FIREBALL INDUSTRIES

IGNITE YOUR FACTORY EFFICIENCY

WHITEPAPER

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 | Fireball Industries | October 2026



SECTION 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 about $38,333 per minute in halted throughput at a large automotive plant.[1] 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: **EmberRTOS** (immutable endpoint OS, 70% attack surface reduction), **EmberFLUX** (dark Zero-Trust Networking, 99.99% API surface reduction), **Plasma** (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 **94 seconds** of unplanned downtime.

$38.3K

Cost per minute of downtime at a large automotive plant (Siemens, 2024).

94 sec

Prevented downtime that covers a year of EmberNet Pro in a large automotive plant.

4 layers

EmberRTOS, EmberFLUX, Plasma, and hardened K3s, each hardened on its own.

SECTION 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:

1. **Initial Compromise**: An attacker gains access through a phishing email, a compromised VPN credential, or an exposed Remote Desktop Protocol (RDP) service on the IT network.
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.

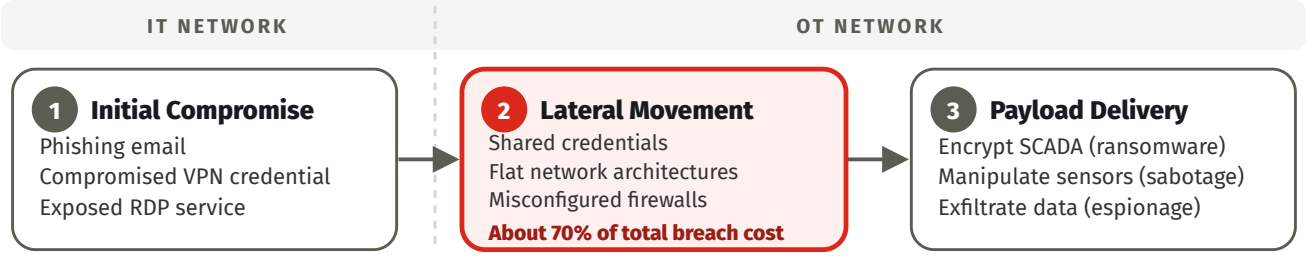

Figure 1. The three-phase attack path described above. Phase 2, lateral movement from IT into OT, is the critical failure point.

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:

REGULATION	SECTOR	KEY REQUIREMENT	PENALTY FOR NON-COMPLIANCE
SEC Cyber Disclosure Rules	All publicly traded	Material incidents disclosed within 4 business days[2]	Enforcement actions, shareholder lawsuits
NERC CIP v7+	Energy & Utilities	Mandatory security controls for Bulk Electric System	Up to $1,584,648 per day per violation[3]
CMMC 2.0	Aerospace & Defense	Certified maturity model for DoD contractors[4]	Loss of Authority to Operate (ATO) and contracts
HIPAA / HITECH	Healthcare	Protection of electronic Protected Health Information	$145 to $73,011 per violation, up to $2,190,294 per year[5]
FDA 21 CFR Part 11	Pharmaceuticals	Electronic records integrity and audit trails[6]	Product recalls, consent decree, criminal prosecution
EPA / Clean Water Act	Water & Wastewater	Integrity of treatment process controls	$60,000+ per day per violation[7]
EU NIS2 Directive	All essential services (EU)	Risk management and incident reporting	Up to €10M or 2% of global turnover[8]

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.

SECTION 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	BENCHMARK
Average cost per minute of line stoppage	**$38,333** (large automotive plant)[1]
Average cost per hour	**$2,300,000** (large automotive plant)[1]
Average total breach cost	**$4.6M**
Mean time to identify a breach (industry avg)	**181 days** (IBM 2025)[9]

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: **$10.35 million**. The OEM customer activates penalty clauses for missed shipments: **$2.1 million**. Total loss: **$12.45 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: **$12.45 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	BENCHMARK
Average value of WIP per batch	$250K to $1M
Average total breach cost	$1.8M
Regulatory recall cost (FDA Class I)	$10M+[10]
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.[6] 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.

THE LITERAL COST OF SECONDS

METRIC	BENCHMARK
Average cost per compromised batch	$500K to $2M
Average total breach cost	$4.61M (IBM 2025)[9]
Cost of FDA consent decree	$100M+[11]
Cost of re-validation after system compromise	$1M to $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	BENCHMARK
Average cost per hour of production stoppage	About $500,000 (2021/22)[12]
Average total breach cost	$4.72M
Cost of pipeline incident (environmental)	$100M+[13]
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 **$1,584,648 per day per violation**, the current inflation-adjusted maximum.[3] Beyond fines, a successful attack on the grid has implications for public safety and national security.

