

Protect Your Business with the Highest Security Standard You've Never Heard Of

Executive Summary

For integrators and business leaders unfamiliar with the term “ATO”, this paper highlights how adopting such a federally endorsed solution can fortify your organization's defenses against sophisticated cyber threats. This paper aims to illuminate the significance of the Authority to Operate (ATO)—the federal government's most stringent security standard—and how Onclave Networks' TrustedPlatform leverages this certification to offer unparalleled cybersecurity advantages not found elsewhere in the commercial market.

What Is the Authority to Operate (ATO)?

The Authority to Operate (ATO) indicates that a system has undergone exhaustive testing, often spanning several years, and complies with the strictest federal cybersecurity standards. Unlike commercial certifications such as ISO/IEC 27001 or SOC 2, which focus on procedural adherence and security practices, the ATO involves comprehensive risk management and authorization processes unique to federal protocols. Once awarded there are ongoing reviews and testing to maintain the ATO certificate.

Unparalleled Testing: The ATO process rigorously examines every aspect of a platform's security, including architecture, functionality, resilience to cyberattacks, and ability to maintain secure operations in dynamic threat environments. This level of scrutiny surpasses any equivalent certification in private industry, ensuring that systems are equipped to handle sophisticated and advanced cyber threats that are often beyond the scope of standard commercial security measures. From HVAC, doors, medical device to manufacturing and robots.

Exclusive Recognition: Being issued an Authority to Operate (ATO) is a significant achievement that underscores an organization's commitment to the highest standards of cybersecurity. An ATO is the federal government's most rigorous security endorsement, indicating that a system has undergone exhaustive testing and comprehensive risk assessments unique to federal protocols. This distinction goes beyond standard commercial certifications; it signifies that the system is trusted to protect the nation's most sensitive data against sophisticated cyber threats. Achieving an ATO not only validates the system's resilience and compliance

with stringent federal requirements but also sets the organization apart as a leader in cybersecurity excellence—a distinction not commonly found in the private sector.

Why Does This Matter to Commercial Integrators and Business Leaders?

For those in the private sector who may not be aware of the ATO's value, leveraging a solution that has met these rigorous federal standards offers unmatched cybersecurity benefits:

- **Unrivaled Security Levels:** The ATO-certified solutions provide a level of cybersecurity not available elsewhere in the commercial market, protecting against threats that solutions such as ISO 27001, 15408 and SOC 2 may not cover.
- **Independent Validation:** The ATO serves as an independent validation, by the federal government, of a platform's security capabilities, assuring that it can withstand both current and future sophisticated attack threats.
- **Cost-Effective Implementation:** The TrustedPlatform overlays current networks without the need for a complete infrastructure overhaul, utilizing existing hardware and aligning with business processes rather than requiring network rebuilds.
- **Market Differentiation:** Utilizing an ATO-certified solution differentiates your organization as one that prioritizes the highest possible security standards, enhancing reputation and trust among clients and partners.

Onclave's TrustedPlatform

The Onclave TrustedPlatform® is a purpose-built Zero Trust Architecture (ZTA) solution developed from first principles to provide secure communications. It represents a significant advancement in cybersecurity technology, designed to meet and exceed the demands of today's complex threat landscape—offering security levels not found elsewhere in the private sector.

Zero Trust Implementation

Onclave TrustedPlatform adopts a comprehensive Zero Trust approach, leveraging continuous trust validation, cryptographic microsegmentation, and blockchain technologies for identity management to ensure the highest levels of secure communications throughout the network.

Strategic Advantage

First Zero Trust solution to secure an ATO from the Defense Health Agency and the White House Communications Agency, providing a level of credibility and trust unmatched in the commercial market.

Verified as quantum-resistant, future-proofing your organization's security infrastructure.

What Makes the TrustedPlatform Unique?

1. **Zero Trust, Purpose-Built:** Unlike competitors who retrofit existing solutions to align with Zero Trust concepts, the TrustedPlatform was engineered from the ground up to meet Zero Trust principles, providing a more robust and effective security posture.
2. **Dynamic Network Refactoring (DNR):** It is the first and only Zero Trust platform that enables dynamic movement between secure enclaves while maintaining Zero Trust controls, offering flexibility without compromising security.
3. **Blockchain-Based Identity Management:** Utilizes blockchain technology for identity verification, ensuring identity data is immutable and tamper-proof, enhancing security beyond traditional identity systems often found in the private sector.
4. **Continuous Trust Validation:** Performs constant checks of protected devices within defined enclaves against trusted signatures at the time they were protected, ensuring ongoing integrity.
5. **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.
6. **Ease of Integration and Cost Efficiency:** Designed to overlay existing networks with minimal disruption, the TrustedPlatform can be implemented using existing hardware, eliminating the need for costly "rip and replace" cybersecurity upgrades. Overlays can be tailored to match business processes rather than requiring a network rebuild, simplifying deployment and reducing operational costs.

Cost-Effective Security

One of the most significant advantages of the TrustedPlatform is its cost-effectiveness:

- **Affordable Licensing:** Retail pricing starts at \$22 per protected device per year, and enterprise levels drop to as low as \$10 per device, the TrustedPlatform offers an economical solution without compromising on security.
- **No Need for Infrastructure Overhaul:** By overlaying existing networks and utilizing current hardware, organizations avoid the substantial costs associated with infrastructure replacement.
- **Alignment with Business Processes:** Overlays can be designed to match business processes, not just network architecture, ensuring that security measures integrate seamlessly with operational workflows.

Implications for the Commercial Market

For commercial organizations, adopting the TrustedPlatform means leveraging a solution that is certified to protect the nation's valuable communications. Tested and proven to meet the highest security standards—levels of security not available through any other commercial cybersecurity solutions.

Unmatched Differentiation

ATO distinction provides a competitive edge that other commercially available solutions can't claim. This sets a new benchmark in cybersecurity, offering private sector organizations the opportunity to adopt federal-level security measures without significant financial burden or operational disruption.

Conclusion

Harness top-tier cybersecurity from government to business without replacing your existing infrastructure. Onclave Networks offers a strategic advantage with its TrustedPlatform—a solution that not only meets but exceeds stringent federal standards.

By recognizing the value of an Authority to Operate (ATO) certification and implementing a platform certified at this level, integrators and commercial business leaders can access unparalleled cybersecurity capabilities. TrustedPlatform overlays existing networks, leverages current hardware, and aligns with established business processes—all at a cost-effective price—making it an attractive and practical solution for enhancing security without disrupting operations.

Embracing Onclave's TrustedPlatform is more than adopting new technology; it's about elevating your organization's defense mechanisms to a level previously unattainable in the private sector, while ensuring seamless and cost-efficient integration.