paloalto NETWORKS | Cybersecurity Partner of Choice

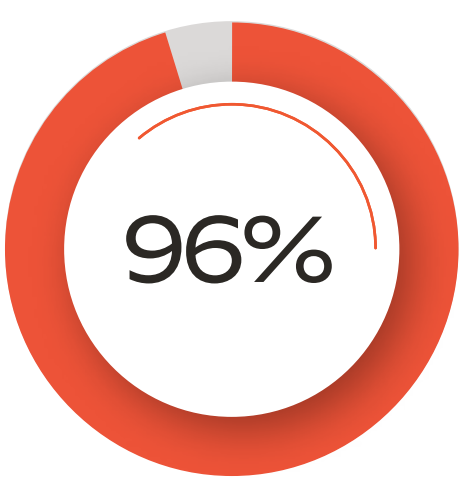
Netdata CYBERSECURITY

Cyber Transformation: 3 Key Areas to Prioritize

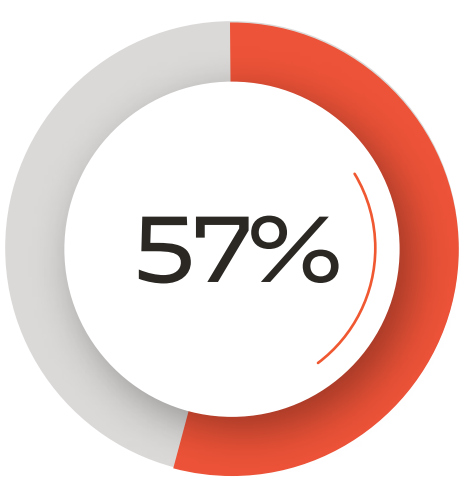
Organizations today face a cyber landscape characterized by rapid change and evolving threats. Digital transformation has moved most workloads from legacy systems to the cloud—creating a maze of IT complexities and security blind spots. Meanwhile, more workers are hybrid and remote than ever, contributing to an expanding volume of vulnerable endpoints and applications.

Further complicating this is the emergence of AI-driven threats that allow malicious actors to launch sophisticated attacks at scale. In the midst of so much change, your organization needs cyber transformation built upon consolidating your security infrastructure.

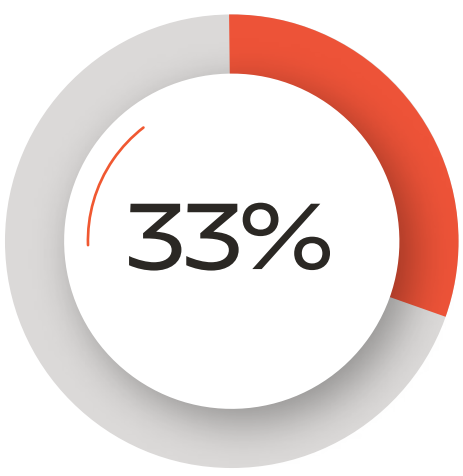
WE SURVEYED 1,300 C-SUITE LEADERS FROM ACROSS THE WORLD AND FOUND THAT:*



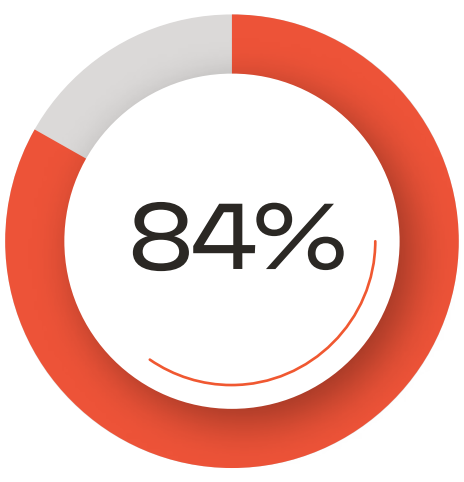
of all respondents experienced at least one breach



experienced three or more breaches



of CXOs said they experienced an operational disruption as a result of a breach



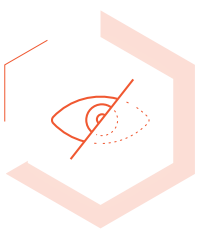
agree (to varying levels) that they have seen more security incidents due to hybrid work

HERE ARE THE TOP 3 AREAS TO PRIORITIZE:

1. Reduce Security Complexity

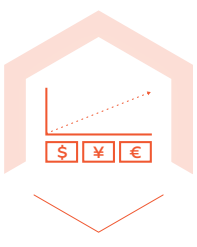
Is your security infrastructure a tangled web of siloed vendors, solutions, and services? Adding a new tool for every emerging security requirement might be effective in the short term, but it also adds to the growing complexity of your environment in the long term.