METRIC	BENCHMARK
NERC CIP fine potential	**$1,584,648 per day per violation**[3]
Average total breach cost (energy sector)	**$4.83M** (IBM 2025)[9]
Cost of grid instability event	**$50M to $500M**
Days to remediate NERC CIP violation	**About 269 days** (NERC 2011 average, all standards)[14]

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 have reached eight figures.[15])

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.[9] 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	BENCHMARK
Average cost per compromised record	**$429** (IBM 2019)[16]
Average total breach cost	**$7.42M** (highest of any industry, IBM 2025)[9]
Cost of life-safety IoT compromise	**Litigation: $10M to $100M+**
HIPAA fine per violation category	**$145 to $73,011 per violation**[5]

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	BENCHMARK
Average cost of process safety incident	**$1.2M per day**
EPA fine for unauthorized release	**$100K+ per day**[7]
Average total breach cost	**$4.0M**
Cost of facility shutdown for investigation	**$5M to $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.[17] Beyond compliance, the exfiltration of controlled technical data, such as CNC machining files for proprietary components, represents an existential threat to competitive advantage.

METRIC	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 to $500M[18]
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	BENCHMARK
Average cost per hour of fab stoppage	$1M to $2M+ (advanced fabs)[19]
Cost of cleanroom recertification	$500K to $2M
Average wafer lot value	$20,000 to $500,000+ (25-wafer lot)[20]
Lead time to replace lost production	12 to 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	BENCHMARK
Average cost per hour of hub outage	**$5,000 to $100,000** (warehouse downtime)[21]
Average total breach cost	**$3.9M**
SLA penalty exposure per event	**$50K to $500K**
Customer churn rate post-breach	**15 to 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	BENCHMARK
Average cost per hour of treatment disruption	**$100,000+**
EPA fine per day of violation	**$60,000+**[7]
Cost of "boil water" advisory (public trust)	**About $16.6M** (2-day citywide notice, large city)[22]
Average total breach cost	**$3.5M**

THE LITERAL COST OF SECONDS

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	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 to 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 to 6 hours**.

THE LITERAL COST OF SECONDS

METRIC	BENCHMARK
Average cost per hour of paper machine downtime	$80,000 to $150,000[23]
Average time to clear a paper break	2 to 6 hours
Cost of dryer section restart	$300K to $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	BENCHMARK
Average cost per hour of SMT line stoppage	$500 to $2,000 (mid- to high-volume line)[24]
Cost of defective production run (undetected)	$500K to $2M
Average total breach cost	$3.8M
Customer penalty for quality escape	$100K to $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.

THE LITERAL COST OF SECONDS

METRIC	BENCHMARK
Average cost per minute of trading system outage	**$100,000+**[25]
Average total breach cost	**$5.56M** (IBM 2025)[9]
SEC fine for late disclosure	**$1M to $10M+**[26,27,28,29]
Average customer churn post-breach	**5.9%** (IBM 2019)[16]

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.

SECTION IV

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

A $4.99 million breach (IBM's 2026 global average)[30] 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.

What closes a small manufacturer 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: for small and mid-size companies, NetDiligence puts the average at $152,000 for crisis services (forensics, counsel, notification) and $264,000 per incident overall.[31] For a small manufacturer, this is the difference between survival and closure.

Formula:

> **L = (Annual Revenue ÷ 250 working days) × Days of Outage + Fixed Recovery Costs**

Key Assumptions:

- 100% operational loss during breach
- No redundant systems
- Average outage duration: 7 to 21 days[32]
- Fixed recovery costs: $152K to $264K (NetDiligence averages)[31]
- 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 (top of the NetDiligence range)	$264,000
Total Loss	**$1,944,000**
EmberNet annual subscription (Starter, $2,500/mo; nodes are never billed)	$30,000
ROI if breach prevented (first-year basis)	**6,380%**

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.[33] A breach is not just a financial event; it is a **qualification event** that can disqualify the supplier from future contracts.

Formula:

> **L = Downtime Cost + SLA Penalty Fees + Customer Churn Value + Re-Qualification Cost**

Key Assumptions:

- 40% operational loss during breach (partial redundancy)
- Revenue per day: annual revenue ÷ 250 working days, as in 4.1
- SLA penalty flat fee: $50K to $500K per customer per incident
- Customer churn: 10 to 20% of revenue at risk
- Re-qualification cost (CMMC Level 2 assessment, three years): $104,670 to $117,768[34]

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
Revenue per working day ($250,000,000 ÷ 250)	$1,000,000
40% operational loss × 5 working days	$2,000,000
SLA penalties (3 customers)	$450,000
Customer churn (1 lost account)	$3,500,000
Re-qualification costs (top of the DoD estimate)	$117,768
Total Loss	**$6,067,768**
EmberNet annual subscription (Pro, $5,000/mo; nodes are never billed)	$60,000
ROI if breach prevented (first-year basis)	**10,013%**

