Zero Trust Made Real: C1 Security Services with Palo Alto Networks

Enforce least privilege. Validate continuously. Protect everywhere.

Zero trust. Expertly delivered.

Today's enterprises face relentless attacks that exploit excessive access, lateral movement, and blind spots in digital environments. Traditional perimeter-based defenses can no longer protect users, workloads, and data distributed across cloud, remote, and hybrid workforces.

That's why C1 and Palo Alto Networks have partnered to deliver a fully managed, practical approach to Zero Trust Security—powered by intelligent automation and backed by 24/7 operational expertise.

C1 makes Zero Trust a reality by integrating Palo Alto's leading technologies—NGFWs, Prisma Access, Cortex XDR, Cloud Identity Engine, and more—into your environment with seamless design, deployment, and managed protection. From user authentication to workload segmentation, we help you enforce least-privilege access policies across every digital surface.

The C1 advantage: Practical Zero Trust in action

Unified access control across users and devices

- Enforce Zero Trust policies at every access point using Palo Alto NGFWs and Prisma Access.
- Implement adaptive identity-based access through Cloud Identity Engine and App-ID™.
- Validate every user, device, and application before granting access.

Least privilege enforcement for workloads and applications

- Use Prisma Cloud and Microsegmentation to restrict East-West traffic and enforce policy boundaries.
- Gain real-time visibility into cloud workloads and prevent privilege creep across SaaS and infrastructure.

Continuous monitoring with AI-based enforcement

- Leverage Cortex XDR™ and XSIAM™ for real-time monitoring, behavior analytics, and rapid containment.
- Automate threat detection, correlation, and response across all telemetry.

Managed Zero Trust journey

- C1 delivers a step-by-step Zero Trust implementation plan—tailored to your priorities and environment.
- Services include architecture design, technology integration, managed detection and response, and ongoing optimization.

Policy automation and threat prevention

- Deploy Panorama™ for centralized Zero Trust policy control across distributed environments.
- Integrate Cortex XSOAR™ to automate workflows and accelerate response to policy violations or threats.

Core solution components

Network & access security

- **Palo Alto NGFW:** Identity- and application-aware firewall enforcement
- **Prisma Access (SASE):** Secure remote and mobile access with policy enforcement
- **Panorama™:** Centralized configuration and control

Identity & access management

- **Cloud Identity Engine:** Unified user and device identity for Zero Trust policies
- **App-ID™ & User-ID™:** Granular application and identity-based controls
- **Duo Security (optional):** MFA for Zero Trust Network Access

Cloud & workload protection

- **Prisma Cloud:** Code-to-cloud risk visibility and workload protection
- **Microsegmentation:** Enforce least-privilege at workload level
- **SaaS Security Posture Management (SSPM):** Monitor misconfigurations and policy drift

Threat detection & automation

- **Cortex XDR™:** AI-based endpoint detection and response
- **Cortex XSOAR™:** Orchestrated Zero Trust policy enforcement and incident response
- **XSIAM™:** Autonomous SOC operations with real-time analytics

Secure access

- **Prisma Access Secure Browser:** Isolated, cloud-delivered browser that enables secure access to web apps without exposing endpoints to risk
- Prevents browser-based threats like malicious scripts, phishing payloads, and session hijacking
- Ideal for unmanaged or BYOD devices, contractors, and third-party access use cases and seamlessly integrates with existing Zero Trust policies and identity providers

C1 Zero Trust journey: From strategy to execution

1. **Assess:** Evaluate identity, access, and workload exposures
2. **Design:** Architect your Zero Trust framework around your environment
3. **Deploy:** Integrate Palo Alto solutions with C1-managed implementation
4. **Manage:** Offload detection, policy enforcement, and monitoring to C1
5. **Refine:** Continuously optimize controls and maintain policy hygiene

Why choose C1 + Palo Alto for Zero Trust?

- **Integrated Zero Trust stack:** Built on best-in-class Palo Alto security platforms
- **End-to-end expertise:** Strategy, implementation, and 24/7 operations
- **Faster time to protection:** Accelerated rollout without burdening internal teams
- **Measurable risk reduction:** Least privilege enforcement and attack surface control
- **Flexible delivery models:** OPEX-based pricing and modular design

Get started today

Ready to bring Zero Trust to life across your enterprise? Speak with a C1 security expert and discover how we make Zero Trust practical, scalable, and secure.

Request a Zero Trust Consultation: OneC1.com/security-experience/ztastrategicprogram