



The Literal Cost of Seconds: Quantifying ROI in the Era of Industry 5.0

Shifting from Reactive Cybersecurity to Proactive Revenue Assurance with EmberNet

By: Eric Seme

I. Executive Summary

The industrial cybersecurity landscape in 2026 is defined by a single, uncomfortable truth: **a security breach is no longer a data loss event—it is a physical stoppage of the economic engine.** The convergence of AI-driven threats, expanding attack surfaces via Industrial IoT (IIoT), and the stubborn persistence of legacy Operational Technology (OT) hardware has rendered traditional IT-centric security models dangerously inadequate.

For a plant manager in Detroit, a breach doesn't mean stolen credit card numbers. It means \$50,000 per minute in halted throughput. For a pharmaceutical operations director in New Jersey, it means a \$1 million batch of product destroyed because a temperature sensor was manipulated for eleven minutes. For a water utility operator in a rural county, it means an EPA investigation and potential public health crisis.

This white paper presents the **EmberNet ROI Framework**, a methodology for calculating the **literal dollar loss** of a security breach based on an organization's specific industry, operational profile, and market size. By quantifying the cost in terms that operations leaders, CFOs, and board members understand—revenue lost per second, batches destroyed, fines accrued per day—we move the cybersecurity conversation from abstract "risk mitigation" to concrete **Revenue Assurance**.

The core finding is this: while generic Zero-Trust architectures reduce security incidents by 50%, EmberNet's defense-in-depth platform compounds four independently hardened layers—**EmberOS** (immutable endpoint OS, 70% attack surface reduction), **Ember Flux**

(dark Zero-Trust Networking, 99.99% API surface reduction), **Crucible** (hardened network firewall with OS diversity), and **hardened K3s containers** (workload isolation with 95.8% lateral movement prevention)—to architecturally eliminate the attack paths that cause the majority of industrial breaches. EmberNet doesn't detect breaches faster. It ensures the attack path does not exist. For many industrial operators, EmberNet pays for itself the moment it prevents just **70 seconds** of unplanned downtime.

II. The Changing Landscape of Industrial Risk

The Velocity of Production

The global manufacturing economy in 2026 runs on speed. Just-in-Time (JIT) manufacturing, lean inventory models, and tightly coupled supply chains have created extraordinary efficiency—but also extraordinary fragility. A single point of failure on the digital side can cascade into millions of dollars of physical loss within minutes.

Consider the modern automotive assembly line. Every component arrives precisely when it is needed. There is no warehouse buffer. When a ransomware attack encrypts the Manufacturing Execution System (MES), the line doesn't just slow down—it stops completely. And because of JIT dependencies, that stoppage ripples upstream and downstream through the entire supply chain. Tier 1 suppliers miss delivery windows. Dealerships lose allocation. The financial damage compounds exponentially with each passing hour.

This is the **Cost-Velocity Gap**: the widening chasm between the speed at which production generates revenue and the speed at which a cyber event destroys it. In 2026, that gap has never been wider.

The Convergence of IT and OT

For decades, IT (Information Technology) and OT (Operational Technology) existed as separate domains. IT managed email, ERP systems, and databases. OT managed Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and Human-Machine Interfaces (HMIs). They were air-gapped—physically disconnected from each other and from the internet.

That air gap is gone.

The rise of IIoT, cloud-based analytics, remote monitoring, and predictive maintenance has connected millions of previously isolated OT devices to corporate networks and the broader internet. A temperature sensor in a food processing plant now feeds data to a cloud dashboard. A PLC controlling a chemical valve can be configured remotely. A robotic welding cell streams performance telemetry to an AI optimization engine halfway around the world.

Each of these connections is a potential attack vector. And unlike IT systems—which are regularly patched, updated, and hardened—many OT devices run on decades-old firmware with no encryption, no authentication, and no ability to be updated without shutting down the entire production process.

The Lateral Movement Trap

Traditional firewall-based security models assume a clear perimeter: keep the bad actors out, and the inside stays safe. In the converged IT/OT environment, this assumption is fatally flawed.

The typical attack pattern in 2026 follows a predictable path:

2. Lateral Movement: From the IT network, the attacker traverses to the OT network through shared credentials, flat network architectures, or misconfigured firewalls. This phase accounts for an estimated **70% of total breach costs** in industrial environments.

3. Payload Delivery: Once on the OT network, the attacker can encrypt SCADA workstations (ransomware), manipulate sensor readings (sabotage), or exfiltrate proprietary process data (espionage).

The critical failure point is Phase 2. In environments without microsegmentation or Zero-Trust enforcement, a single breached sensor or workstation provides a highway to every PLC, HMI, and safety system on the network.

Regulatory Pressure in 2026

The regulatory environment has caught up to the threat landscape. Organizations operating in critical infrastructure and manufacturing now face a multi-layered compliance burden:

Here you go:

Regulation	Sector	Key Requirement	Penalty for Non-Compliance
SEC Cyber Disclosure Rules	All publicly traded	Material incidents disclosed within 4 business days	Enforcement actions, shareholder lawsuits
NERC CIP v7+	Energy & Utilities	Mandatory security controls for Bulk Electric System	Up to \$1M per day per violation
CMMC 2.0	Aerospace & Defense	Certified maturity model for DoD contractors	Loss of Authority to Operate (ATO) and contracts
HIPAA / HITECH	Healthcare	Protection of electronic Protected Health Information	\$100–\$50,000 per record, up to \$1.5M annually
FDA 21 CFR Part 11	Pharmaceuticals	Electronic records integrity and audit trails	Product recalls, consent decree, criminal prosecution

EPA / Clean Water Act	Water & Wastewater	Integrity of treatment process controls	\$60,000+ per day per violation
EU NIS2 Directive	All essential services (EU)	Risk management and incident reporting	Up to €10M or 2% of global turnover

Non-compliance is no longer a "risk to manage"—it is a **cost to calculate**. And in many cases, the fines alone exceed the cost of the breach itself.