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[2] has added a new dimension: public market reaction. Comparitech's analysis of breached companies found share prices fell an average of **1.4%**, bottoming out 41 business days after disclosure, then recovered to pre-disclosure levels after 53 days while trailing the NASDAQ by 3.2% at six months.[35]

Formula:

> **L = (Δ Stock Price × Outstanding Shares) + Regulatory Fines + Incident Response (@ $600/hr) + Litigation Reserves**

Key Assumptions:

- 10% operational loss during breach (redundancy absorbs most impact)
- Stock price impact: 1.4% decline (average, Comparitech)
- Regulatory fine baseline: $1M+
- Incident response duration: 2,000 to 10,000 hours at $600/hr[36]
- Litigation reserves: $5M to $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 (1.4%)	$112,000,000
Regulatory fines	$5,000,000
Incident response (5,000 hrs × $600)	$3,000,000
Litigation reserves	$15,000,000
Total Loss	**$135,000,000**
EmberNet annual cost	Enterprise, by agreement (contact sales)



Figure 2. A robotic production cell. Section IV prices the same stoppage three ways, depending on who owns the line.

SECTION 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.

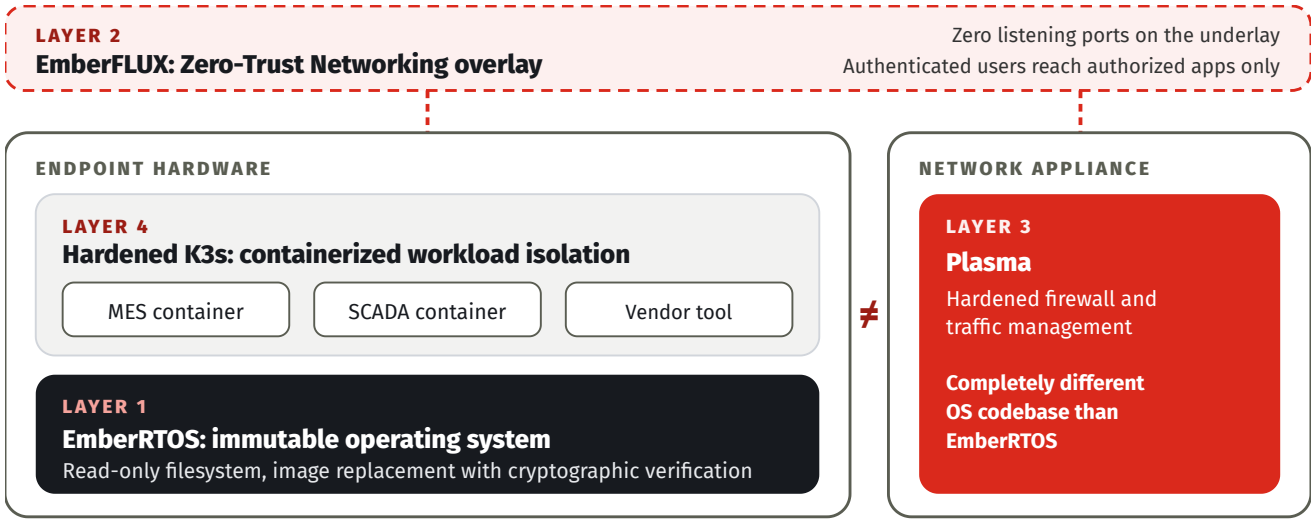

Figure 3. The four layers of EmberNet as described in this section: EmberRTOS and hardened K3s on the endpoint hardware, Plasma on the network appliance with its own OS codebase, and EmberFLUX across both.

The Four Layers of EmberNet

Layer 1: EmberRTOS (Immutable Operating System)

EmberRTOS 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: EmberFLUX (Zero-Trust Networking)

EmberFLUX is a software-defined overlay network that connects authenticated users directly to authorized applications. Unlike traditional networks where services listen on open ports, EmberFLUX 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%**[37]
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: Plasma (Network Appliance Firewall)

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

METRIC	PUBLISHED BENCHMARK
Microsegmentation lateral movement prevention	**87.3%** (standalone)[38]
Combined ZTA + microsegmentation prevention	**95.8%**[38]
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 EmberRTOS, that exploit is useless against Plasma, 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 EmberFLUX 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)[39] is eliminated by EmberFLUX'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** (EmberFLUX: zero listening ports)
Lateral movement	64.8% reduction[38]	**95.8% prevention** (Plasma microsegmentation + ZTA)
Persistent malware / rootkits	Partially mitigated (EDR)	**Eliminated** (EmberRTOS: immutable filesystem)
Configuration drift / unauthorized changes	Monitored (SIEM)	**Eliminated** (EmberRTOS: 72% fewer config vulns)
Cross-layer exploitation	Single OS = single exploit chain	**Dual OS diversity** (EmberRTOS ≠ Plasma)
Container escape to host	Host is mutable / writable	**Host is read-only** (EmberRTOS: nowhere to persist)
Credential theft / VPN compromise	MFA + monitoring	**Architecturally neutralized** (EmberFLUX: 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 **241 days** (IBM 2025)[9] 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 percentage:

$$\text{ROI} = \frac{(\text{Expected Loss} - \text{Mitigated Loss}) - \text{EmberNet Cost}}{\text{EmberNet Cost}}$$

