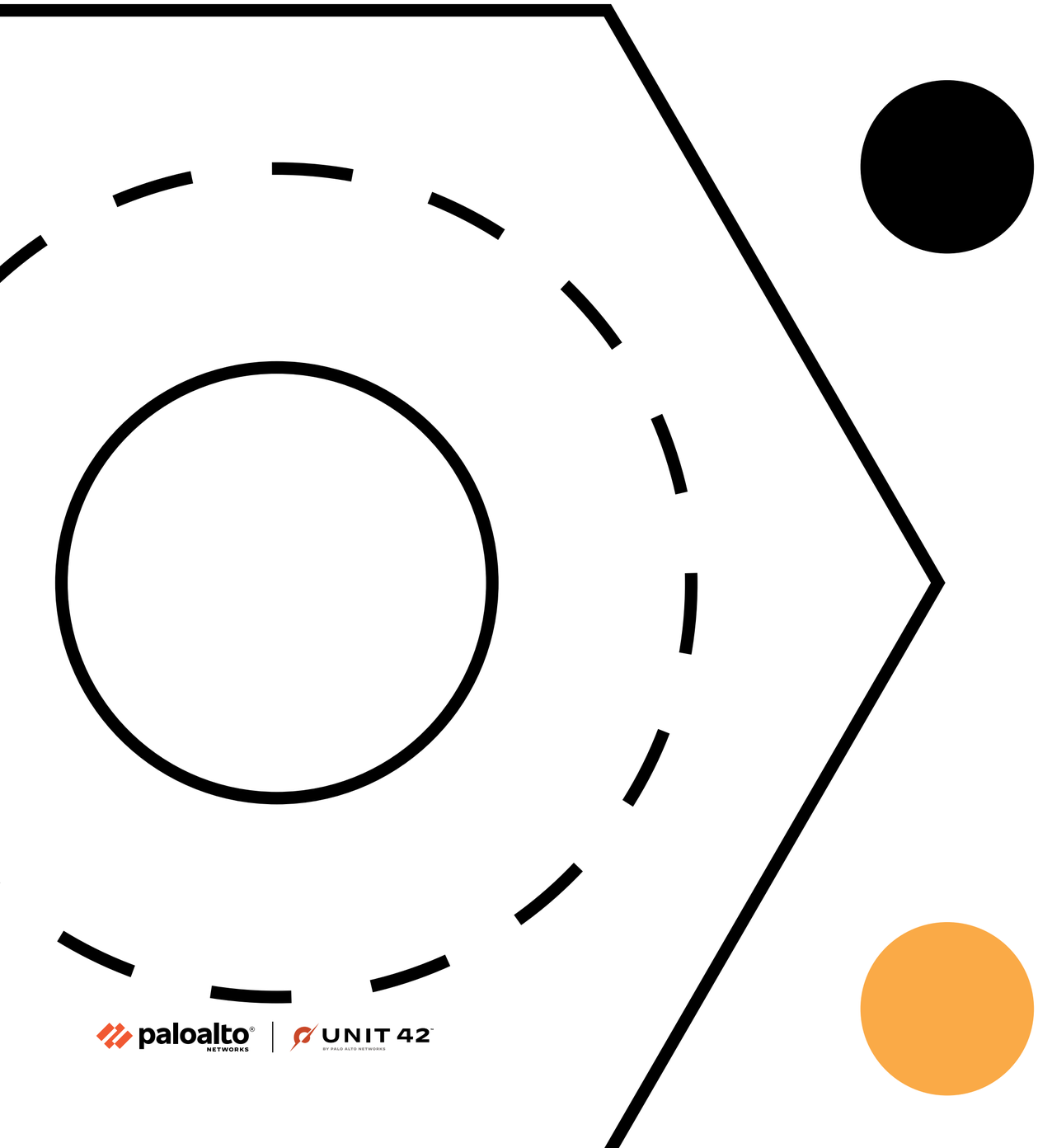
A Threat-Informed Approach to

Sustainable Cyber Resilience

Assessing Security Controls, Transforming Strategy, and Responding in Record Time