III. The Industry-Specific Loss Matrix

A security breach does not cost the same across the industrial supply chain. The financial impact is determined by the **Loss Archetype** that dominates each sector. EmberNet's ROI model identifies three distinct archetypes that define the modern industrial risk landscape:

Loss Archetype	Definition	Primary Sectors
Throughput Velocity	Cost is driven by halted production output—fixed labor plus lost units per hour	Automotive, Electronics, Mining
Material Integrity	Cost is driven by destroyed or contaminated Work-in-Progress (WIP)	Pharma, Food & Bev, Chemicals
Regulatory Friction	Cost is driven by compliance fines, legal exposure, and public safety liability	Energy, Utilities, Water, Aerospace

The following sections detail the literal dollar-loss logic for each industry covered by the EmberNet ROI Calculator.

3.1 Automotive (High-Volume Manufacturing)

Loss Archetype: Throughput Velocity

The Pain Point: Just-in-Time (JIT) manufacturing means that a 60-minute stoppage does not just lose one hour of output—it ripples through the entire supply chain. Upstream suppliers miss delivery windows. Downstream assembly plants starve for components. Contractual penalties activate.

Metric	2026 Benchmark
Average cost per minute of line stoppage	\$50,000
Average cost per hour	\$3,000,000
Average total breach cost	\$4.6M
Mean time to identify a breach (industry avg)	197 days

Literal Loss Scenario: A ransomware attack encrypts the MES controlling two body-welding lines at a Tier 1 supplier. The lines are down for 4.5 hours while the incident response team isolates the infection and restores from backups. Direct downtime cost: **\$13.5 million**. The OEM customer activates penalty clauses for missed shipments: **\$2.1 million**. Total loss: **\$15.6 million**.

EmberNet Value: EmberNet's Zero-Trust Networking architecture eliminates the attack path entirely. The MES runs as a containerized workload on EmberNet's immutable OS, and ZTN enforces app-level authentication—the compromised VPN credential has no implicit trust to reach the MES. The ransomware payload never reaches the welding line controllers because the lateral movement path does not exist. Avoided loss: **\$15.6 million**.

3.2 Food & Beverage (Process Manufacturing)

Loss Archetype: Material Integrity

The Pain Point: Spoilage and food safety. If cooling systems, pasteurization sensors, or environmental monitoring are compromised, the organization does not just lose time—it loses the entire batch. Depending on the product, a single batch can represent hundreds of thousands of dollars in raw materials, energy, and labor.

Metric	2026 Benchmark
Average value of WIP per batch	\$250K–\$1M
Average total breach cost	\$1.8M
Regulatory recall cost (FDA Class I)	\$10M+
Cost of lost consumer trust (brand impact)	Incalculable

Literal Loss Scenario: An attacker gains access to the SCADA system monitoring pasteurization temperatures in a dairy plant. They subtly adjust the temperature setpoint by 3°F for a 45-minute window. The batch passes through the process appearing normal, but post-production testing reveals bacterial contamination. The entire production run—72,000 units already packaged and partially shipped—must be recalled. Cost of recall logistics, destroyed product, and FDA investigation: **\$4.2 million**. If the contaminated product reaches consumers: **litigation costs potentially exceeding \$50 million**.

EmberNet Value: EmberNet's immutable OS on the endpoint hardware ensures the SCADA workstation cannot be tampered with—the operating system is read-only and centrally orchestrated. ZTN enforces that only authenticated operators, from authorized devices, can access the pasteurization control interface. An attacker who compromises a network credential cannot see or reach the SCADA application. Avoided loss: **\$4.2 million minimum**.

3.3 Pharmaceuticals

Loss Archetype: Material Integrity + Regulatory Friction

The Pain Point: Pharmaceutical manufacturing is governed by FDA 21 CFR Part 11, which requires absolute data integrity and complete audit trails for all electronic records. A breach that compromises the integrity of batch records—even if production itself is unaffected—can result in an entire production lot being deemed "adulterated" and destroyed.

Metric	2026 Benchmark
Average cost per compromised batch	\$500K-\$2M
Average total breach cost	\$5.01M
Cost of FDA consent decree	\$100M+
Cost of re-validation after system compromise	\$1M-\$5M

Literal Loss Scenario: A supply-chain attack compromises a third-party software component used in a biologic manufacturing facility's environmental monitoring system. The attacker does not attempt ransomware—instead, they subtly alter historical temperature logs in the batch record database. During a routine FDA audit, the discrepancy is flagged. The FDA issues a Form 483 observation, which escalates to a warning letter. All batches produced during the compromised period (estimated at 6 months of undetected access) are quarantined. Total loss: **\$47 million** in destroyed product, re-validation costs, and legal fees.

EmberNet Value: EmberNet's containerized workload model isolates each application component. The third-party monitoring tool runs in its own container with no implicit network access to the batch record database. ZTN requires explicit, authenticated, per-application authorization, the compromised component simply cannot reach the database because it was never granted that path. The immutable OS prevents persistent rootkits or backdoors on the endpoint. Avoided loss: **\$47 million**.

3.4 Oil & Gas

Loss Archetype: Throughput Velocity + Regulatory Friction

The Pain Point: Oil and gas operations are characterized by high-value throughput, geographically dispersed assets, and safety-critical control systems. A breach targeting Safety Instrumented Systems (SIS) or pipeline SCADA can have catastrophic physical consequences in addition to financial ones.

Metric	2026 Benchmark
Average cost per hour of production stoppage	\$1M+
Average total breach cost	\$4.72M
Cost of pipeline incident (environmental)	\$100M+
Mean time to recover OT systems	21 days

Literal Loss Scenario: An attacker compromises an engineering workstation at a remote pipeline compressor station and uploads a modified program to the station's PLC, disabling the high-pressure safety interlock. The anomaly is not detected for 72 hours. While no physical incident occurs, once the modification is discovered, the entire pipeline segment must be shut down for safety audit and PLC re-verification. Downtime: 14 days. Direct revenue loss: **\$22 million** . Regulatory investigation and remediation: **\$8 million**.