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 ZTA benchmarks (IBM, 2022), organizations with fully deployed Zero-Trust architectures reduce their breach costs by an average of **$1.51 million** compared with early-stage deployments.[40] 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)	DOWNTIME COST PER MINUTE	MINUTES OF PREVENTION TO COVER A YEAR
Automotive	$60,000	$38,333	**1.6 minutes (94 seconds)**
Semiconductors	$60,000	$33,333	**1.8 minutes (108 seconds)**
Oil & Gas	$60,000	$8,333	**7.2 minutes**
Pharma	$60,000	1 batch = $500K+	**< 1 batch**
Food & Bev	$60,000	1 batch = $250K+	**< 1 batch**
Energy (Fines)	$60,000	$1,100/min ($1,584,648/day)	**55 minutes of fine avoidance**

Note: EmberNet is priced per control plane, never per node, and Industrial PC hardware is purchased separately. The Pro subscription is the same every year, so the payback threshold does not change after Year 1. Per-minute rates: automotive is Siemens' $2.3 million an hour for a large plant; semiconductors the top of Schneider Electric's $1 million to $2 million an hour for advanced fabs; oil and gas Siemens' almost $500,000 an hour; energy the inflation-adjusted NERC maximum.[1,19,12,3]

The "Aha!" Moment: EmberNet pays for itself if it prevents just **94 seconds of unplanned downtime** in a large automotive plant, **108 seconds** in a semiconductor fab, **one spoiled batch** in Pharma or Food & Bev, or **less than an hour** of NERC CIP fine exposure.

SECTION 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 published 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: $10.35M	Direct downtime cost: $0
SLA penalties: $2.1M	SLA penalties: $0
Recovery & forensics: $800K	Incident investigation: $50K (IT-side credential compromise only)
Total: $13.25M	**Total: $50K**
	Avoided Loss: $13.2M

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**.

SECTION 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 to $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., **+$639/second** for a large automotive plant. This visual device creates the psychological urgency necessary to convert a security evaluation into a purchase decision.

How EmberNet Access Actually Works

Section V says an attacker cannot see what they are not authorized to reach. This is the mechanism behind that sentence, taken from the EmberNet product documentation.

Identity instead of addresses

NIST describes zero trust as a set of paradigms that move defenses "from static, network-based perimeters to focus on users, assets, and resources."[41] On EmberNet, that focus is identity. Every node, service, and user on EmberNet is issued a cryptographic identity when it enrolls. Access is granted between identities, not between IP addresses, and routing follows identity rather than network location. That is the property that takes lateral movement off the table: there is no address space to scan, because reachability is not a function of addressing. Policy then decides which identities may talk to which services, and the default is deny.[42]

Outbound only, on 443

Nodes make outbound connections to the fabric. Nothing dials in, so there is no inbound port to open, no port forward, and no public IP on plant equipment. Connections are mutually authenticated with TLS, using certificates the platform issues at enrollment, rotates before they expire, and can revoke immediately. Validity periods are deliberately short, which limits how useful a stolen certificate is.[42] Traffic rides port 443, so it passes through restrictive networks without special firewall changes.[43]

PROPERTY	WHAT IT MEANS AT THE PLANT
No inbound ports	No firewall exceptions, no port forwarding, no exposed equipment
No VPN	No site-to-site tunnels to build, document, or maintain
Automatic certificates	Issued on enrollment, rotated before expiry, revocable instantly
NAT traversal	Works through carrier-grade NAT with no configuration
Network agnostic	Runs over cellular, satellite, Wi-Fi, or ethernet
Everything over 443	Passes through restrictive networks without special handling

Source: EmberNet documentation, Zero-Trust Networking.[42]