The challenge:

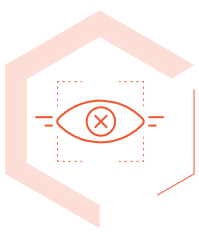


Minimal visibility across the infrastructure

Increased implementation timespots



Increased procurement time and costs



Security gaps and blind spots

Higher risk exposure

The average number of security vendors and tools used by organizations today:

13.39
vendors*

31.58
security tools*

To transform your security and elevate cyber resilience, your goal should be reducing the number of vendors, tools, and services—all without compromising on security efficacy.

Consider how consolidating your cybersecurity vendors can help save significant time and resources, improve your risk posture, and increase your ROI.

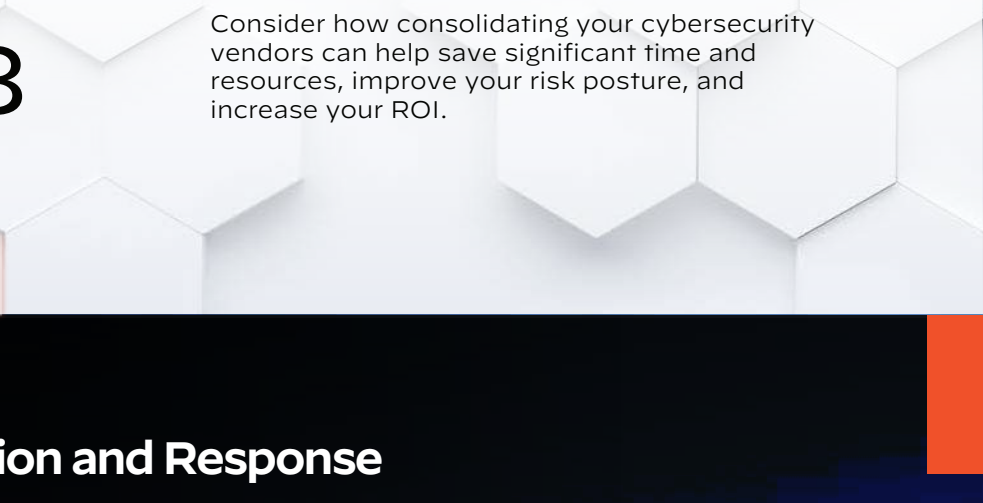
2. Automate Threat Detection and Response

Today's threat actors use emerging technologies such as AI and automation to avoid detection, exploit vulnerabilities, and launch sophisticated campaigns. SOC teams can't keep up—especially those that still rely on manual investigations of alerts. Coupled with the complex web of siloed security products and the global shortage of cybersecurity talent, you have a perfect storm for a successful breach.

It's time to fight fire with fire. Your security teams should leverage ML-powered automation to prevent, detect, and respond to threats with minimal human intervention. Environments with security automation baked in can easily recognize and thwart attacks before they occur, enhancing your cybersecurity and allowing your team to focus on more impactful tasks.

Consider how consolidating your security infrastructure enables you to automate incident response and better orchestrate across your organization.

3. Supercharge Risk Posture

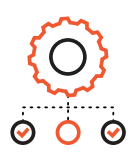


An environment built upon siloed security products isn't just a technical and logistical headache, it poses real risks to your organization. Today's attacks are highly targeted—and they thrive in infrastructures with siloes and blind spots. Security products that don't offer a holistic view of your attack surface will fail to detect advanced attacks.

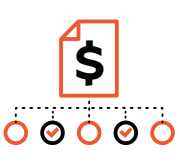
To elevate your cyber resilience, your goal should be to create synchronization between your different tools. For example, tools that are highly integrated share threat intelligence—such as security data points—and give you complete visibility across your entire environment.

Consider how consolidating your cybersecurity can help your SOC stay multiple steps ahead of attackers and supercharge your risk posture.

BENEFITS OF CYBERSECURITY CONSOLIDATION



Simplified management



Simplified procurement

Complete visibility

Streamlined operations

Eliminated security gaps

Accelerated response time

Want to Know More About Cybersecurity Consolidation?

Get the e-book:
Secure From Every Angle

Know more www.netdatanetworks.com

* "*What's Next in Cyber*," Palo Alto Networks, December 13, 2022.

paloalto NETWORKS

Methodology
The Palo Alto Networks 2022 global *What's Next in Cyber Survey*, conducted by Wakefield Research between July 26 and August 16, 2022, polled 1,300 C-suite leaders who are responsible for cybersecurity at large companies (those with $250+ million in revenue) around the globe (NAM: US and Canada; EMEA: UK, France, Germany, Netherlands, Italy, and Spain; LATAM: Brazil and Mexico; JAPAC: Japan, Singapore, India, Australia, and New Zealand), and asked them to share their priorities, concerns, and opinions on the industry that is shaping every other.