

Competitive Analysis of Onclave TrustedPlatform in the Zero Trust Security Market

Contents

Summary Narrative	1
Security Analysis: Identifying Competitive Advantages of Onclave TrustedPlatform	2
Conclusion.....	4
Competitive Comparison Table	5

Summary Narrative

In the rapidly evolving landscape of cybersecurity, Zero Trust Architecture (ZTA) has emerged as a pivotal strategy for safeguarding digital assets against sophisticated threats. Onclave Networks' **TrustedPlatform** distinguishes itself in this competitive market by offering a purpose-built, system-agnostic solution that seamlessly integrates with existing infrastructures without incurring substantial costs or deployment times. Unlike many competitors that often rely on bundled or generalized security features, the TrustedPlatform is meticulously engineered to provide robust protection across all layers of IP communications, including IT, IoT, OT, and SCADA systems.

Key differentiators of the Onclave TrustedPlatform include its **Layer 2 encryption**, ensuring that data transmissions remain invisible to unauthorized monitoring tools, thereby mitigating common interception tactics employed by malicious actors. Additionally, the platform's **Dynamic Network Refactoring** capabilities empower organizations with advanced network management tools to adapt in real-time to emerging threats and operational demands. The TrustedPlatform's **Federal Government Authority to Operate (ATO)** and **FIPS 140-3 certification** underscore its compliance with stringent security standards, making it a trusted choice for government and enterprise sectors alike.

Furthermore, the TrustedPlatform's **quantum compliance**, validated by the USAF, future-proofs organizations against the impending challenges posed by quantum computing advancements. Its seamless integration with leading SIEM tools such as Dragos, Claroty, and Dark Trace enhances threat detection and response mechanisms, providing comprehensive visibility and monitoring across diverse network environments. By enabling rapid deployment through its overlay capability, Onclave ensures that organizations can achieve an enhanced security posture swiftly, saving both time and financial resources.

When compared to leading competitors like BeyondTrust, CrowdStrike, Palo Alto Networks, Zscaler, Twingate, Nozomi Networks, Fortinet, and others, Onclave TrustedPlatform not only

matches but often surpasses their offerings in critical areas of federal compliance, security features, and operational efficiency. This positions Onclave as a superior choice for organizations seeking a resilient, flexible, and certified Zero Trust solution tailored to their unique security needs.

Security Analysis: Identifying Competitive Advantages of Onclave TrustedPlatform

1. BeyondTrust:

- **Potential Security Holes:** BeyondTrust primarily focuses on privileged access management. While it offers comprehensive ZTA features, its integration depth across various network layers may be limited.
- **Onclave Advantage:** The TrustedPlatform's **Layer 2 encryption** and **system-agnostic overlay capability** provide a more pervasive security layer that BeyondTrust lacks, ensuring broader protection across all IP communications.

2. CrowdStrike Falcon ZTA:

- **Potential Security Holes:** CrowdStrike excels in endpoint protection but may have vulnerabilities in securing data in transit and at rest across diverse network environments.
- **Onclave Advantage:** With its **enclave-based data protection** and **Layer 2 encryption**, the TrustedPlatform ensures data security both in transit and at rest, addressing potential gaps in CrowdStrike's ZTA implementation.

3. Palo Alto Networks Prisma Access:

- **Potential Security Holes:** Prisma Access is heavily cloud-centric, which might pose challenges for organizations with on-premises or hybrid environments.
- **Onclave Advantage:** The TrustedPlatform's **system-agnostic nature** and **ease of deployment as an overlay** make it more adaptable to various infrastructure setups, offering on-premise flexibility that Prisma Access may not provide.

4. Zscaler:

- **Potential Security Holes:** Zscaler focuses on secure web and application access, potentially overlooking comprehensive network-level encryption.
- **Onclave Advantage:** Onclave's **Layer 2 encryption** ensures that all IP communications are secured, providing a more holistic approach to network security beyond just web and application layers.

5. Twingate:

- **Potential Security Holes:** While Twingate offers secure remote access and application control, it may not provide extensive network management capabilities.
- **Onclave Advantage:** The **Dynamic Network Refactoring** of the TrustedPlatform offers advanced network management tools that enhance overall security posture, a feature where Twingate falls short.

6. Nozomi Networks Guardian:

- **Potential Security Holes:** Nozomi specializes in industrial network threat detection but may not offer comprehensive ZTA features for broader IT environments.
- **Onclave Advantage:** TrustedPlatform's **quantum compliance** and **layer 2 encryption** provide superior security for both industrial and general IT environments, ensuring versatility beyond Nozomi's niche focus.

7. Palo Alto Networks Cortex:

- **Potential Security Holes:** Cortex offers robust IoT security but may integrate its features in a way that lacks the unified, purpose-built architecture of Onclave.
- **Onclave Advantage:** The TrustedPlatform's **purpose-built Zero Trust architecture** ensures that all security features are seamlessly integrated and optimized for performance, unlike Cortex's more modular approach.

8. Fortinet:

- **Potential Security Holes:** Fortinet's solutions like FortiGate and FortiEDR are comprehensive but may require significant hardware investments and complex deployments.
- **Onclave Advantage:** The TrustedPlatform's **overlay deployment** minimizes hardware costs and simplifies the integration process, offering cost and time efficiencies that Fortinet's solutions might not achieve as effectively.

Conclusion

The **Onclave TrustedPlatform** stands out in the Zero Trust security market through its unique combination of federal certifications, comprehensive security features, and superior performance and integration capabilities. Its **Layer 2 encryption, system-agnostic overlay deployment, and quantum compliance** not only meet but exceed the offerings of leading competitors, addressing potential security vulnerabilities and operational inefficiencies inherent in other solutions. For organizations seeking a robust, flexible, and certified Zero Trust platform, Onclave TrustedPlatform offers unmatched advantages that ensure both current and future security needs are comprehensively met.

Competitive Comparison Table

Feature Category	Onclave TrustedPlatform	BeyondTrust	CrowdStrike Falcon ZTA	Palo Alto Networks Prisma Access	Zscaler	Twingate	Nozomi Networks Guardian	Palo Alto Networks Cortex	Fortinet
Federal Approvals									
- Authority to Operate (ATO)	Yes	No	No	No	No	No	No	No	No
- FIPS 140-3 Certification	Yes	No	No	No	No	No	No	No	No
Security Features									
- Zero Trust Architecture	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
- Granular Access Control	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
- Continuous Authentication	Yes	Limited	Yes	Yes	Yes	Yes	Limited	Yes	Yes
- Micro-segmentation	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
- Least Privileged Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
- Zero Trust Network Access	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
- Visibility & Monitoring	Comprehensive	Comprehensive	Comprehensive	Comprehensive	Comprehensive	Comprehensive	Comprehensive	Comprehensive	Comprehensive
Performance and Integration									
- System Agnostic Nature	Yes	Limited	Limited	Limited	Limited	Yes	Limited	Limited	Limited
- Ease of Deployment (Overlay)	Rapid overlay capability	Traditional deployment models	Integrated within suite	Cloud-centric deployment	Cloud-centric deployment	Cloud-native, easy setup	Integrated within suite	Integrated within suite	Traditional deployment models
- Cost and Time Savings	High (overlay, minimal costs)	Moderate	Moderate	Moderate	Moderate	High (quick deployment)	Moderate	Moderate	Moderate
Additional Features									
- Quantum Compliance	Yes	No	No	No	No	No	No	No	No
- Layer 2 Encryption	Yes	No	No	No	No	No	No	No	No
- Dynamic Network Refactoring	Yes	No	No	No	No	No	No	No	No