

What if enterprises could leverage
advanced technology employed by the U.S.
Department of Defense and Intelligence
Community to run and protect their critical
assets?

...and get to **Zero Trust** at scale,
quickly and in a cost-effective way?



Onclave's Approach to Supply Chain Secure Communications

Securing the Chain: The Imperative Role of Onclave in DoD Supply Chain Security

Introduction

The landscape of cybersecurity threats is evolving, with supply chain attacks becoming a focal point for adversaries aiming to infiltrate high-value targets like the DoD. The SolarWinds and Ivanti incidents underscore the vulnerabilities of current security practices, emphasizing the need for a modern, secure, and resilient approach to protecting sensitive communications within the DoD supply chain.

The Challenge: Escalating Supply Chain Threats

Supply chain attacks exploit third-party vendors as entry points to access an organization's primary network. The SolarWinds breach, which affected numerous US government agencies, and the Ivanti VPN software vulnerability, which disrupted DoD operations, exemplify the critical risks associated with these attacks. These incidents reveal the inadequacies of traditional security solutions and the pressing need for enhanced measures.

DoD's Response: CMMC 2.0

In response to these escalating threats, the DoD is implementing the Cybersecurity Maturity Model Certification (CMMC) 2.0, mandating contractors adopt stringent cybersecurity practices. However, CMMC 2.0 solutions that incorporate existing solutions, such as VPNs, are proving insufficient in meeting the demands of this new security landscape.

Onclave's Solution: A Paradigm Shift in Security

Onclave's TrustedPlatform® introduces a groundbreaking Zero Trust Security model tailored for supply chain communications. This platform integrates advanced technologies, including blockchain and identity security, to offer a comprehensive security solution that addresses the following:

Unmatched Security: With industry-leading certifications, Onclave's platform is designed to withstand a range of cyber threats, including those from quantum computing.

Zero Trust Architecture: Onclave minimizes inherent trust, rigorously verifying every access attempt, thus providing a more secure environment than traditional VPNs.

CMMC 2.0 Compliance: The platform ensures adherence to the latest cybersecurity standards, aligning with CMMC 2.0 requirements.

Future-Proof Design: Onclave's adaptable, protocol-agnostic platform ensures compatibility with existing infrastructure, offering a sustainable security solution.

Conclusion: Onclave as the Keystone of DoD Supply Chain Security

Onclave's TrustedPlatform® is the perfect solution for the Department of Defense (DoD) to revolutionize secure communications within its supply chain. This Zero-Trust-Based comprehensive platform offers unparalleled protection against supply chain attacks, ensures the safety of sensitive information, and upholds the integrity of national security operations. By choosing Onclave's TrustedPlatform®, the DoD can confidently navigate the complexities of modern cybersecurity, guaranteeing a fortified and reliable defense mechanism for its critical operations.

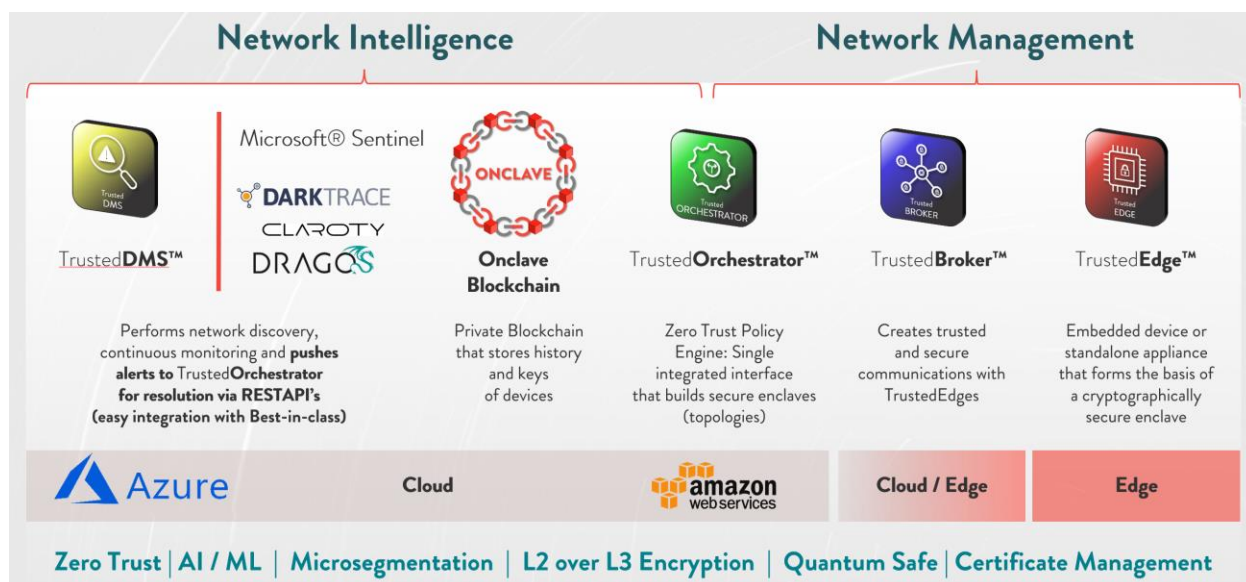


Figure 1 The Intelligent, Zero Trust Network (ATO PENDING)