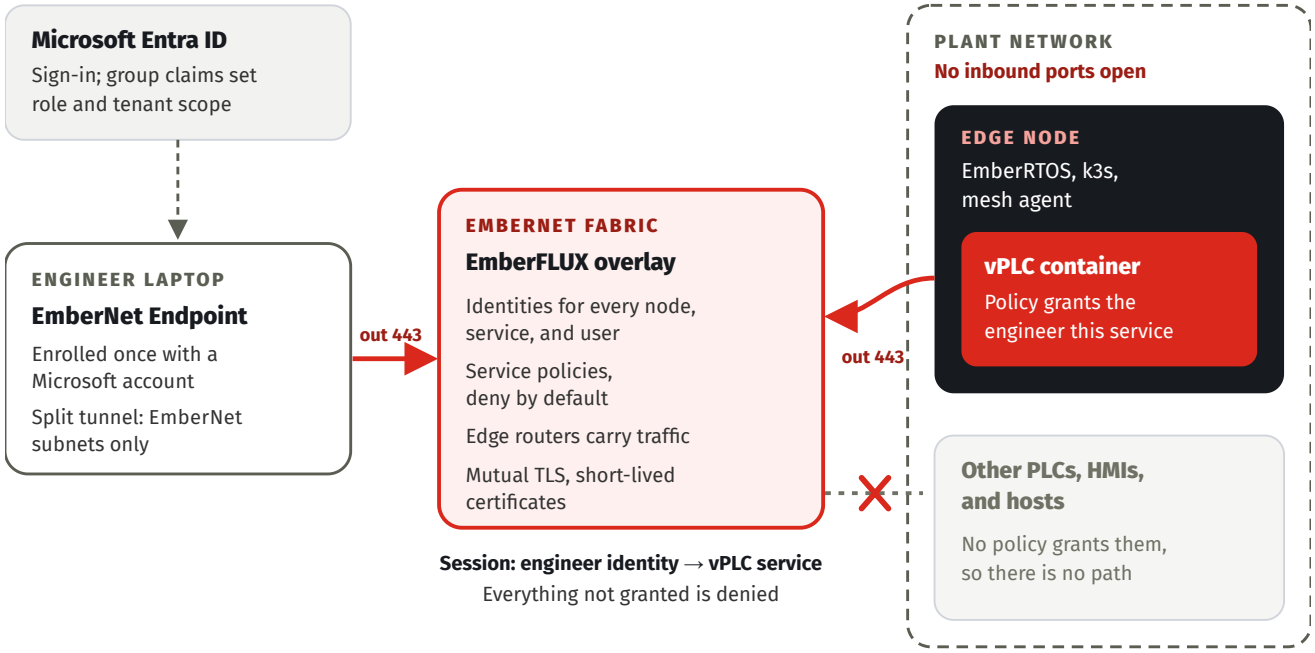

Figure 4. How an engineer reaches one PLC. Both the laptop and the plant node dial out on 443; nothing dials in. A service policy grants the engineer's identity one service, and nothing else on the plant network is reachable. Drawn from the EmberNet documentation.

How a node enrolls

Installation is white-glove: Fireball Industries provisions edge nodes with EmberRTOS already on them. Before a node goes in, the site needs outbound HTTPS on port 443, working DNS and NTP, and a Microsoft Entra ID tenant with single sign-on configured. Then the process runs in five steps:[44]

1. **Provisioning.** The node is imaged with EmberRTOS. First boot reads a configuration medium and applies site-specific settings: hostname, networking, and any keys the node needs.
2. **Cluster formation.** A single-node site is a cluster of one. A multi-node site joins additional nodes to the first.
3. **Platform services.** Telemetry ingestion, time-series storage, the console, the alert engine, the API, and the mesh agent come up as containerized workloads on the node. There is no manual orchestration step.
4. **Mesh enrollment.** The node generates an identity, dials out to the mesh, receives its certificates and policy, and becomes reachable to authorized services. Nothing dials in.
5. **Tenant setup.** The tenant is created and bound to directory groups, so its users resolve to the right roles and scope.

One detail matters more than it looks. Short-lived certificates make clock accuracy load-bearing: a node with significant clock skew fails certificate validation and enrollment, and the symptom looks like a network problem rather than a time problem.[42]

How an engineer reaches one PLC, and nothing else

The engineer's laptop runs EmberNet Endpoint, which is built for Windows and Linux. It enrolls once with the engineer's Microsoft account through a device-code sign-in and then keeps its own tunnels healthy. It is split-tunnel by default, claiming routes only for EmberNet-assigned subnets, so the rest of the laptop's network works exactly as before. Its local management interface listens on loopback only, never on the network.[45]

There is no separate EmberNet password. Sign-in is delegated to the organization's identity provider, and the engineer's directory group membership decides both their role and which tenants they can see.[46]

Reaching a PLC is then a policy question. A policy grants a source identity access to a target service, for example the engineer's identity to one vPLC, and everything not granted is denied. Policies cover four kinds of traffic: service to service, user to service, tenant to tenant (denied by default), and access from outside the mesh.[42] Posture checks can also require an endpoint to meet conditions, such as OS, a running process, or MFA, before it is trusted.[43] When an engineer sees "access denied", it is usually the system working correctly: no policy grants that path.[42]

Every one of those decisions leaves a record. EmberCORE, the platform console, shows node connectivity and latency, certificate validity and rotation schedule, policy evaluation logs, and connection attempt history.[42] That is the visibility and audit logging Section V refers to.

