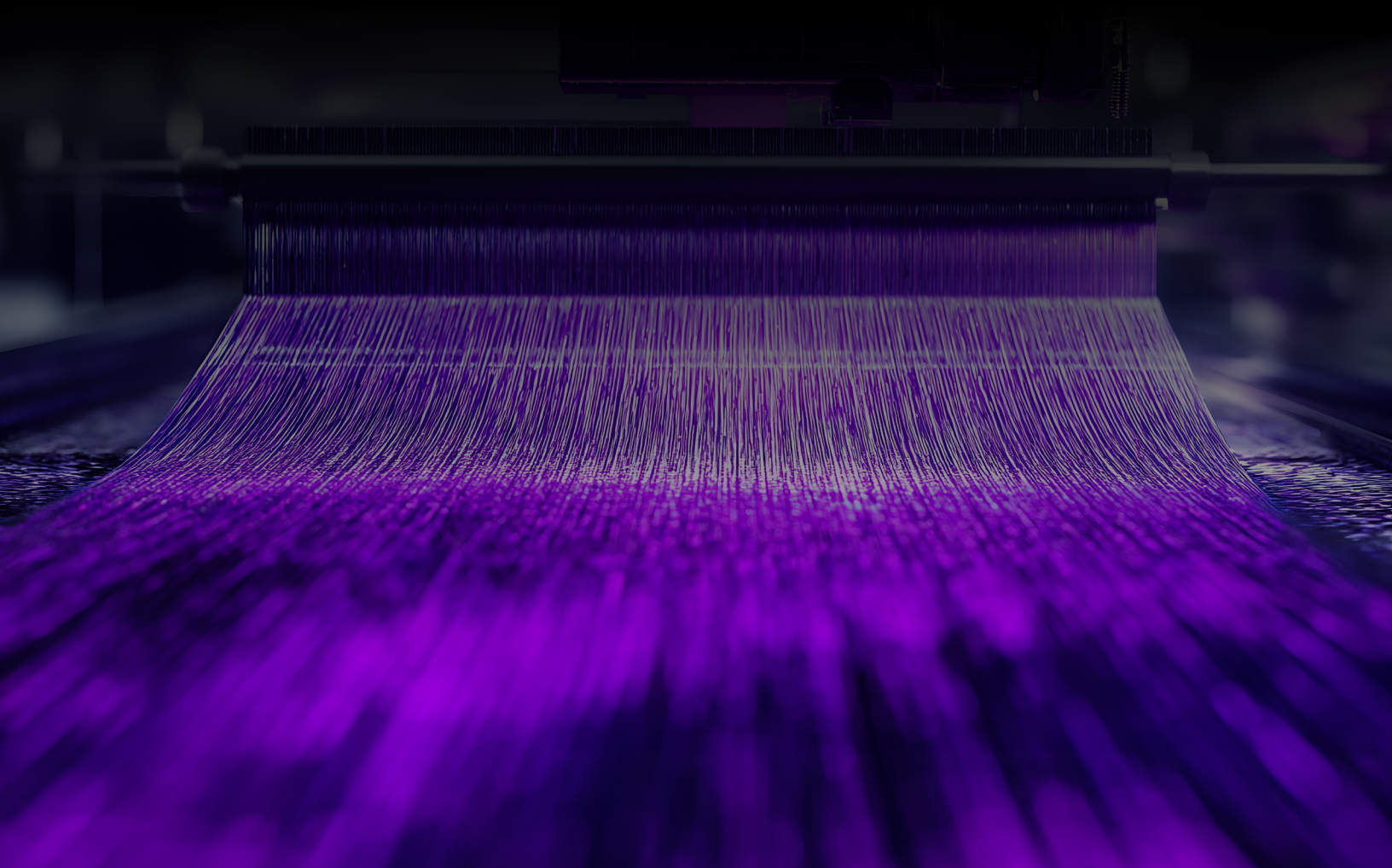
Is Your Cybersecurity Stack Ready for AI Automation?

How C1 and Palo Alto Networks Deliver Smarter Threat Defense



Why Security Teams Need AI Now

Cybercriminals have entered the AI era—and most enterprise security stacks haven't caught up. From AI-powered phishing and deepfake attacks to autonomous malware and zero-day exploitation, threats now move faster than ever.

While defenders still depend on outdated tools and manual workflows, attackers use automation, machine learning, and cloud-based obfuscation to bypass defenses.

According to IBM's 2023 Data Breach Report:

- Organizations with AI and automation saved $1.76M more per breach
- The average breach lifecycle in non-automated environments was 277 days

In response, security leaders are asking:

"Is my current security stack equipped to defend against AI-powered threats?"

