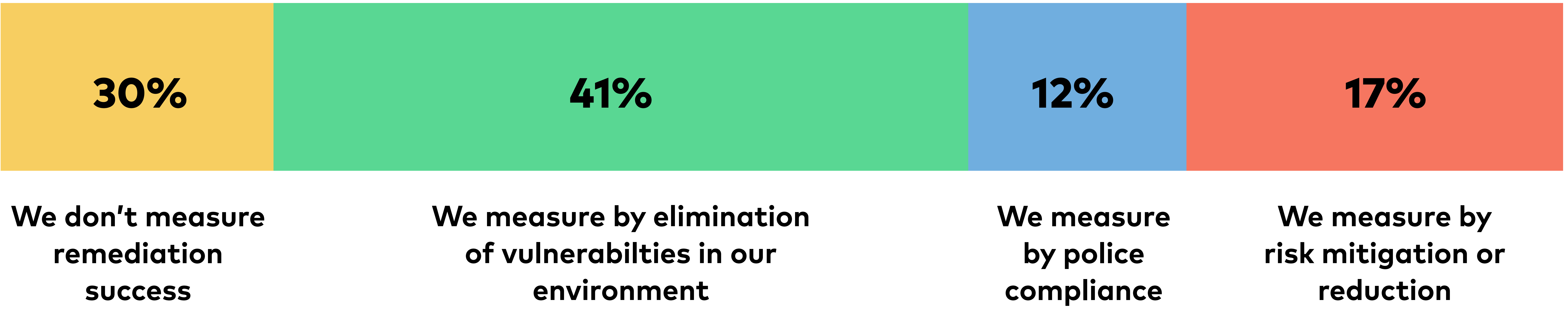
How long does it take for your organization to find the appropriate solution, remedy, or fix for a vulnerability?



And even when a resolution is implemented, the majority

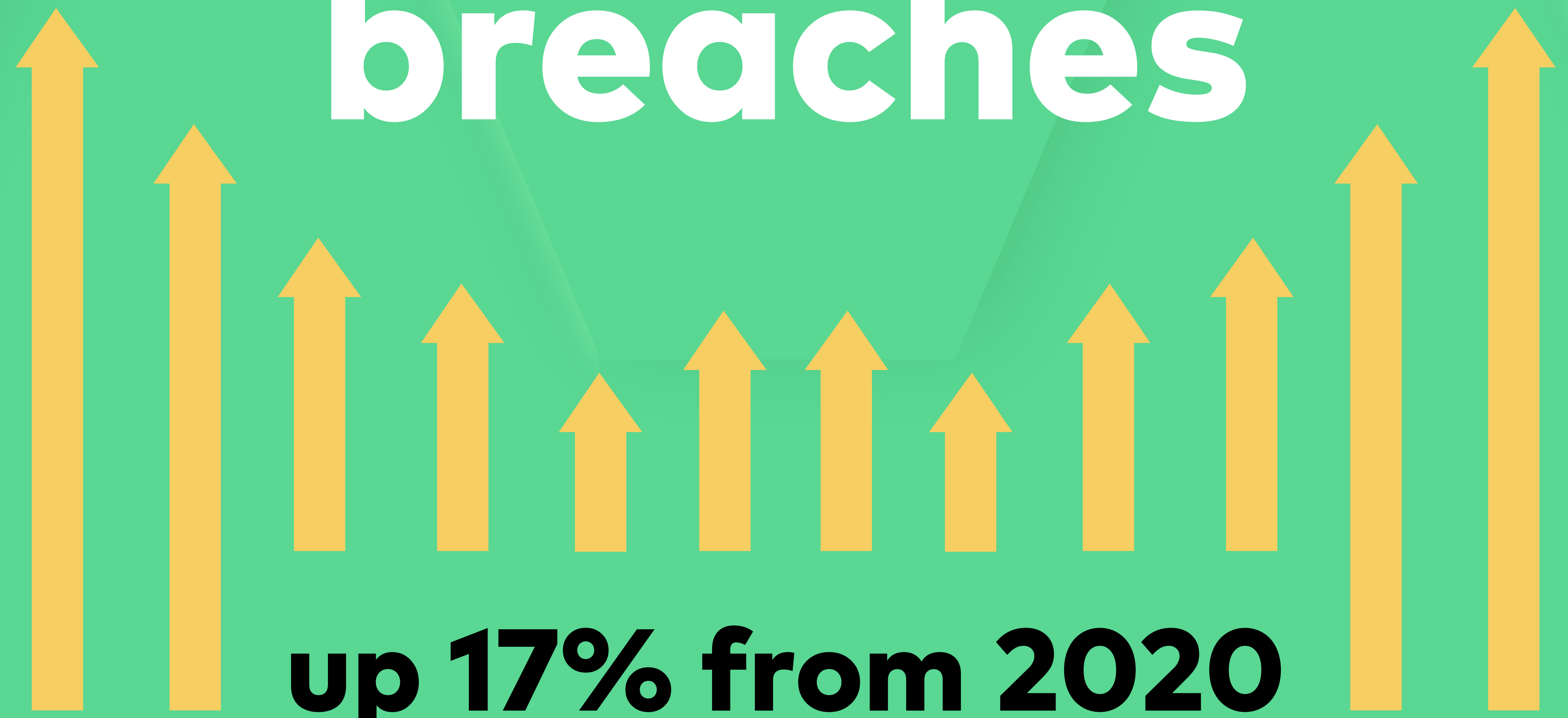
either don’t measure risk remediation success, or do so based on vulnerability elimination

? How long does it take for your organization to find the appropriate solution, remedy, or fix for a vulnerability?