FIELD PROOF

Proof from EmberNet

Sections III through VII rest on industry benchmarks and modeled scenarios. This section is different. It reports what EmberNet has actually done, with the test conditions attached.

Real-time control on EmberRTOS

Layer 1 in Section V describes EmberRTOS as an immutable operating system. The real-time kernel is a per-machine toggle on the same immutable base.[47] With the real-time kernel switched on, a Raspberry Pi 5 (BCM2712) held a worst-case wake-up latency of **23 µs** over **86,423 seconds (24 hours)** and about **627 million samples**. The test ran three SCHED_FIFO priority 99 threads at 200, 700, and 1200 µs intervals, measured with `cyclictest`. The per-thread worst cases were 17, 20, and 23 µs, and the average was 1 µs. The board ran from about 30 °C to about 60 °C with no throttling.[48]

23 µs
Worst-case wake-up latency, Raspberry Pi 5, real-time kernel on.

24 hours
86,423 seconds of continuous measurement.

627 M
About 627 million latency samples across three threads.

Industrial control loops target a band of 100 to 200 µs. A 23 µs worst case sits 4 to 9 times inside it.[48]

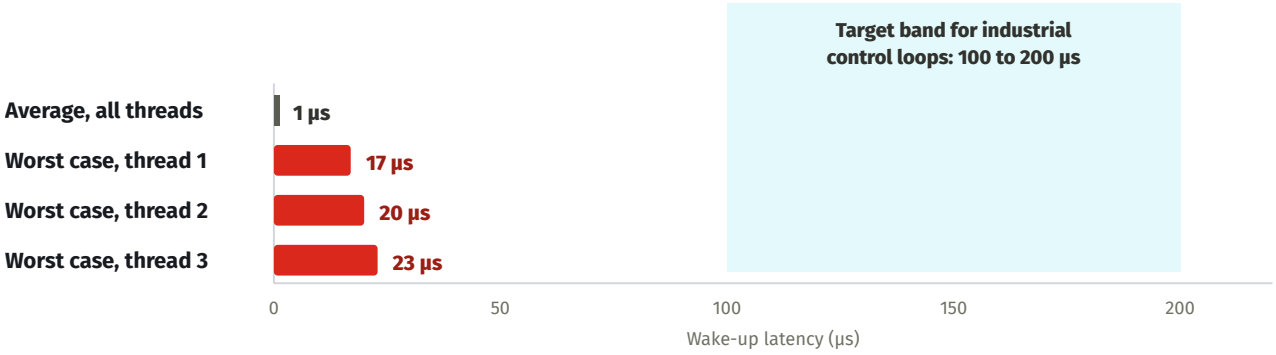

Figure 5. EmberRTOS real-time results on a Raspberry Pi 5 over 24 hours: per-thread worst cases and the average, against the 100 to 200 µs target band. Source: EmberRTOS hardware results.[48]

HOW THE TEST WAS LOADED

The stress load (hackbench, two CPU-burn loops, and a memory streamer) was pinned to the housekeeping core, so the real-time cores stayed isolated. It is not an all-core adversarial test, and these numbers should not be read as one.

Austin to Cleveland: a PLC download across 1,200 miles

On September 29, 2026, an engineer in Austin, Texas downloaded the PLC application from the CODESYS IDE (CODESYS V3.5 SP22 Patch 2) to a virtual PLC (vPLC) in Cleveland, Ohio, over EmberNet. The Cleveland node is an Industrial PC (arm64, running k3s) with CODESYS Control for Linux ARM64 SL 4.22 in a container, reached over the node's EmberNet overlay address on port 11740. There was no VPN, no port forwarding, and nothing exposed on the plant network. The distance is about 1,200 miles (1,184 miles straight-line). The project is deployed with the client.

That is the scenario from Section 3.4 turned around. There, the question was whether a compromised workstation could reach a PLC. Here, an authorized engineer reached a vPLC from another state, with nothing exposed on the plant network.

Cleveland to Mumbai: 7,900 miles

An engineer in Cleveland, Ohio downloaded a CODESYS application to a virtual PLC at a plant in Mumbai, India, over EmberNet. The distance is about 7,900 miles (7,946 miles great-circle). The client is anonymous.

