TD SYNNEX intel Trust Authority

Put Zero Trust Within Reach and Offer Public Cloud Flexibility with Private Cloud Security

Data is one of your customer's biggest assets. They should be able to trust the systems that run it.

When datasets contain sensitive information or intellectual property, or are subject to heightened compliance, enterprise organizations may require workloads and environments to be verified by a third party that is operationally independent from the infrastructure provider. To solve this requirement, Intel is introducing a zero-trust, SaaS approach to attestation, rooted in silicon and scalable across multiple workloads and cloud environments—regardless of who provides the infrastructure.

Security Threats: By the Numbers

^50%
Increase in 2021 cyberattacks YoY

93%
Networks at risk of cyberattack

277 days
Average time to detect and contain a data breach

$4.35M
Average cost of a single data breach in 2021

2s
Pace of new ransomware attacks by 2031

$458.9B
Projected global cybersecurity spending by 2025

Introducing a Consistent, Independent, Scalable Attestation Service

Intel Trust Authority is a new portfolio of software and services that brings enhanced security and assurance to Confidential Computing with Zero Trust principles.

In its first generation, Intel Trust Authority offers an independent attestation service that attests to Trusted Execution Environments (TEEs) that are based on (Intel® SGX) and (Intel® TDX). This single, consistent attestation process provides assurance to any relying party that the TEE and any data and workloads within it have not been compromised.

Intel Trust Authority's attestation service operates independently of the cloud or edge infrastructure provider that hosts your confidential computing workloads. It's cloud-agnostic and designed to work across on-premises, hybrid, and multi-cloud environments.

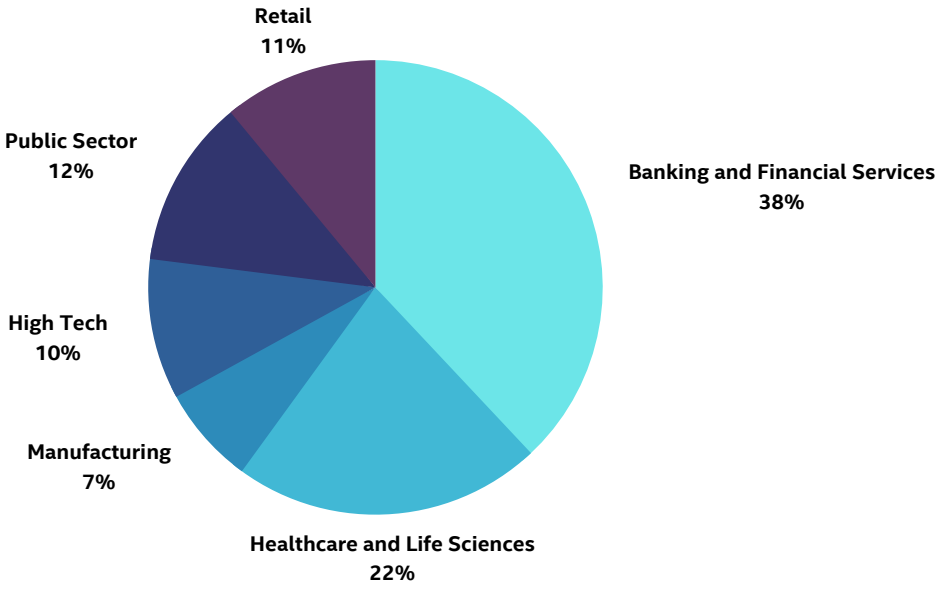
You can configure and maintain security policies consistently across cloud deployments without having to build and maintain an expensive and complex attestation service.

MARKET OPPORTUNITY

Confidential Computing Market Forecast

The cybersecurity market is projected to experience an explosive compound annual growth rate of 65% from 2021 to 2026, expanding from $2 billion to a projected $24 billion.

Resellers have a prime opportunity to tap into this rapid market growth, offering Intel's cutting-edge security solutions to meet the escalating demand for robust cyber protection.



Qualifying an Opportunity

Key Opportunities

Zero-Trust access is ranked as one of the top challenges when managing access to infrastructure; only 21% of critical infrastructure organizations have deployed a Zero-Trust approach.

Hybrid cloud is the most preferred cloud deployment model (36%). 68% of organizations want a deployment of security software both on cloud and on-premises.

NEXT STEPS

Leverage TD SYNNEX Intel

Need additional Trust Authority training or sales strategies?

Reach out to the TD SYNNEX Intel team at IntelSoftwareUS@tdsynnex.com for all of your needs and opportunities.

Qualifying Questions

- What are your current top security concerns?
- What workloads are you currently prioritizing? Do those workloads include sensitive data and if so, are you concerned about migrating those workloads due to visibility and security?
- Is your organization making new investments in technology or adopting new policies that are focused on regulatory compliance around data?
- What are the current requirements to meet regulatory compliance with any of your applications or services?
- Is your organization evaluating a strategy around data sovereignty and making sure your data is under your control, even in the cloud?
- What is your organization's stance on Zero Trust architecture? Is it an active area of investment or research?
- Are you investing in, or researching, any privacy preserving technologies such as secure multi-party computing? Do you have a need to securely collaborate with other organizations or third parties?
- Have you heard of confidential computing?