

6 Questions to Determine If Your Security Strategy Is Ready for AI-Driven Threat Defense

Why Modern Enterprises Need a Smarter Defense

Cybersecurity is at a tipping point.

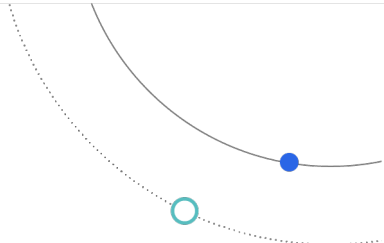
Gone are the days when firewalls and endpoint antivirus alone could keep your business safe. In today's world of generative AI, cloud-first operations, and highly automated attack campaigns, threats move faster and adapt faster than traditional defenses can handle.

According to IBM's 2023 Cost of a Data Breach Report, the average breach takes 277 days to identify and contain—yet AI-driven threats can compromise systems in under an hour. And despite billions invested in security, many organizations still depend on fragmented, legacy tools that can't respond at the speed or scale required to protect their environments.

Meanwhile, cybercriminals are using machine learning, AI-based phishing generators, and ransomware-as-a-service to exploit vulnerabilities across hybrid and multi-cloud ecosystems. The result? More frequent, more damaging, and harder-to-detect attacks.

So how do you know if your current security strategy is ready?

This checklist—created by C1 and Palo Alto Networks—offers a practical, insight-driven tool for IT and security leaders to assess their readiness for AI-powered threat defense. Each question is designed to uncover critical gaps and point you toward solutions that combine next-generation technology with expert-led services.



The Checklist

1

Can you detect and respond to threats in real time?

Why it matters to your business: Modern attacks—especially those powered by AI—move at machine speed. If your SOC (Security Operations Center) takes hours or days to investigate alerts, attackers may already have exfiltrated data or deployed ransomware.

Example: A healthcare provider using legacy SIEM tools detected an intrusion—but only after 48 hours. By then, attackers had already accessed 4,000 patient records. With Cortex XSIAM and C1's MDR, this could have been detected in seconds and stopped before any data was lost.

Yes No Not Sure

2

Are your defenses integrated across endpoints, cloud, and network?

Why it matters to your business: Siloed tools create blind spots. Without cross-platform integration, security tools can't share data or respond cohesively to threats across hybrid environments.

Example: A manufacturer was breached through a SaaS app after attackers exploited a misconfiguration that endpoint tools didn't flag. Palo Alto's Prisma Access, NGFW, and Cortex XDR—deployed and integrated by C1—could've detected the anomaly in real time.

Yes No Not Sure

3

Are you using AI to reduce alert fatigue??

Why it matters to your business: SOC teams are overwhelmed. More than 77% of alerts go uninvestigated because security staff are buried in false positives (Cisco Security Report 2024). AI helps automate triage, improve signal-to-noise ratio, and prioritize actual threats..

Example: A regional bank's team received 10,000+ alerts daily. With Palo Alto's Precision AI™ and C1's managed services, only the most critical 2-3% were escalated—allowing analysts to focus on what matters.

Yes No Not Sure



4 Have you implemented Zero Trust with continuous identity verification?

Why it matters to your business: 81% of breaches involve stolen or weak credentials (Verizon DBIR, 2024). Without Zero Trust, attackers can move laterally after breaching a single endpoint or account.

Example: A university fell victim to ransomware via a student's compromised VPN login. C1's Zero Trust deployment with ZTNA 2.0 from Palo Alto would have denied access based on device posture and geolocation—even if credentials were valid.

Yes No Not Sure

5 Is your security strategy aligned with business and compliance goals?

Why it matters to your business: Effective security must also meet regulatory standards (HIPAA, PCI-DSS, NIST) and support business continuity. Misaligned tools may create compliance gaps—even if they work well individually.

Example: A retail group passed all pen tests—but still failed a PCI-DSS audit due to gaps in identity governance. C1's Advisory Services helped align detection policies with compliance requirements and operational objectives.

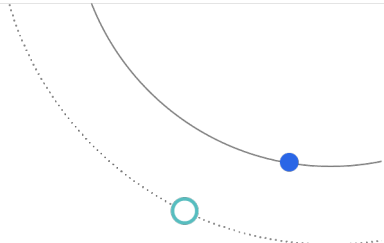
Yes No Not Sure

6 Are you continuously improving your security operations?

Why it matters to your business: Security isn't a set-it-and-forget-it effort. Threat actors constantly evolve tactics. Organizations must continually adapt detection logic, playbooks, and risk models to stay ahead.

Example: An energy company suffered a breach from a novel exploit that its static antivirus didn't detect. With C1's Managed Services, automated threat intelligence updates and tuning would've closed the gap before the attack occurred.

Yes No Not Sure



How Did You Score?

5-6 Yes Answers:

You're on the leading edge of AI-driven security. C1 can help you optimize and scale your capabilities.

3-4 Yes Answers:

You're making progress, but critical vulnerabilities remain. Let's map out your next steps.

0-2 Yes Answers:

Your strategy is outdated. The time to modernize is now—before a breach forces your hand.

Take the Next Step with C1 and Palo Alto Networks

C1's **Advisory, Professional, and Managed Security Services**—integrated with **Palo Alto Networks' AI-powered platforms**—enable modern enterprises to:

- Detect and contain threats in real time
- Automate and integrate defenses across hybrid environments
- Meet compliance goals with confidence
- Reduce response time, cost, and risk

Don't wait until it's too late.

Start your modernization journey at www.onec1.com/security



C1, the global technology solutions provider, transforms businesses by creating connected experiences that shape the future. With more than 6,000 customers, C1 empowers industries through secure, innovative technologies, collaborating with leading partners to deliver total lifecycle solutions. Learn more at onec1.com.