INVARY

Runtime Integrity

PARTNER ENABLEMENT GUIDE

The Consultative Problem Statement

The security tools your customer has invested in are the right decisions. Their endpoint protection, threat detection platform, and SOC operations represent serious, well-reasoned investments that are doing exactly what they were built to do.

But every one of those tools operates on one assumption they were never designed to verify: that the systems running them are actually telling the truth about what is happening. Sophisticated adversaries are not trying to break through security anymore. They are going underneath it.

When that happens, the security investment is not just ineffective. It is actively working against the customer, generating confident alerts and clean reports based on data that has been corrupted at the source. The tools are working perfectly. They are working on a lie.

THE PROBLEM

"Your security tools are solid investments. They work exactly as designed. But attackers now go underneath them, compromising the systems your entire stack depends on and persisting invisibly."

THE SOLUTION

"Invary does not replace your tools. It makes them trustworthy. A lightweight sensor continuously verifies each system's state against a certified baseline, catching tampering or changes. Your existing security investments keep working. Now on a foundation you can trust."

THE LINE THAT LANDS

"Your tools are working exactly as designed, but they cannot see what is underneath them, and an attacker who controls that layer controls what your tools see."

INVARY

THE ROI ANCHOR

- Invary closes the exposure window where attacks are undetected, which is 35% of attacks.
- Average dwell time without verification: 212 days. Invary cuts that to hours.
- Avoiding even a single breach, or a single day of operational disruption, covers the cost of Runtime Integrity many times over.

“How Does It Work?”

Each system is measured against a baseline built from published repositories, not from the live system. The verification runs off-system, so an attacker who has already compromised the environment cannot tamper with the measurement or the result.

Invary’s Runtime Integrity is built on technology exclusively licensed from the NSA, the same approach used to protect the most sensitive computing environments in the U.S. government.

Invary co-authored the MITRE Continuous Remote Attestation Framework, the emerging open standard that defines continuous runtime verification as a security architecture requirement.

“Tell Me More”

Every dollar invested in security tools operates on one assumption: that the systems being monitored report what is happening honestly. When an attacker compromises the system at its foundation, that assumption is wrong. The SIEM never sees the events actually taking place. The EDR monitors a system that has been modified to control what it sees. The SOC team monitors an environment the attacker now influences and controls.

AI has lowered the barrier to these attacks by an order of magnitude in the last 18 months. The capability that was once limited to nation-state actors is becoming broadly available. The Department of Defense and Intelligence Community have already implemented Runtime Integrity, because they cannot afford to have their security investments neutralized at the foundation.

INVARY

Objection Handling

"Our EDR would catch that."

It is designed to catch only what it already knows about. The question is, "Does your EDR detect what hasn't been previously seen?" If the system underneath the tooling has been modified, EDR is executing its detection logic on inputs the attacker controls. Invary verifies that the system is in the state it should be in, independently of what it reports to your tools.

"We already have a full security stack."

That is exactly why this matters. Every technology in your security architecture depends on the systems underneath them being trustworthy. Invary does not replace any of it. It makes all of it reliable and verifies it is working properly.

"How is this different from EDR or XDR?"

Detection tools find and report what they know about. Invary verifies. It does not look for attack patterns or use signatures. It confirms whether the system is still in the known-good state it was built to be in. That is a different question, and it is the one your detection tools were never designed to ask.

"What is the integration lift?"

Lightweight sensor deployment. No rip and replace. No displacement of existing tools. No reboots on install, updates, or removal. Invary integrates as a verification trust layer beneath them, with flexible cloud, on-premise, or hybrid deployment.

"Who else is using it?"

The Intelligence Community, Department of Navy, and organizations across legal, telecom, and where regulation & compliance are requirements. These are environments whose security investments cannot afford to operate on an unverified foundation.

NOTE: Never let this conversation feel like a critique of their security decisions. The right frame: their tools are doing exactly what they were built to do. The gap is not a flaw in those tools. It is beneath them.