EmberNet Value: EmberNet's ZTN ensures that the engineering workstation, even if compromised, cannot reach the PLC without authenticated, authorized access through the centrally orchestrated network policy. The attacker has no network path to the PLC—the connection is simply not available to unauthenticated sessions. The pipeline continues operating safely because the attack surface was architecturally removed. Avoided downtime: 14 days. Avoided loss: **\$30 million**.

3.5 Energy & Utilities

Loss Archetype: Regulatory Friction

The Pain Point: Electric utilities operating Bulk Electric System (BES) assets are subject to NERC CIP (Critical Infrastructure Protection) standards. Non-compliance fines can reach **\$1 million per day per violation** . Beyond fines, a successful attack on the grid has implications for public safety and national security.

Metric	2026 Benchmark
NERC CIP fine potential	\$1M per day per violation
Average total breach cost (energy sector)	\$4.78M
Cost of grid instability event	\$50M–\$500M
Days to remediate NERC CIP violation	60–180 days

Literal Loss Scenario: A NERC CIP audit discovers that an employee's compromised credentials were used to access a BES Cyber System from an unauthorized location 4 months prior. The utility self-reports, triggering an investigation. Fines for the access control violation: **\$500,000 per day for 120 days = \$60 million** . (Note: While the maximum is rarely applied in full, settlements routinely reach seven to eight figures.)

EmberNet Value: EmberNet's ZTN connects users directly to applications, not to the network. Stolen credentials are useless without the authorized device running EmberNet's immutable OS—the BES Cyber System is invisible to unauthorized endpoints. The access attempt never occurs because the application is not discoverable. Avoided fine exposure: **\$60 million.**

3.6 Healthcare

Loss Archetype: Regulatory Friction + Material Integrity (Patient Safety)

The Pain Point: Healthcare has been the costliest industry for data breaches for over a decade. But in 2026, the risk extends beyond Protected Health Information (PHI) to connected medical devices—infusion pumps, ventilators, imaging systems—that are increasingly networked and often running outdated operating systems.

Metric	2026 Benchmark
Average cost per compromised record	\$160
Average total breach cost	\$10.93M (highest of any industry)
Cost of life-safety IoT compromise	Litigation: \$10M–\$100M+
HIPAA fine per violation category	\$100–\$50,000 per record

EmberNet Value: EmberNet's containerized architecture and ZTN make clinical IoT devices invisible to the IT network. Even if the hospital's administrative systems are fully compromised, the attacker cannot discover or reach life-support and diagnostic devices—the network paths do not exist unless explicitly authorized through centrally orchestrated policy.

3.7 Chemicals

Loss Archetype: Material Integrity + Regulatory Friction

The Pain Point: Chemical manufacturing involves hazardous materials where a compromised process variable—temperature, pressure, flow rate—can cause an environmental release or explosion. The loss calculation includes physical damage, environmental remediation, regulatory fines, and potential loss of life.

Metric	2026 Benchmark
Average cost of process safety incident	\$1.2M per day
EPA fine for unauthorized release	\$100K+ per day
Average total breach cost	\$4.0M
Cost of facility shutdown for investigation	\$5M–\$50M

EmberNet Value: EmberNet's immutable OS on the process control endpoints prevents unauthorized software modifications at the hardware level. ZTN ensures that only authenticated engineering workstations can communicate with PLCs controlling hazardous processes—removing the lateral movement path that enables unauthorized setpoint changes.

3.8 Aerospace & Defense

Loss Archetype: Regulatory Friction + Intellectual Property

The Pain Point: Defense contractors must achieve CMMC 2.0 (Cybersecurity Maturity Model Certification) to maintain eligibility for Department of Defense contracts. Beyond

compliance, the exfiltration of controlled technical data—such as CNC machining files for proprietary components—represents an existential threat to competitive advantage.

Metric	2026 Benchmark
Average total breach cost	\$5.46M
Cost of losing CMMC certification	Loss of all DoD contracts
R&D sunk cost of exfiltrated IP	\$10M–\$500M
Average hourly cost of production stoppage	\$620,000+

EmberNet Value: EmberNet's immutable OS on CNC machines and design workstations prevents both unauthorized software installation and data exfiltration. ZTN enforces that these machines can only communicate with explicitly authorized internal endpoints—there is no outbound path to external infrastructure, even if a workstation is compromised. This architectural enforcement directly supports CMMC 2.0 certification requirements.

3.9 Semiconductors

Loss Archetype: Throughput Velocity + Material Integrity

The Pain Point: Semiconductor fabrication operates in cleanroom environments where atmospheric conditions—temperature, humidity, particulate count, vibration—are controlled to extreme precision. A cyber attack that subtly alters environmental sensor readings can ruin an entire wafer lot without any visible indication until post-fabrication testing.

Metric	2026 Benchmark
Average cost per hour of fab stoppage	\$1M–\$3M
Cost of cleanroom recertification	\$500K–\$2M
Average wafer lot value	\$1M–\$10M
Lead time to replace lost production	12–16 weeks

EmberNet Value: EmberNet's immutable OS on cleanroom control endpoints ensures that environmental sensor firmware and configuration cannot be tampered with. ZTN restricts access to cleanroom control systems exclusively to authenticated, authorized personnel and automation systems—eliminating the possibility of unauthorized parameter changes from compromised network positions.

3.10 Logistics & Third-Party Logistics (3PL)

Loss Archetype: Throughput Velocity

The Pain Point: Modern logistics operations are digital-first. Warehouse Management Systems (WMS), automated sortation, and fleet management platforms coordinate millions of shipments per day. A single distribution hub going offline doesn't just delay packages—it diverts thousands of shipments to competitors.

Metric	2026 Benchmark
Average cost per hour of hub outage	\$200,000+
Average total breach cost	\$3.9M
SLA penalty exposure per event	\$50K–\$500K
Customer churn rate post-breach	15–25%

EmberNet Value: EmberNet's ZTN makes the WMS and sortation systems invisible to the corporate IT network. There is no network path to pivot through—applications are only accessible to authenticated users on authorized devices running EmberNet's immutable OS. Even if an attacker fully compromises the office IT environment, the operational systems are architecturally unreachable.