This guide will help you answer that question—and show how C1 and Palo Alto Networks provide the technology and services to close the gap.

Table of Contents

5 Signs Your Stack Isn't AI-Ready

1. You rely on manual triage and investigation

Legacy SIEMs generate floods of alerts—many irrelevant. Security teams burn time chasing false positives, missing real threats.

Problem: SOC fatigue leads to alert dismissal or slow response

Business Impact: Delayed containment, greater damage, regulatory risk

Example: A retail chain's SOC manually investigated every critical alert, averaging 12 hours to triage. Meanwhile, an attacker exploited stolen credentials to move laterally undetected.

C1 + Palo Alto Fix:

Cortex XSIAM triages alerts autonomously

2. You have limited visibility across your cloud and hybrid environments

Point solutions monitor individual environments, but attackers move across platforms—cloud to endpoint to SaaS.

Problem: Fragmented views miss threat movement and misconfigurations

Business Impact: Exfiltration, unauthorized access, untraceable attacks

Example: A healthcare system experienced data leakage from a misconfigured cloud storage instance that the legacy SIEM couldn't monitor.

C1 + Palo Alto Fix:

Prisma Access + Cortex XDR unify visibility across users, endpoints, and apps

C1 Professional Services architect and integrate comprehensive telemetry sources for real-time insight

3. Your threat response depends on human availability

If it takes hours—or days—to confirm and act on an alert, the damage may already be done. .

Problem: 24/7 response isn't scalable with manual operations

Business Impact: Extended dwell time, higher remediation costs, public fallout

Example: A financial services firm took 38 hours to contain a malware infection. It cost them $2.2M in response, downtime, and customer churn.

C1 + Palo Alto Fix:

SOAR playbooks automate containment (e.g., isolating compromised endpoints, revoking access)

4. Your security architecture hasn't adopted Zero Trust

Legacy perimeter defenses and VPNs can't prevent lateral movement, insider threats, or third-party breaches.

Problem: Credential abuse and internal movement go undetected

Business Impact: Escalation of privileges, ransomware spread, compliance failure

Example: A global logistics company was breached through an employee's VPN credentials. Once inside, the attacker accessed critical billing data over weeks.

C1 + Palo Alto Fix:

ZTNA 2.0 ensures user and device trust is revalidated continuously

C1 Advisory Services assess maturity, define segmentation policy, and guide phased Zero Trust adoption

5. Your detection rules don't evolve with the threat landscape

Static signatures, rules, and threat models quickly become outdated.

Problem: Emerging threats bypass traditional detection methods

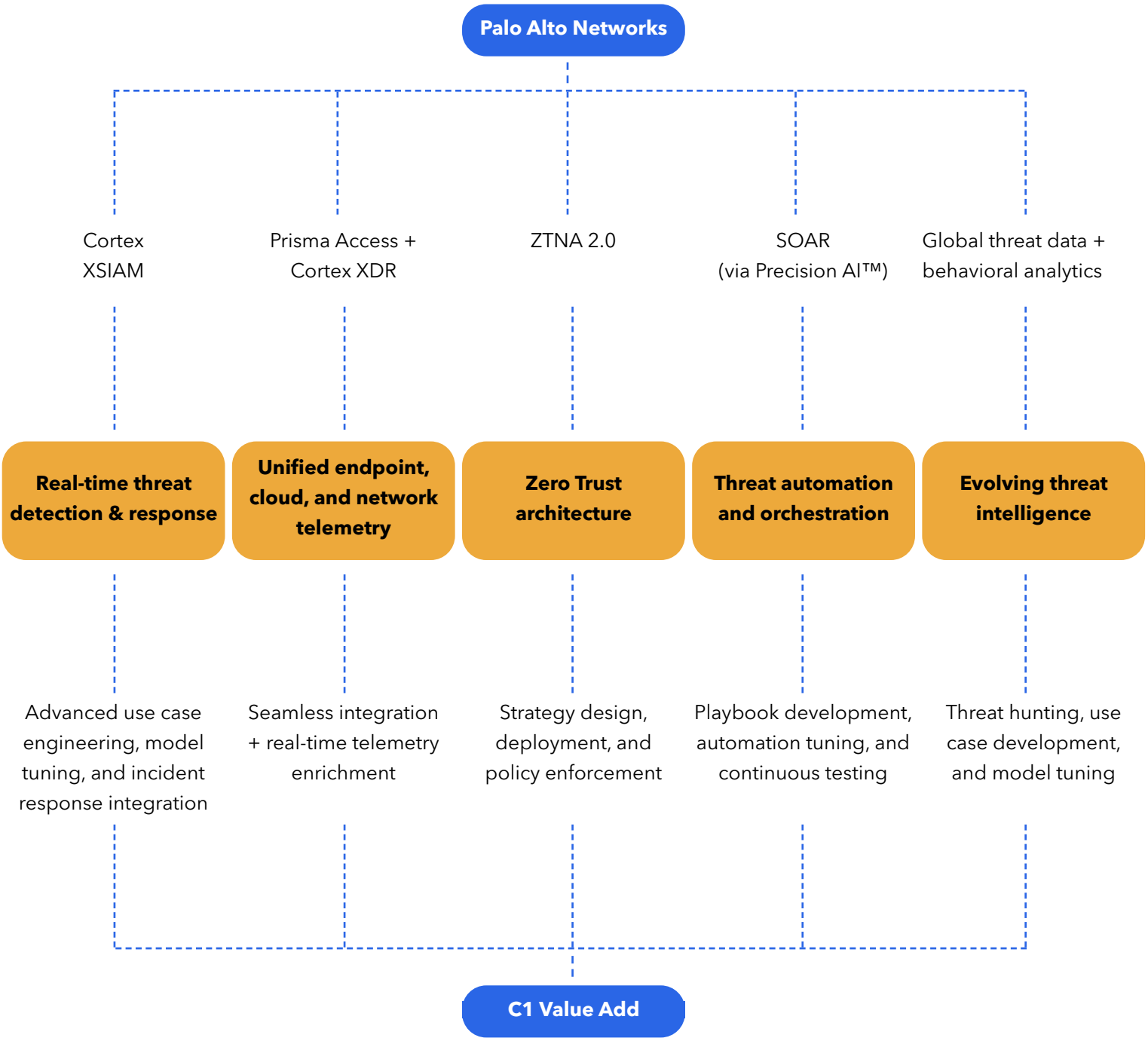
Business Impact: Missed attacks, ineffective patch prioritization, growing risk