INVARY

Vertical Quick-Reference

The messaging on the preceding pages works across all verticals. The cards below add industry-specific context that ties Runtime Integrity to outcomes the customer cares about.

Transportation and Logistics

Validate integrity, expose hidden threats, and keep freight moving.

THREAT HOOK

Transportation consistently ranks among the most-attacked industries worldwide. Ransomware operators target TMS platforms, dispatch systems, and telematics gateways because a single compromise can strand freight across an entire network. An attacker who controls the foundation beneath your security stack can halt operations while every dashboard reports normal.

SYSTEMS INVARY PROTECTS

- TMS and dispatch platforms
- WMS, yard, and terminal operations
- Telematics gateways and fleet edge devices

COMPLIANCE

TSA Security Directives, C-TPAT, CMMC, ISO 28000, SOC 2

BUSINESS IMPACT LINE

"One network-wide outage costs more than years of Runtime Integrity. Invary finds what your detection tools were never built to see, before freight stops moving."

Manufacturing

Validate integrity, expose hidden threats, and keep lines running.

THREAT HOOK

Manufacturing has been the most-attacked industry for four years running. Attackers monetize production downtime. When a system compromise reaches the plant floor, the result is line-down events, scrapped product, and missed shipments. Detection tools that depend on compromised systems report clean while production stops.

SYSTEMS INVARY PROTECTS

- MES and production control systems
- Historians and engineering workstations
- IT/OT gateways and edge servers

COMPLIANCE

CMMC, NIST 800-171, IEC 62443, SOC 2, ISO 27001

BUSINESS IMPACT LINE

"One line-down event costs more than years of Runtime Integrity. Invary verifies the foundation before attackers pivot from enterprise IT to the plant floor."

INVARY

Commodities

Validate integrity, expose hidden threats, and keep product flowing.

THREAT HOOK

Energy and commodities rank among the most-attacked critical infrastructure sectors. The dual exposure of financial trading and physical delivery creates compounding risk: frozen trades, halted pipelines, failed settlements. An attacker with persistent access to trading or scheduling systems can cause damage that cascades from the trading desk to the terminal.

SYSTEMS INVARY PROTECTS

- ETRM/CTRM trading and risk platforms
- Scheduling, nominations, and logistics systems
- Pipeline, terminal, and storage operations

COMPLIANCE

NERC CIP, TSA Pipeline Directives, SOX audit, SOC 2, ISO 27001

BUSINESS IMPACT LINE

"One halted trading or delivery day costs more than years of Runtime Integrity. Invary verifies the systems that clear trades and move product."

Telecommunications

Validate integrity, expose hidden threats, and protect essential services.

THREAT HOOK

Salt Typhoon infiltrated nine major U.S. telecom companies in 2024, maintaining undetected access for months using living-off-the-land techniques that blended into normal operations. Traditional detection tools never identified the compromise. For telecom providers, a security failure is not a business inconvenience. It is a disruption to essential services that communities depend on. Nation-state actors are specifically and persistently targeting this sector.

SYSTEMS INVARY PROTECTS

- Network management and subscriber data systems
- Edge and core infrastructure
- Operations support and business support systems (OSS/BSS)

COMPLIANCE

FCC cybersecurity requirements, TSA Security Directives, SOC 2, ISO 27001

BUSINESS IMPACT LINE

"Salt Typhoon proved that detection tools miss nation-state persistence in telecom environments. Invary is the class of control that would have exposed it."

INVARY

Legal Services

Validate integrity, expose hidden threats, and protect client confidentiality.

THREAT HOOK

Law firms are custodians of extraordinarily sensitive client information: pending M&A transactions, patent filings, litigation strategy, and privileged communications. The legal sector recorded a record number of ransomware attacks in 2024, and the FBI issued a specific advisory in 2025 identifying threat groups targeting U.S. law firms. For legal organizations, the risk is compounded by professional obligation: ABA Model Rule 1.6(c) requires "reasonable efforts" to protect client information. A firm that cannot verify the integrity of its systems faces both a security risk and a professional liability exposure.