3.11 Water & Wastewater Utilities

Loss Archetype: Regulatory Friction + Public Safety

The Pain Point: Water treatment facilities rely on Remote Terminal Units (RTUs) and PLCs to control chemical dosing (chlorine, fluoride, pH adjustment). Many of these systems are

decades old, run on legacy protocols, and are now connected to the internet for remote monitoring. An attacker who gains access to dosing controls can create a public health emergency.

Metric	2026 Benchmark
Average cost per hour of treatment disruption	\$100,000+
EPA fine per day of violation	\$60,000+
Cost of "boil water" advisory (public trust)	\$1M–\$5M
Average total breach cost	\$3.5M

Literal Loss Scenario: An attacker exploits a default password on an internet-facing HMI at a small municipal water utility. They increase the chlorine dosing setpoint by 200% for a 3-hour window overnight. The change triggers the high-limit alarm, but the alarm is routed to an unmanned control room and is not acknowledged for 2.5 hours. Emergency response, EPA investigation, public notification, and system remediation: **\$3.8 million** .

EmberNet Value: EmberNet wraps legacy PLCs and RTUs in a hardened perimeter—the immutable OS runs on the endpoint gateway hardware, and ZTN ensures the HMI is not internet-facing. The dosing controls are only accessible to authenticated operators on authorized devices. Default passwords become irrelevant because the application is invisible to unauthorized users. Avoided loss: **\$3.8 million** .

3.12 Mining & Metals

Loss Archetype: Throughput Velocity

The Pain Point: Modern mining operations increasingly rely on autonomous haul trucks, conveyor systems, and ventilation controls connected via private 5G or mesh networks. If the network goes down, the autonomous fleet stops—and each truck represents a **\$5 million asset** sitting idle.

Metric	2026 Benchmark
Average cost per hour of fleet stoppage	\$500,000+
Average total breach cost	\$4.1M
Cost of underground ventilation failure	\$1M+ (safety evacuation)
Private 5G network recovery time	4–24 hours

EmberNet Value: EmberNet's immutable OS runs directly on the endpoint hardware controlling the mesh network and autonomous fleet systems. ZTN enforces that fleet management applications are only accessible through authenticated, authorized connections—completely isolated from the corporate IT network by architecture, not by firewall rules that can be misconfigured.

3.13 Pulp & Paper

Loss Archetype: Throughput Velocity + Material Integrity

The Pain Point: Pulp and paper manufacturing is a continuous process. Unlike discrete manufacturing (where you can restart a machine), a continuous process must maintain specific conditions (temperature, pressure, speed) without interruption. An unplanned stop in a paper machine's dryer section causes a "paper break"—the web of paper tears and must be rethreaded, a process that can take **2–6 hours** .

Metric	2026 Benchmark
Average cost per hour of paper machine downtime	\$150,000+
Average time to clear a paper break	2–6 hours
Cost of dryer section restart	\$300K–\$900K
Average total breach cost	\$3.2M

EmberNet Value: EmberNet's immutable OS on dryer section control endpoints prevents unauthorized software or configuration changes at the hardware level. ZTN ensures that only authenticated process engineers from authorized workstations can modify drive control parameters—eliminating the risk of unauthorized speed or temperature changes that trigger catastrophic paper breaks.

3.14 Electronics Manufacturing

Loss Archetype: Throughput Velocity + Material Integrity

The Pain Point: PCB assembly and electronics manufacturing rely on high-precision robotics—pick-and-place machines, reflow ovens, automated optical inspection (AOI). Even minor disruptions to machine calibration can produce thousands of defective units before the issue is detected.

Metric	2026 Benchmark
Average cost per hour of SMT line stoppage	\$100,000+
Cost of defective production run (undetected)	\$500K–\$2M
Average total breach cost	\$3.8M
Customer penalty for quality escape	\$100K–\$1M

EmberNet Value: EmberNet's immutable OS on robotics control hardware ensures machine parameters cannot be modified by unauthorized software. ZTN restricts calibration and configuration access to authenticated engineering sessions only—protecting high-precision equipment from both external attackers and insider threats by making the control interfaces invisible to unauthorized users.

3.15 Financial Services

Loss Archetype: Regulatory Friction + Throughput Velocity

The Pain Point: While not a traditional "industrial" sector, financial services firms rely on high-speed transaction processing infrastructure—data centers, trading platforms, payment networks—where milliseconds matter and regulatory scrutiny is intense.

Metric	2026 Benchmark
Average cost per minute of trading system outage	\$100,000+
Average total breach cost	\$5.97M
SEC fine for late disclosure	\$1M–\$10M+
Average customer churn post-breach	5.9%

EmberNet Value: EmberNet's containerized workload model and ZTN ensure that trading and payment processing systems are only accessible to authenticated applications and

operators. The immutable OS prevents persistent compromise of data center endpoints, and centralized orchestration enables instant policy enforcement across the entire infrastructure—preventing lateral movement to critical transaction systems.

IV. The Market Size Logic: Survival vs. Stability vs. Scale

A \$4.4 million breach—the 2026 global average—is a profoundly different event depending on the size of the organization experiencing it. For a \$20 million manufacturer, it is a potential extinction event. For a \$20 billion enterprise, it is a bad quarter. The EmberNet ROI Calculator accounts for this disparity through three market-size models.

4.1 Small Market (SMB): The "Extinction" Model

Revenue Range: Under \$50 million

The Reality: Small and mid-size manufacturers typically lack redundant systems, dedicated security staff, and robust backup infrastructure. When a breach occurs, **100% of operations stop** until a third-party Managed Service Provider (MSP) or incident response firm resolves the issue.