paloalto NETWORKS | UNIT 42 BY PALO ALTO NETWORKS



Cyber Resilience Requires a Threat-Informed Approach to Breach Preparedness

Organizations like yours are facing a number of challenges, making it increasingly difficult to protect against security breaches. Due to infrastructure moving to the cloud and organizations moving to a hybrid workforce, your attack surface is expanding and changes beyond your control are occurring daily. And because of the security skills shortage, organizations are having difficulty finding and retaining experienced analysts and incident responders. Research shows that 63 percent of organizations were breached in the past 12 months. Organizations were breached an average of three times in that time frame.[1]

The threat landscape continues to evolve at a faster pace than most organizations are adapting their defenses. In fact, enterprises spend a

[1] The 2021 State of Enterprise Breaches, Forrester, April 8, 2022.

37 days

Enterprises spend a median of 37 days and an average of $2.4 million to find and recover from a breach.

median of 37 days and an average of $2.4 million to find and recover from a breach,[2] and the immediacy of cyberthreats has changed with the evolution of trends like ransomware as a service. You can't afford to be slow to respond when you are hit with ransomware, halting all of your business operations.

Cybersecurity needs attention from your entire organization. Security and resiliency are now board-level issues. There is greater pressure from the board for transparency and continuous demonstration that your organization is protected and prepared to respond to ever-evolving threats. In fact, the U.S. Securities and Exchange Commission recently "proposed amendments to its rules to enhance and standardize disclosures regarding cybersecurity risk management, strategy, governance, and incident reporting by public companies."[3] This enables investors to evaluate organizations' cybersecurity posture and incident reporting in order to make better informed decisions.

63%

of organizations were breached in the past 12 months. Organizations were breached an average of three times in that time frame.

[2] Ibid.

[3] "SEC Proposes Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies" press release, U.S. Securities and Exchange Commission, March 9, 2022.

Stuck in a Reactive Vortex

As if immediate risks weren't enough to manage, now there's yet another dimension: not only are you expected to respond faster than ever before, you're expected to learn from the attack in progress — and apply that knowledge to head off future breaches.

You're focused on protecting your business from risk, but with immediate dangers always on the horizon, **it's easy to get stuck in a reactive vortex rather than incorporate new lessons learned.**

To address these issues, many organizations measure success over time by focusing mostly on operational SOC metrics — number of attacks, alerts, and closed incidents — to show progress and demonstrate compliance.

While these are important, focusing on them alone won't help you proactively address these critical questions:

- Are the right people in place, and are processes optimized?
- Have you invested in the right tools and technology?
- Is there proper governance to protect the organization?

Relying on Cyber Insurance Alone Won't Work ...