SYSTEMS INVARY PROTECTS

- Document management and practice management platforms
- Privileged file servers and client data repositories
- Email and communications infrastructure

COMPLIANCE

ABA Model Rule 1.6(c), SOC 2, state bar data protection requirements

BUSINESS IMPACT LINE

"One compromise of privileged client data is a security incident, a professional liability exposure, and a reputation event. Invary verifies the foundation before any of those become real."

Financial Services

Validate integrity, expose hidden threats, and protect the systems that move money.

THREAT HOOK

Financial institutions operate under intense regulatory scrutiny and face attackers who target the systems where a single compromise can halt trading, freeze settlements, or trigger regulatory penalties. The convergence of real-time transaction processing, sensitive customer data, and strict compliance obligations creates an environment where unverified system integrity is not just a security risk but a regulatory and fiduciary one.

SYSTEMS INVARY PROTECTS

- Core banking and payment processing platforms
- Trading systems and settlement infrastructure
- Customer data repositories and digital banking platforms

COMPLIANCE

SOX, PCI DSS 4.0, FFIEC guidance, NYDFS cybersecurity regulation, SOC 2

BUSINESS IMPACT LINE

"One undetected compromise of a trading or payment system creates cascading financial, regulatory, and reputational damage. Invary verifies the foundation those systems depend on."

INVARY

Healthcare

Validate integrity, expose hidden threats, and protect patient safety.

THREAT HOOK

Healthcare is among the most-targeted sectors and carries the highest average breach cost of any industry. Ransomware attacks on hospitals and health systems do not just compromise data. They disrupt clinical operations, delay treatment, and put patient safety at risk. The systems that manage electronic health records, medical devices, and clinical workflows operate in environments where an undetected compromise can have consequences that extend beyond financial loss.

SYSTEMS INVARY PROTECTS

- Electronic health record (EHR) platforms
- Medical device gateways and clinical networks
- Pharmacy, lab, and imaging system infrastructure

COMPLIANCE

HIPAA Security Rule, HITECH Act, SOC 2, NIST CSF, state health data privacy laws

BUSINESS IMPACT LINE

"Healthcare carries the highest breach cost of any industry. When the compromise reaches clinical systems, the cost is measured in patient safety, not just dollars. Invary verifies the systems that cannot afford to be silently compromised."

SLED (State, Local, and Education)

Validate integrity, expose hidden threats, and protect the systems citizens depend on.

THREAT HOOK

State and local governments and school districts manage critical citizen data with some of the smallest security teams and tightest budgets in any sector. Ransomware operators target SLED organizations precisely because limited staff means longer dwell times and higher pressure to pay. The systems that manage student records, tax data, benefits, elections, and emergency services cannot afford to operate on an unverified foundation.

SYSTEMS INVARY PROTECTS

- Citizen-facing portals and records management
- Student information systems and administrative platforms
- Elections infrastructure and public safety systems

COMPLIANCE

CIS Controls, StateRAMP, CJIS Security Policy, FERPA, NIST CSF

BUSINESS IMPACT LINE

"SLED organizations need a force multiplier, not another tool that requires a team to manage. Invary delivers verification-grade assurance at a scale and cost that fits the public sector."

INVARY

Federal and Defense

Validate integrity, expose hidden threats, and protect the mission.

THREAT HOOK

Nation-state adversaries target federal and defense systems with the most advanced persistent access techniques available. AI-driven vulnerability discovery and exploitation at machine speed means that any system trusted today may carry unknown zero-days tomorrow. The Department of Defense and Intelligence Community have already implemented Runtime Integrity because they cannot afford to have their security investments neutralized at the foundation.

SYSTEMS INVARY PROTECTS

- Mission-critical and classified systems
- HPC and AI compute clusters
- Returning assets from foreign or untrusted environments

COMPLIANCE

CMMC, NIST 800-171, FedRAMP, ATO, CNSSI 1253, DISA STIGs

BUSINESS IMPACT LINE

"Invary is deployed across the Intelligence Community, Department of Navy, Five Eyes partners, and defense primes including RTX and Lockheed Martin. This is proven where the mission cannot fail."