The statistics are stark: **60% of small businesses fail within six months of a major cyber incident.** The reason is not the breach itself—it is the **Fixed Cost of Recovery**. Whether a company makes \$5 million or \$50 million in revenue, the cost of forensic investigation, legal counsel, notification, and system restoration is roughly the same: \$200,000–\$500,000 minimum. For a small manufacturer, this is the difference between survival and closure.

Formula:

$$L = (\text{Annual Revenue} \div 250 \text{ working days}) \times \text{Days of Outage} + \text{Fixed Recovery Costs}$$

Key Assumptions:

- 100% operational loss during breach
- No redundant systems
- Average outage duration: 7–21 days
- Fixed recovery costs: \$200K–\$500K
- Cyber insurance denial rate increasing (40% of claims disputed in 2025)

The Value Case: *"For the cost of one entry-level IT technician's salary, you get enterprise-grade edge protection that ensures you never have to tell your biggest customer you've been breached."**

Sample Calculation:

Input	Value
Annual Revenue	\$30,000,000
Revenue per working day	\$120,000
Days of outage	14
Lost revenue	\$1,680,000
Fixed recovery costs	\$350,000
Total Loss	\$2,030,000
EmberNet first-year cost (Starter tier: \$6K/yr + 50 nodes × \$200 hardware)	\$16,000
EmberNet ongoing annual cost	\$6,000
ROI if breach prevented (first-year basis)	12,588%

4.2 Mid-Market: The "Contractual Erosion" Model

Revenue Range: \$50 million to \$1 billion

The Reality: Mid-market firms are often Tier 2 or Tier 3 suppliers to large OEMs. Their biggest loss in a breach is not always the direct downtime—it is the **contractual consequences** . Large customers have Service Level Agreements (SLAs) with penalty clauses for delivery failures. More critically, a breach can cost a mid-market supplier its **"Preferred Supplier" status** , effectively ending a multi-year, multi-million-dollar relationship.

In 2026, major OEMs in automotive, aerospace, and electronics are increasingly requiring cybersecurity certifications (ISO 27001, CMMC, TISAX) as a condition of doing business. A breach is not just a financial event—it is a **qualification event** that can disqualify the supplier from future contracts.

Formula:

$$L = \text{Downtime Cost} + \text{SLA Penalty Fees} + \text{Customer Churn Value} + \text{Re-Qualification Cost}$$

Key Assumptions:

- 40% operational loss during breach (partial redundancy)
- SLA penalty flat fee: \$50K–\$500K per customer per incident
- Customer churn: 10–20% of revenue at risk
- Re-qualification cost (ISO/CMMC audit): \$100K–\$500K

The Value Case: *"EmberNet protects your reputation. It allows you to prove to Tier 1 customers that your facility meets 2026 Zero-Trust standards, making you a lower-risk partner."*

Sample Calculation:

Input	Value
Annual Revenue	\$250,000,000
40% operational loss × 5 days	\$1,370,000
SLA penalties (3 customers)	\$450,000
Customer churn (1 lost account)	\$3,500,000
Re-qualification costs	\$250,000
Total Loss	\$5,570,000
EmberNet first-year cost (Pro tier: \$18K/yr + 200 nodes × \$200 hardware)	\$58,000
EmberNet ongoing annual cost	\$18,000
ROI if breach prevented (first-year basis)	9,503%

4.3 Large Market (Enterprise): The "Systemic Decay" Model

Revenue Range: Over \$1 billion

The Reality: Enterprises have redundant systems, backup data centers, and dedicated security operations centers (SOCs). They rarely experience 100% operational failure. Instead, their losses manifest as **systemic decay** : stock price erosion that persists for months after the breach announcement, class-action lawsuits filed within days, regulatory investigations spanning years, and enterprise-wide remediation programs costing tens of millions.

In 2026, the SEC's 4-day "material incident" disclosure rule has added a new dimension: public market reaction. Studies show that breached companies experience an average **3.5% decline in stock price** in the week following disclosure, with recovery taking 6–12 months.

Formula:

$$L = (\Delta \text{ Stock Price} \times \text{Outstanding Shares}) + \text{Regulatory Fines} + \text{Incident Response (@ \$600/hr)} + \text{Litigation Reserves}$$

Key Assumptions:

- 10% operational loss during breach (redundancy absorbs most impact)
- Stock price impact: 3.5% decline (average)
- Regulatory fine baseline: \$1M+
- Incident response duration: 2,000–10,000 hours at \$600/hr
- Litigation reserves: \$5M–\$50M

The Value Case: *"Consolidate your fragmented OT security posture. EmberNet provides the unified visibility required for SEC 'Material Incident' reporting, NERC CIP compliance, and board-level risk dashboards."*

Sample Calculation:

Input	Value
Market Cap	\$8,000,000,000
Stock price erosion (3.5%)	\$280,000,000
Regulatory fines	\$5,000,000
Incident response (5,000 hrs × \$600)	\$3,000,000
Litigation reserves	\$15,000,000
Total Loss	\$303,000,000
EmberNet annual cost (Enterprise tier starting at \$5K/mo + server-grade hardware)	\$60,000+/yr (subscription)
ROI if breach mitigated by 50%	252,400% (at \$60K/yr base)

V. The EmberNet ROI Framework: The "Avoided Loss" Formula

The Architecture Gap

Traditional cybersecurity tools focus on **detection speed** —reducing the Mean Time to Identify (MTTI) and Mean Time to Contain (MTTC) a breach. These metrics matter, but they accept a flawed premise: that the attacker will get in, and the question is how fast you notice.

EmberNet takes a fundamentally different approach. Rather than a single security product, EmberNet is a **defense-in-depth platform** composed of four hardened technology layers, each with independently verified security benefits. The compound effect of these layers

operating together creates threat reduction far beyond what any single technology achieves alone.

The Four Layers of EmberNet

Layer 1: EmberOS — Immutable Operating System

EmberOS runs on the endpoint hardware as a read-only, immutable operating system. Critical system files cannot be modified—any change requires a complete image replacement with cryptographic verification, making unauthorized modifications immediately detectable and impossible to persist.