Example: An attacker leveraged AI-based evasion to manipulate a rule-based antivirus system. The breach persisted for months.

C1 + Palo Alto Fix:

Precision AI™ continuously learns from billions of global threat signals

What a Modern, AI-Ready Security Stack Looks Like



C1 Services That Power Your AI Readiness

Advisory Services

- Security posture and AI readiness assessments
- Zero Trust strategy and maturity planning
- Business-aligned roadmap for automation and compliance

Value: Helps stakeholders align risk, compliance, and technology goals—before transformation begins.

Professional Services

- Deployment of Palo Alto Networks' AI-powered platforms
- Cloud-to-endpoint integration and configuration
- Policy and playbook creation tailored to your threat landscape

Value: Rapid deployment and reduced friction—minimizing complexity and ensuring operational alignment.

Managed Services

- Firewall Managed Services with advanced policy management and reporting
- Prisma Access Managed Services for secure access and cloud-delivered enforcement
- Ongoing configuration tuning, compliance alignment, and telemetry monitoring

Value: Enterprise-grade protection and simplified management—ideal for resource-constrained security teams needing continuous oversight without adding headcount.24/7 SOC operations with human-led + AI-enhanced defense.

Real-World Outcomes with C1 + Palo Alto Networks

Organizations that modernized with C1 and Palo Alto have achieved:

98% reduction

in mean-time-to-response (MTTR)

92% accuracy

in detecting malicious activity using Precision AI™

$1.76M cost savings

per breach with AI-driven automation (IBM)

50% fewer

false positives post SOAR deployment and tuning

88% improvement

in visibility across hybrid environments (ESG Research)

Faster audit readiness

and compliance validation with integrated reporting

AI is the Future of Cybersecurity—Is Your Stack Ready?

The pace of cybercrime has changed—your defenses must evolve to match. Manual processes, siloed tools, and perimeter-based architectures simply can't keep up with AI-powered attackers.

Modern enterprises need:

- ✓ Real-time visibility across cloud, endpoint, and network
- ✓ Automated triage, containment, and response
- ✓ Zero Trust enforcement and segmentation
- ✓ Continuous optimization driven by analytics and AI
- ✓ A partner to help them design, deploy, and manage it all

That's where C1 and Palo Alto Networks come in.

Get started today

C1 brings the people and processes to unlock the full potential of Palo Alto's industry-leading technology. Whether you're evaluating your current stack or ready to transform, we help you move faster, reduce risk, and stay ahead of what's next.

CONTACT US

C1 is a global leader in technology solutions known for elevating connected human experiences. With a comprehensive portfolio of services and deep expertise, C1 helps organizations across industries leverage cutting-edge technology to drive growth, enhance efficiency, and unlock new possibilities.