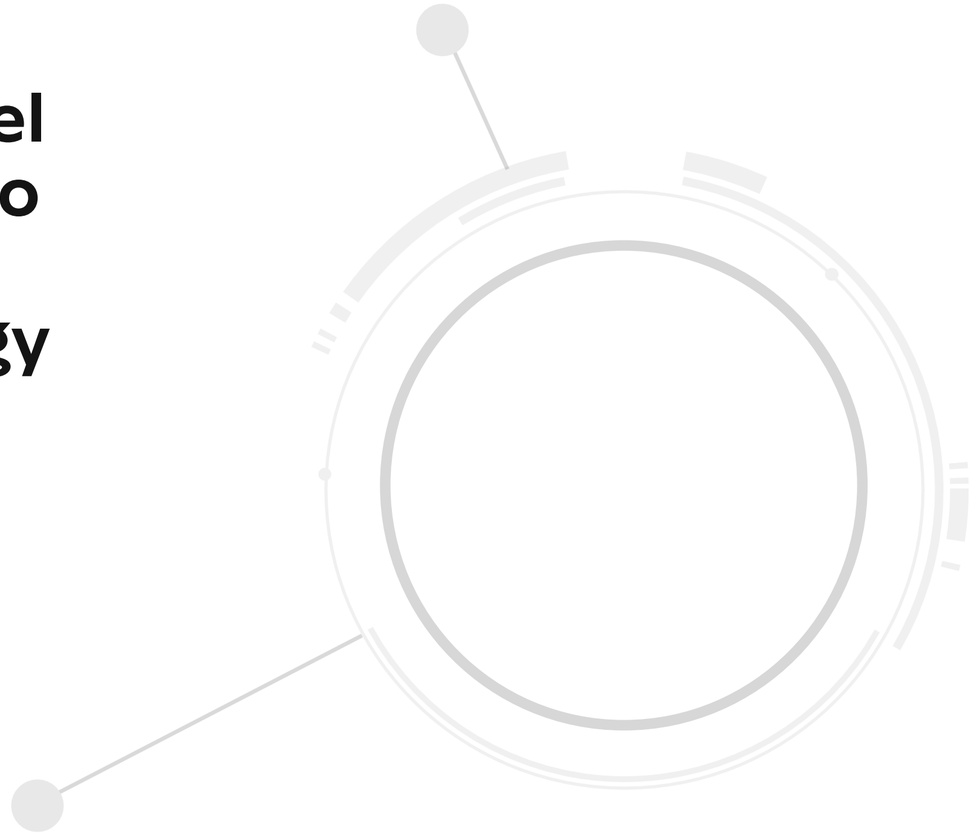
As far as resiliency goes, organizations hope an attack never comes, knowing they will need to react and learn in a time of crisis. Some businesses rely heavily on cyber insurance carriers to guard against financial losses. However, this won't protect your data, guard your organization from revenue loss and reputational brand damage associated with employee turnover, or change your ability to respond to cyberattacks.

Additionally, if you don't see the bigger picture beyond your operational metrics and incorporate leading indicators that help you make proactive threat-informed decisions, you may be wasting limited resources on projects that aren't aligned with the biggest risks facing your organization. You eventually recover, but because most organizations are stretched so thin, the team is running to the next fire drill instead of incorporating lessons learned — so you aren't improving.

... but Prioritizing Resilience Will

Organizations now realize the real issue they face is achieving resiliency by moving from a reactive to a proactive security strategy that aligns your defenses to protect against your biggest risk. To accomplish this, you need to assess and test your security controls, transform your strategy with a threat-informed approach, and respond in record time when faced with a security incident.

Harness a Threat-Intel Informed Approach to Continuously Evolve Your Security Strategy



But How?

Work with Unit 42:
Intelligence driven. Response ready.

Our Unit 42 world-renowned threat researchers, elite incident responders, and expert security consultants will guide you before, during, and after an incident with an intelligence-driven approach. By partnering with us, you can do all of the following.

Assess and test your security controls against real-world threats.

Your security risk constantly changes as your attack surface expands and adversaries shift their techniques. With Unit 42, you can continually test and refine your security controls to reduce the likelihood of successful attacks and spend your limited resources where they matter most: focused on the threats that represent the biggest risk to your organization.

Learn more

Transform your security posture with a threat-informed approach.

Adopting a proactive security posture focused on understanding the most credible threats to your business is critical to reducing cyber risk. Unit 42 will brief you on the evolving threat landscape and, after each response, help you apply lessons learned to protect against future attacks.

Learn more

Respond in record time to minimize the impact of an attack.

When an attack occurs, there is a material threat to your business. By having Unit 42 incident responders on speed dial, you will investigate, respond to, and recover from attacks while creating a feedback loop to strengthen your defenses after each response.

Learn more

When you're able to learn from past cyber incidents and focus on the shape of future attacks, you'll better protect your organization from security threats now and in the future.

Visit **paloaltonetworks.com/unit42** to learn about the evolving threat landscape and how Unit 42 is taking a threat-informed approach to help you identify gaps based on the latest threats that represent the biggest risk to your organization.

About Unit 42

Unit 42™ by Palo Alto Networks brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster.

Get in touch with one of our team members to learn more about how Unit 42 can help your organization defend against and respond to severe cyberthreats.