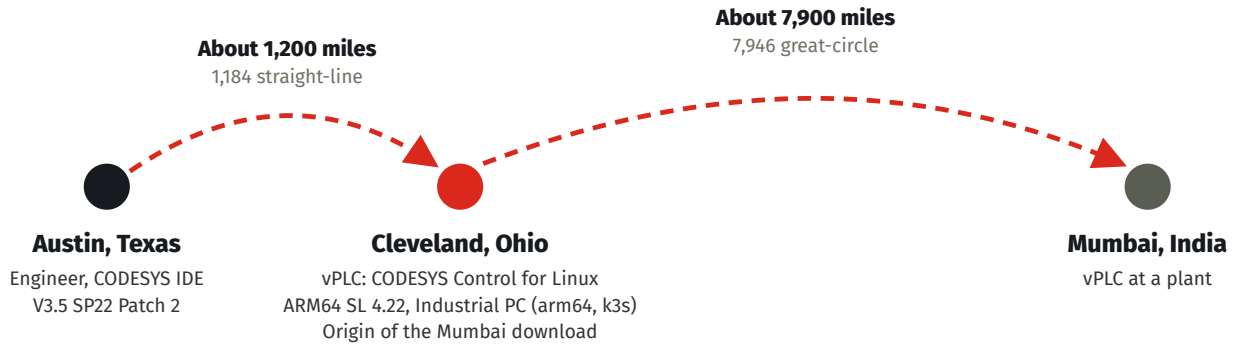

Figure 6. Two CODESYS downloads to virtual PLCs over EmberNet: Austin to Cleveland on September 29, 2026, and Cleveland to Mumbai. Schematic, not to scale.

Fireball Industries is a CODESYS System Partner.

SECTION 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.

ENGAGEMENT

How to Get There with Fireball

From a conversation to a protected line

Fireball Industries designs, builds, commissions, and supports industrial automation. This is how an engagement runs, as we describe it on fireballz.ai.[49]

1. **Conversation.** We start with a conversation about your operations and goals.
2. **Scope and quote.** We scope a solution that fits your timeline and budget, then send back a quote you can act on.
3. **Design and build.** Controls design and system architecture, robotics and motion integration, panel builds, and prototype and pilot-line development.
4. **Digital commissioning.** We validate systems before they reach your floor, for faster, safer rollouts with less downtime and fewer surprises at startup.
5. **Installation and startup.** Project management and site startups, on-site installation, and SCADA support.
6. **Support.** Remote and on-site troubleshooting, preventive and predictive maintenance, retrofit and modernization, and the Manufacturing Excellence Program: monthly support for continuous automation, AI, and process improvement, without the overhead of full-time staff.[50]

A phased migration plan

The recommendations in Section VIII become four phases. Each phase has a short checklist, and every item on it is something your team does.

Phase 1 Quantify the exposure

- Calculate your cost per minute: fixed labor plus lost throughput plus material at risk.
- Pick your market-size model from Section IV and rerun its sample calculation with your own revenue.
- List your crown jewels: the systems that would do the most damage if compromised for 10 minutes.
- Inventory every remote access path into OT: VPNs, RDP, vendor connections, jump hosts, and port forwards.
- Map everywhere OT can be reached from IT through implicit trust: shared credentials, flat VLANs, and firewall rules.
- Pull your cyber insurance policy and list the controls it requires.

Phase 2 Pilot on one crown jewel

- Choose one line or one system from your crown-jewel list.
- Confirm outbound 443, DNS, and NTP from the site, tested from the node itself, not assumed from the firewall policy.
- Configure single sign-on in your Microsoft Entra ID tenant and map security groups to roles.
- Write the first policies: which identities may reach which services. Start from deny.
- Move one remote access path onto EmberNet, then close the old one.
- Work the validation list: services healthy, node in the fleet, telemetry from a real device, a test alert delivered.

Phase 3 Expand across the site and the fleet

- Move the remaining remote access paths one at a time, closing each old path as you go.
- Move workloads into containers so each one gets its own identity and its own policy.
- Retire flat-network paths, port forwards, and shared credentials between IT and OT.
- Track cyber-caused downtime with the same rigor as mechanical downtime.

Phase 4 Operate and prove it

- Review policy evaluation logs and connection attempt history on a fixed schedule.
- Recalculate your cost per minute and payback period every year, in minutes, hours, or batches.
- Report to the board in dollars per minute, not in threat-landscape language.
- Check your insurance and regulatory requirements against what you now enforce.

WHAT EMBERNET COSTS

EmberNet is priced per control plane, never per node. Pilot is free, one per organization. Starter is $2,500 a month, Pro is $5,000 a month, and Enterprise is by agreement (contact sales). Industrial PC hardware is purchased separately.

SECTION 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?**



Figure 7. A production floor. The cost of an open attack path is measured in seconds.

