Comparing Zscaler and Onclave TrustedPlatform: A Comprehensive Overview of Zero Trust Security Solutions

Introduction

In today's rapidly evolving digital landscape, traditional network security models like the "castle and moat" approach are no longer sufficient to protect against sophisticated cyber threats. Organizations are under increasing pressure to implement Zero Trust cybersecurity solutions that assume no user or device is inherently trustworthy, whether inside or outside the network perimeter.

This article provides a high-level comparison of two prominent cybersecurity platforms: **Zscaler** and **Onclave TrustedPlatform®**. Zscaler is renowned for its comprehensive cloud security offerings, while Onclave TrustedPlatform introduces innovative technologies such as Dynamic Network Refactoring (DNR), quantum resistance, and blockchain-based identity management. Our goal is to outline each platform's features and capabilities, highlighting how they support the implementation of Zero Trust security principles, to assist you in making an informed decision that aligns with your organization's cybersecurity needs.

Zscaler Overview

Zscaler offers a suite of cloud-based security services designed to secure enterprise traffic comprehensively. Key features include:

- **Secure Web Gateway (SWG):** Provides robust inspection and filtering of web traffic, blocking malicious content before it reaches users or the network.
- **Zero Trust Network Access (ZTNA):** Implements identity-based security policies, device posture checks, and least-privileged access to applications, aligning with Zero Trust principles.
- **Cloud Security Posture Management (CSPM):** Helps monitor and manage security posture in cloud environments, crucial for organizations with significant cloud deployments.
- **Deployment Considerations:** Integration with existing infrastructure can be complex, potentially leading to higher initial setup costs and longer deployment times.

Onclave TrustedPlatform Overview

Onclave TrustedPlatform emphasizes Zero Trust security through innovative technologies. Key features include:

- **Dynamic Network Refactoring (DNR):** The first and only Zero Trust platform that enables dynamic movement between secure enclaves while maintaining Zero Trust controls.

- **Blockchain-Based Identity Management:** Utilizes blockchain technology for identity verification, ensuring identity data is immutable and tamper-proof, enhancing security beyond traditional identity systems.
- **Continuous Trust Validation:** Performs a constant check of the protected devices within the defined enclaves against the trusted signatures at the time they were protected.
- **Zero Trust Access Controls:** Enforces access based on rigorous verification of identity, device health, and other contextual factors, embodying the essence of Zero Trust principles.
- **Deployment Considerations:** Designed to overlay existing networks with minimal disruption, offering simplicity and ease of integration.

Key Differences and Advantages

1. Zero Trust Implementation

- **Onclave TrustedPlatform** adopts a comprehensive Zero Trust approach, leveraging a continuous trust validation, cryptographic microsegmentation, DNR, and blockchain technologies to ensure the highest levels of secure communications throughout the network.
- **Zscaler** integrates Zero Trust principles within its broader security framework, providing identity-based policies and least-privileged access, though it may not offer the same level of microsegmentation as Onclave.

2. Flexibility and Deployment

- **Onclave** offers a plug-and-play solution that can be overlaid on existing networks with minimal changes, appealing to organizations seeking a straightforward path to Zero Trust.
- **Zscaler** requires integration into its cloud-based ecosystem, which may involve more extensive planning and resource allocation for deployment.

3. Cost Considerations

- **Onclave** positions itself as a cost-effective solution, potentially attractive to organizations mindful of budget constraints or seeking scalability without proportional cost increases.
- **Zscaler's** pricing may reflect its broad suite of services, and costs can vary depending on customization and the specific needs of the organization.

4. Third-Party Validation and Certifications

- **Onclave** has obtained a Federal Government Authority to Operate (ATO), indicating compliance with stringent security standards applicable to sensitive government operations.
- **Zscaler** holds FedRamp High certification and various other certifications and industry recognitions; however, specific validations related to Zero Trust in government contexts may differ from those of Onclave.