Metric	Published Benchmark
Attack surface reduction vs. mutable OS	70%
Configuration-related vulnerability reduction	72%
Security incidents from defective/malicious updates	58% reduction
Ransomware persistence capability	Eliminated (filesystem is read-only)

What this means: Rootkits, backdoors, and persistent malware—the tools attackers use to maintain access after initial compromise—are architecturally impossible. After every reboot, the system is guaranteed to be in its known-good state.

Layer 2: Ember Flux — Zero-Trust Networking

Ember Flux is a software-defined overlay network that connects authenticated users directly to authorized applications. Unlike traditional networks where services listen on open ports,

Ember Flux applications have **zero listening ports on the underlay network** . They are invisible to port scanners, network probes, and unauthorized users.

Metric	Published Benchmark
API attack surface reduction (dark networking)	99.99%
Service discoverability to unauthorized users	Zero (no listening ports)
Lateral movement via network scanning	Eliminated (nothing to discover)
VPN credential theft impact	Neutralized (credentials alone are insufficient)

What this means: The most common initial attack vector—scanning a network for open services and exploiting them—produces zero results. Applications only exist for authenticated users on authorized devices. An attacker with stolen VPN credentials cannot even see the target applications, let alone reach them.

Layer 3: Crucible — Network Appliance Firewall

Crucible runs on the physical network appliance hardware as a hardened firewall and traffic management layer. Critically, it runs a **completely different OS codebase** than EmberOS, providing genuine OS diversity across the stack.

Metric	Published Benchmark
Microsegmentation lateral movement prevention	87.3% (standalone)
Combined ZTA + microsegmentation prevention	95.8%
Zero-day cross-exploitation (different OS kernel)	Independent attack surface

What this means: Even in the unlikely event that an attacker discovers a kernel-level exploit for EmberOS, that exploit is useless against Crucible—and vice versa. The network layer and the compute layer are protected by different codebases, different package ecosystems, and different attack surfaces. This is genuine defense-in-depth, not marketing language.

Layer 4: Hardened K3s — Containerized Workload Isolation

All application workloads run in hardened Kubernetes (K3s) containers, isolated from each other and from the host OS. Combined with Ember Flux overlay networking; containers can only communicate with explicitly authorized services—there is no implicit pod-to-pod trust.

Metric	Published Benchmark
Exposed critical vulnerabilities with hardening	50% reduction
Blast radius of compromised workload	Single container (no lateral movement)
Container-to-host escape with immutable OS	No writable host to escape to

What this means: The dominant Kubernetes security risk—misconfiguration leading to lateral movement between pods—is eliminated by Ember Flux's per-application authorization. And even if a container escape vulnerability existed, the attacker lands on an immutable, read-only OS with no ability to persist or modify the system.

The Compound Effect

The generic industry benchmark for Zero-Trust architecture adoption is **50% fewer security incidents**. This figure represents organizations that have implemented ZTA in some form—typically identity policies layered on top of conventional, mutable infrastructure with traditional network architecture.

EmberNet's stack goes substantially further by eliminating entire categories of attack that generic ZTA still leaves open:

Attack Category	Generic ZTA	EmberNet (All 4 Layers)
Network scanning / service discovery	Reduced (firewall rules)	Eliminated (Ember Flux: zero listening ports)
Lateral movement	60% reduction	95.8% prevention (Crucible microsegmentation + ZTA)
Persistent malware / rootkits	Partially mitigated (EDR)	Eliminated (EmberOS: immutable filesystem)
Configuration drift / unauthorized changes	Monitored (SIEM)	Eliminated (EmberOS: 72% fewer config vulns)
Cross-layer exploitation	Single OS = single exploit chain	Dual OS diversity (EmberOS ≠ Crucible)
Container escape to host	Host is mutable / writable	Host is read-only (EmberOS: nowhere to persist)
Credential theft / VPN compromise	MFA + monitoring	Architecturally neutralized (Ember Flux: credentials alone insufficient, apps invisible)

The result is not an incremental improvement over generic ZTA. It is a **qualitative shift** in the threat model: the majority of attack vectors that produce the 50% residual incident rate in generic ZTA are architecturally eliminated in EmberNet.

Where Detection Still Applies

EmberNet's architectural prevention handles the dominant cost driver—lateral movement, which accounts for an estimated 70% of industrial breach costs. However, EmberNet also reduces the impact of the remaining scenarios: insider threats from authorized devices, social engineering of authenticated operators, and zero-day exploits against application logic (not the OS or network). In these cases, EmberNet's centralized orchestration provides visibility and audit logging that compresses detection and response timelines from the industry average of **266 days** to hours—because the blast radius is architecturally contained to a single container on a single node before any detection occurs.

The Formula

The EmberNet ROI is calculated as **Avoided Loss minus Solution Cost** , expressed as a

ROI = (Expected Loss – Mitigated Loss) – EmberNet Cost

EmberNet Cost

Where:

Expected Loss = The total calculated loss using industry-specific and market-size models, assuming no Zero-Trust architecture in place

Mitigated Loss = The reduced loss assuming EmberNet's architectural prevention (lateral movement path eliminated) and compressed containment for residual threat scenarios

EmberNet Cost = Annual subscription/deployment cost of EmberNet for the organization's footprint

Based on published 2026 ZTA benchmarks, organizations with fully deployed Zero-Trust architectures reduce their breach costs by an average of **\$1.51 million**. For organizations in high-downtime industries, the actual savings are significantly higher because the prevented downtime is worth more per minute than the cross-industry average.