The result?

A record-breaking year for data breaches

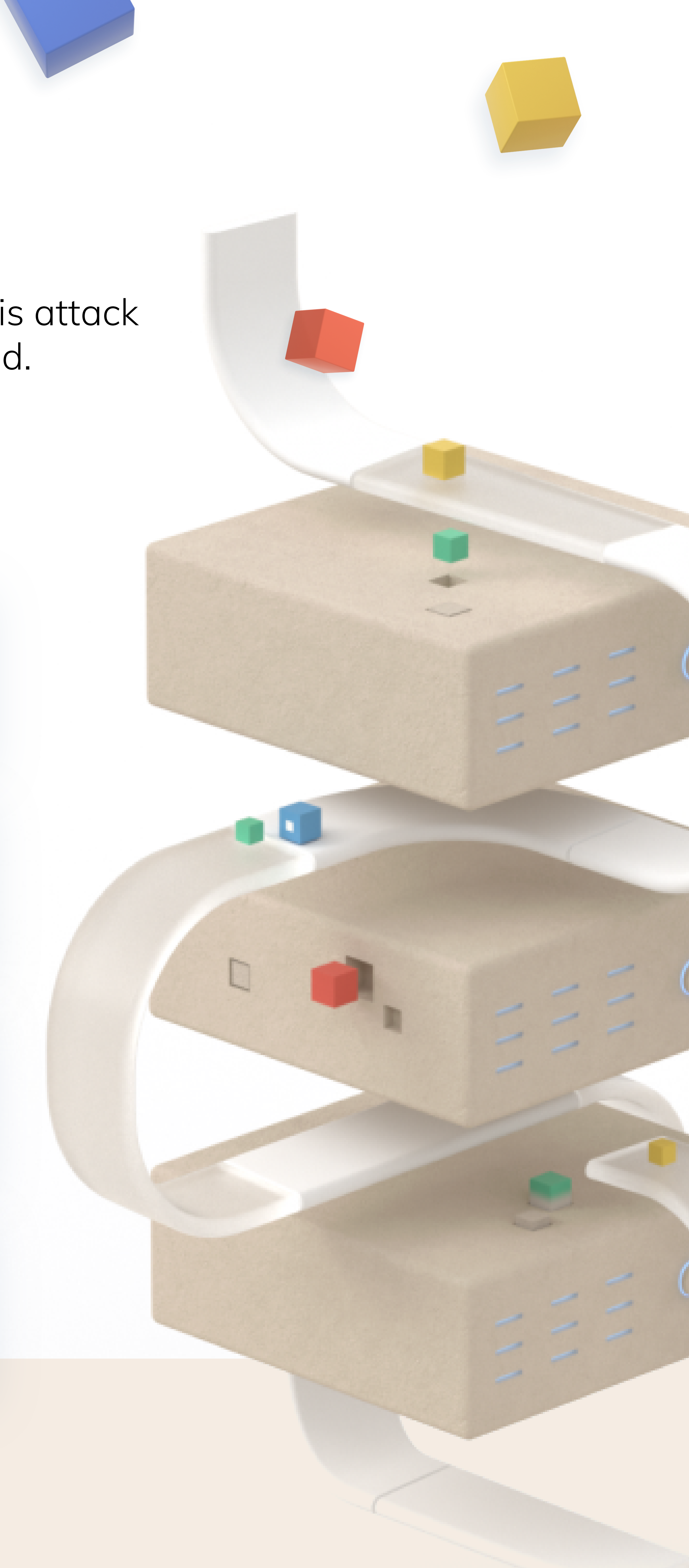


up 17% from 2020

Cybersecurity teams must become **even more vigilant** in protecting their organizations' assets. But many teams depend on instinct and limited processes to assess danger to their businesses. A shift away from a strategy aimed at simply reducing vulnerabilities, and towards one which **actually focuses on managing and mitigating risk end-to-end** will ensure security professionals strengthen their vulnrerability management security posture and own risk.

Looking ahead to 2022

Teams need better visibility into their assets and greater ownership of their risk. But as we enter a new year, we expect this attack surface to only keep growing, meaning more unmanageable vulnerability data and leaving many organizations unprepared.



IN 2022, WE NEED TO BE SMARTER AND MORE PROACTIVE ABOUT HOW WE ADDRESS OUR RISK:

1. **SEE YOUR RISK CLEARLY:** better visibility means better decision making. That starts with the right processes and dedicated tools for better risk mitigation.

2. **SMARTER PRIORITIZATION:** external sources aren't enough to define the most critical vulnerabilities - teams must be proactive about identifying the risk that most affects their business. The best way to get started? Try Vulcan Free.

3. **STAY UP TO DATE WITH REMEDIATION INTELLIGENCE:** With more targets for attackers, teams need to be more vigilant than ever. Tools like the Vulcan Remedy Cloud can help you stay ahead of the latest vulnerabilities and their fixes.

4. **YOU CAN'T MITIGATE RISK IF YOU CAN'T ARTICULATE IT:** cyber risk management is a shared responsibility across an entire organization. For 2022, learn how some of the leading cyber security pros communicate risk within their businesses.

Vulcan Cyber® gives you full ownership of your cyber risk and lets you articulate risk and delegate responsibility across your organization. Prioritization. Orchestration. Mitigation. Wherever you are in the lifecycle - Vulcan gives you everything you need to finally go beyond your risk – and actually reduce it.

VULCAN.