5. Approach to VPN and Traditional Security Models

- **Onclave** inherently designs its solution around Zero Trust principles, providing nuanced and segmented security models that go beyond traditional VPN offerings.
- **Zscaler** offers VPN capabilities, but reliance on traditional VPN technologies may not fully align with Zero Trust principles, as VPNs can create broad network perimeters lacking granular controls.

Conclusion

Both Zscaler and Onclave TrustedPlatform offer robust cybersecurity solutions, but they differ in their approaches to implementing Zero Trust principles. **Onclave** stands out for its innovative use of DNR and blockchain technology, providing a high level of network isolation and identity assurance. This may offer a more streamlined path to Zero Trust for organizations seeking significant security enhancements.

Zscaler remains a formidable player with a comprehensive suite of cloud-based security services, suitable for enterprises invested in extensive cloud usage and seeking security across multiple vectors. The choice between the two platforms may depend on factors such as your organization's existing infrastructure, future security strategy, and budget considerations.

Organizations are encouraged to assess their specific needs and priorities to determine which solution aligns best with their cybersecurity objectives. By carefully evaluating the features and capabilities of both platforms, you can make an informed decision to enhance your organization's security posture in today's challenging digital environment.

Table of Comparison: Zscaler – vs- The TrustedPlatform

Capability/Feature set	Zscaler	The TrustedPlatform
Zero Trust Maturity	ZTNA capabilities integrated within a broader security framework	Purpose-built Zero Trust architecture with continuous verification
Third-Party Validation	No, Industry-wide ZTNA standards	Yes, Federal Government - Zero Trust Authority to Operate (ATO)
Network Segmentation	Access controls via ZTNA – communications, VPNs which do not meet Zero Trust Standards	Microsegmentation dynamic and isolated network environments – using DNR
Zero Trust Access Controls	Least privilege access based on identity and device posture	Strict Zero Trust MFA principles enforced using blockchain Identity Management
VPN Limitations	Still allows VPN technologies which do not fully align with Zero Trust	VPNs can operate within the TrustedPlatform communications tunnels to achieve full Zero Trust implementation
Third-Party Validation	Federal Government - FedRamp High	Federal Government - Zero Trust Authority to Operate (ATO) – White House Communications Office & Defense Health
Customer Profile	Large enterprises with complex network security needs	Organizations seeking a transformative approach to network security
Scalability	Highly scalable through its cloud platform	Designed for scalability with minimal operational overhead
Cost-Effectiveness	Pricing varies by configuration, can be high for full feature access	Enterprise size starting at less than $10 per device per year
Capability	Zscaler	Onclave TrustedPlatform
Zscaler	Zscaler	Zscaler
Onclave TrustedPlatform	Onclave TrustedPlatform	Onclave TrustedPlatform
Core Technology	Core Technology	Core Technology
Cloud-based security platform	Cloud-based security platform	Cloud-based security platform
Dynamic Network Refactoring (DNR)	Dynamic Network Refactoring (DNR)	Dynamic Network Refactoring (DNR)
Zero Trust Maturity	Zero Trust Maturity	Zero Trust Maturity
ZTNA capabilities integrated within a broader security framework	ZTNA capabilities integrated within a broader security framework	ZTNA capabilities integrated within a broader security framework

Capability/Feature set	Zscaler	The TrustedPlatform
Purpose-built Zero Trust architecture with continuous verification	Purpose-built Zero Trust architecture with continuous verification	Purpose-built Zero Trust architecture with continuous verification
Deployment	Deployment	Deployment
Cloud-based deployment with potentially complex integration	Cloud-based deployment with potentially complex integration	Cloud-based deployment with potentially complex integration
Overlay network with minimal infrastructure changes, easy deployment	Overlay network with minimal infrastructure changes, easy deployment	Overlay network with minimal infrastructure changes, easy deployment
Identity Management	Identity Management	Identity Management
Traditional identity providers, supports multiple IDPs	Traditional identity providers, supports multiple IDPs	Traditional identity providers, supports multiple IDPs
Blockchain-based identity management for enhanced security and immutability	Blockchain-based identity management for enhanced security and immutability	Blockchain-based identity management for enhanced security and immutability
Network Segmentation	Network Segmentation	Network Segmentation