The Payback Period

Perhaps the most compelling metric for budget-conscious decision-makers: **how quickly does EmberNet pay for itself?**

Industry	EmberNet Annual Cost (Pro Tier)	First-Year Total (w/ 200 nodes hardware)	Downtime Cost Per Minute	Minutes of Prevention to ROI
Automotive	\$18,000	\$58,000	\$50,000	1.16 minutes
Semiconductors	\$18,000	\$58,000	\$50,000	1.16 minutes
Oil & Gas	\$18,000	\$58,000	\$16,667	3.5 minutes
Pharma	\$18,000	\$58,000	1 batch = \$500K+	< 1 batch
Food & Bev	\$18,000	\$58,000	1 batch = \$250K+	< 1 batch
Energy (Fines)	\$18,000	\$58,000	\$694/min (\$1M/day)	1.4 hours of fine avoidance

Note: Hardware costs start at \$200/node for edge appliances and scale with application requirements. Ongoing annual cost after Year 1 is subscription only (\$18K/yr at Pro tier), making the payback period even shorter in subsequent years.

The "Aha!" Moment: EmberNet pays for itself if it prevents just **70 seconds of unplanned downtime** in an Automotive or Semiconductor environment, **one spoiled batch** in Pharma or Food & Bev, or **less than 90 minutes** of NERC CIP fine exposure. After Year 1, with hardware already deployed, the threshold drops to just **22 seconds** of prevented downtime at the Pro subscription rate.

VI. Case Study Scenarios

The following hypothetical scenarios illustrate the EmberNet ROI Framework applied to real-world conditions. While the company names are fictional, the cost benchmarks, attack vectors, and regulatory consequences are drawn from 2026 industry data.

Scenario A: Mid-Market Automotive Tier 2 Supplier

Company Profile: Precision stamping and welding, \$320M revenue, 1,200 employees, 3 plants

The Incident: A phishing email compromises an engineer's workstation on the corporate network. The attacker uses the engineer's VPN credentials to access the plant network and deploys ransomware targeting the MES servers at two of three facilities.

Without EmberNet	With EmberNet
Attack path: VPN → flat network → MES servers	Attack path: VPN credential useless—MES invisible to unauthenticated devices
Lines down: 2 plants × 4.5 hours	Lines down: 0 (lateral movement path does not exist)
Direct downtime cost: \$13.5M	Direct downtime cost: \$0
SLA penalties: \$2.1M	SLA penalties: \$0
Recovery & forensics: \$800K	Incident investigation: \$50K (IT-side credential compromise only)
Total: \$16.4M	Total: \$50K
	Avoided Loss: \$16.35M

Scenario B: Large-Scale Food Processor

Company Profile: National frozen food manufacturer, \$1.2B revenue, 8 production facilities

The Incident: A compromised IoT temperature sensor in a blast freezer at the company's largest facility reports normal temperatures while the actual freezer temperature rises above the safe threshold. The manipulation goes undetected for 6 hours during the overnight shift.

Without EmberNet	With EmberNet
Attack path: Compromised network → SCADA sensor interface	Attack path: Sensor control only accessible to authenticated operators on authorized devices
Product destroyed: 180,000 units	Product destroyed: 0
Recall logistics: \$1.8M	Recall: Not required
FDA investigation: \$400K	FDA notification: \$0
Brand damage (estimated): \$3M	Brand damage: \$0
Total: \$5.2M	Total: \$15K (investigation)
	Avoided Loss: \$5.185M

Scenario C: Small Municipal Water Utility

Company Profile: Serves population of 45,000, annual budget \$8M, 12 employees

The Incident: An attacker discovers a default password on the utility's internet-facing HMI (a common finding—over 40% of small water utilities still use default credentials on at least one system). The attacker accesses the chlorine dosing controls.

Without EmberNet	With EmberNet
Attack path: Internet → default password → HMI → PLC	Attack path: HMI not internet-facing; PLC only accessible via authenticated ZTN session
Emergency response: \$200K	Emergency response: \$0
EPA investigation & fines: \$1.2M	EPA: No incident to report
Public notification & testing: \$300K	Public impact: \$0
System remediation: \$180K	Remediation: Routine policy review: \$5K
Total: \$1.88M	Total: \$5K
	Avoided Loss: \$1.875M

For a utility with an \$8M annual budget, the unmitigated breach represents **23.5% of the entire annual operating budget**.

VII. The ROI Calculator: Design & Methodology

User Interface Flow

The EmberNet ROI Calculator is designed as a three-step interactive tool that produces a personalized "Avoided Loss" report.

Step 1: Company Profile (3 Inputs)

Industry — Dropdown selection from 15 industry categories

Company Size — Revenue range selector (Small / Mid / Large) or exact revenue input

Data Sensitivity — Toggle: "Do you store proprietary IP (blueprints, formulas)?" and "Do you store regulated personal data (PII, PHI)?"

Step 2: Incident Scenario

Downtime Slider — "Estimated length of full or partial operational disruption" (1 hour to 2 weeks)

Ransomware Toggle — "Was/would ransomware be involved?" (Adds \$1M–\$5M recovery premium based on market size)

Regulatory Exposure Toggle — "Are you subject to industry-specific compliance mandates?" (Activates regulatory multiplier)

Step 3: The EmberNet Offset (Results)

Side-by-side comparison:

- **Scenario A (Current State):** Open network architecture with implicit trust. Total calculated loss.
- **Scenario B (With EmberNet):** Zero-Trust architecture—attack paths architecturally eliminated. Reduced loss.

- Key Metrics Displayed:

- Total Avoided Loss
- ROI Percentage
- Payback Period (in minutes, hours, or batches)
- "Live Counter" — A real-time dollar ticker running at the organization's cost-per-second rate, creating urgency while the user reviews the report

The Psychological "Cost of Silence"

The results page includes a **real-time loss ticker**. Once the user enters their data, a counter begins running at their industry's cost-per-second rate. While they read the report, the "Current Loss" display climbs steadily—e.g., **+\$833/second** for Automotive. This visual device creates the psychological urgency necessary to convert a security evaluation into a purchase decision.

VIII. Strategic Recommendations

For CISOs and Security Leaders

1. **Quantify your risk in operational terms.** Translate "threat landscape" briefings into dollars-per-minute for your board. The EmberNet ROI Calculator provides the data model to make this translation.
2. **Audit your IT/OT boundary.** The lateral movement phase accounts for 70% of total breach cost in industrial environments. If your OT network can be reached from your IT network through implicit trust (shared credentials, flat VLANs, firewall rules), your exposure is orders of magnitude higher than your risk assessment suggests. A hardened PaaS with ZTN eliminates these paths by architecture.
3. **Validate your cyber insurance.** In 2026, insurers are increasingly denying claims when basic security controls are absent. Deploying edge-level detection and microsegmentation may be a prerequisite for maintaining coverage.

For Plant Managers and Operations Leaders

1. **Calculate your cost-per-minute.** This number—fixed labor plus lost throughput plus material at risk—is the single most important input for any cybersecurity business case.
2. **Identify your "crown jewels."** Which systems, if compromised for 10 minutes, would cause the most damage? Safety systems? Batch records? Autonomous fleet controllers? These are the systems that need edge-level protection first.
3. **Integrate security into operational metrics.** Unplanned downtime caused by a cyber event should be tracked with the same rigor as downtime caused by mechanical failure.

For CFOs and Board Members

1. **Treat cybersecurity as Revenue Assurance, not IT overhead.** The ROI framework presented in this paper demonstrates that edge-level security is not an expense—it is an investment with a measurable, often extraordinary return.
2. **Understand the non-linearity of risk.** A \$2M security investment that prevents a \$16M breach is not a 1:8 ratio—it is the difference between a stable quarter and a crisis that consumes executive attention for a year.
3. **Demand the Payback Period.** Any security vendor should be able to articulate, in minutes or dollars, how quickly their solution pays for itself in your specific operational environment.

IX. Conclusion: The Cost of a Second

In the 2026 industrial landscape, "cybersecurity" is a misnomer. For the organizations that design, build, process, generate, and distribute the physical goods and services that the world depends on, the correct term is **Revenue Assurance**.

The thesis of this paper is simple: **the literal dollar loss of a security breach can be calculated, and the ROI of preventing that breach is extraordinary.**

Whether you are a \$30 million stamping shop where a breach threatens your survival, a \$300 million food processor where it threatens your largest customer relationship, or a \$3 billion utility where it threatens regulatory action and public safety—the calculus is the same. The cost of an open attack path is measured in seconds. The value of eliminating that path is measured in millions.



EmberNet exists to **remove the attack surface entirely** deploying an immutable operating system on endpoint hardware, enforcing Zero-Trust Networking that connects authenticated users directly to applications, and providing centralized orchestration that ensures consistent security policy across every facility. The result is not faster detection. It is the architectural elimination of the lateral movement paths that account for 70% of industrial breach costs.

The only remaining question is: how many seconds can you afford to lose?

X. Appendix: 2026 Industry Benchmark Data Tables

A. Downtime Cost by Industry

Industry	Cost/Minute	Cost/Hour	Cost/Day
Automotive	\$50,000	\$3,000,000	\$72,000,000
Semiconductors	\$16,667–\$50,000	\$1M–\$3M	\$24M–\$72M
Oil & Gas	\$16,667	\$1,000,000	\$24,000,000
Aerospace & Defense	\$10,333	\$620,000	\$14,880,000
Mining & Metals	\$8,333	\$500,000	\$12,000,000
Logistics & 3PL	\$3,333	\$200,000	\$4,800,000
Pulp & Paper	\$2,500	\$150,000	\$3,600,000
Chemicals	\$1,250+	\$75,000+	\$1,200,000+
Electronics Manufacturing	\$1,667	\$100,000	\$2,400,000
Financial Services	\$100,000+	\$6,000,000+	\$144,000,000+
Healthcare	\$167–\$250	\$10K–\$15K	\$240K–\$360K
Water & Wastewater	\$1,667	\$100,000	\$2,400,000
Food & Beverage	Per batch: \$250K–\$1M	—	—
Pharma	Per batch: \$500K–\$2M	—	—
Energy & Utilities	Fines: \$694/min	Fines: \$41,667/hr	Fines: \$1,000,000/day

B. Average Total Breach Cost by Industry (2026)

Industry	Average Total Breach Cost
Healthcare	\$10.93M
Financial Services	\$5.97M
Pharmaceuticals	\$5.01M
Aerospace & Defense	\$5.46M
Energy & Utilities	\$4.78M

Oil & Gas	\$4.72M
Automotive	\$4.60M
Mining & Metals	\$4.10M
Chemicals	\$4.00M
Logistics & 3PL	\$3.90M
Electronics	\$3.80M
Water & Wastewater	\$3.50M
Pulp & Paper	\$3.20M
Food & Beverage	\$1.80M (excl. recalls)
Global Average	\$4.44M

C. Regulatory Fine Schedules

Regulation	Maximum Fine	Typical Settlement Range
NERC CIP	\$1M/day/violation	\$1M–\$10M
HIPAA	\$50K/record, \$1.5M/yr cap	\$500K–\$5M
SEC Cyber Disclosure	Case-by-case	\$1M–\$10M+
EPA (Clean Water Act)	\$60K+/day/violation	\$100K–\$5M
FDA 21 CFR Part 11	Consent decree	\$10M–\$100M+
CMMC 2.0	Loss of DoD contracts	Revenue-dependent
EU NIS2	€10M or 2% global turnover	Varies by member state

D. Market Size Calculation Multipliers

Factor	Small (<\$50M)	Mid (\$50M–\$1B)	Large (>\$1B)
Operational loss during breach	100%	40%	10%
SLA penalty flat fee	N/A	\$50K per customer	\$250K per customer
Brand/Regulatory baseline	\$50K	\$200K	\$1M+
Cyber insurance denial risk	High (40%+)	Moderate (20%)	Low (10%)
Survival risk	Critical (60% fail)	Moderate	Minimal

© 2026 Fireball Industries LLC. All rights reserved. EmberNet is a product of Fireball Industries. All industry benchmarks cited in this paper are drawn from publicly available 2026 research, including IBM Security, Ponemon Institute, Gartner, Siemens, and regulatory agency publications. Specific company scenarios are hypothetical and intended for illustrative purposes only.