SECTION X

Appendix: Industry Benchmark Data Tables

A. Downtime Cost by Industry

INDUSTRY	COST/MINUTE	COST/HOUR	COST/DAY
Automotive (large plant)	$38,333[1]	$2,300,000	$55,200,000
Semiconductors (advanced fabs)	$16,667 to $33,333[19]	$1M to $2M	$24M to $48M
Oil & Gas	$8,333[12]	$500,000	$12,000,000
Aerospace & Defense	$10,333	$620,000	$14,880,000
Mining & Metals	$8,333	$500,000	$12,000,000
Logistics & 3PL (warehouse)	$83 to $1,667[21]	$5K to $100K	$120K to $2.4M
Pulp & Paper	$1,333 to $2,500[23]	$80K to $150K	$1.92M to $3.6M
Chemicals	$833+	$50,000+	$1,200,000+
Electronics Manufacturing (SMT line)	$8 to $33[24]	$500 to $2,000	$12,000 to $48,000
Financial Services	$100,000+	$6,000,000+	$144,000,000+
Healthcare	$167 to $250	$10K to $15K	$240K to $360K
Water & Wastewater	$1,667	$100,000	$2,400,000
Food & Beverage	Per batch: $250K to $1M	N/A	N/A
Pharma	Per batch: $500K to $2M	N/A	N/A
Energy & Utilities	Fines: $1,100/min	Fines: $66,027/hr	Fines: $1,584,648/day[3]

B. Average Total Breach Cost by Industry

INDUSTRY	AVERAGE TOTAL BREACH COST
Healthcare	$7.42M (IBM 2025)[9]
Financial Services	$5.56M (IBM 2025)[9]
Aerospace & Defense	$5.46M
Energy & Utilities	$4.83M (IBM 2025)[9]
Oil & Gas	$4.72M
Pharmaceuticals	$4.61M (IBM 2025)[9]
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	**$4.99M (IBM 2026)**[30]

C. Regulatory Fine Schedules

REGULATION	MAXIMUM FINE	TYPICAL SETTLEMENT RANGE
NERC CIP	$1,584,648/day/violation[3]	Up to $10M (the 2019 record)[15]
HIPAA	$73,011/violation, $2,190,294/yr cap[5]	$100K to $1.19M (OCR actions, late 2024)[51]
SEC Cyber Disclosure	Case-by-case	$1M to $10M+[26,27,28,29]
EPA (Clean Water Act)	$60K+/day/violation[7]	$100K to $5M
FDA 21 CFR Part 11	Consent decree	$10M to $100M+[52]
CMMC 2.0	Loss of DoD contracts[17]	Revenue-dependent
EU NIS2	€10M or 2% global turnover[8]	Varies by member state

D. Market Size Calculation Multipliers

FACTOR	SMALL (<$50M)	MID ($50M TO $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	Moderate	Minimal

APPENDIX

Methodology

How this paper's own numbers are produced, step by step, so anyone can rerun them with their own inputs.

Units and conversions

Appendix A states each industry's downtime rate in three units: cost per hour is cost per minute times 60, and cost per day is cost per hour times 24. A large automotive plant at $2,300,000 an hour is $38,333 a minute and $55,200,000 a day.[1] The live counter in Section VII divides the per-minute rate by 60, which is where $639 a second comes from. Chemicals runs the other way, from Section 3.7's $1,200,000 a day: $50,000 an hour and $833 a minute. For energy, fine exposure starts from the inflation-adjusted NERC maximum of $1,584,648 a day: divided by 24 that is $66,027 an hour, and divided by 1,440 minutes it is about $1,100 a minute.[3] Where a source gives a range, the text shows the range and the payback math uses its top, the same convention as the original paper.

Day count

Both the small market and mid-market models turn annual revenue into a daily figure the same way: annual revenue divided by 250 working days.

Small market model (Section 4.1)

> **L = (Annual Revenue ÷ 250 working days) × Days of Outage + Fixed Recovery Costs**

The sample uses $30,000,000 in revenue: $30,000,000 ÷ 250 = $120,000 a day. Fourteen days of outage is $1,680,000. Fixed recovery costs use the top of the NetDiligence range, $264,000, bringing the total to $1,944,000.[31] The ROI line assumes the breach is prevented outright, so Mitigated Loss is zero: ($1,944,000 – $30,000) ÷ $30,000 = 63.80, or 6,380%.

Mid-market model (Section 4.2)

> **L = Downtime Cost + SLA Penalty Fees + Customer Churn Value + Re-Qualification Cost**

The downtime line applies 40% operational loss for 5 working days: $250,000,000 ÷ 250 = $1,000,000 a day, × 40% × 5 = $2,000,000. Adding $450,000 in SLA penalties, $3,500,000 for one lost account, and $117,768 in re-qualification (the top of DoD's three-year Level 2 estimate) gives $6,067,768.[34] ROI on the Pro subscription: ($6,067,768 – $60,000) ÷ $60,000 = 100.13, or 10,013%.

Large market model (Section 4.3)

> **L = (Δ Stock Price × Outstanding Shares) + Regulatory Fines + Incident Response (@ $600/hr) + Litigation Reserves**

Stock price times outstanding shares is market capitalization, so the first term is the percentage decline applied to market cap: 1.4% of $8,000,000,000 is $112,000,000.[35] Incident response is 5,000 hours × $600 = $3,000,000. With $5,000,000 in fines and $15,000,000 in litigation reserves, the total is $135,000,000. No ROI is shown, because Enterprise pricing is by agreement.

The ROI formula and the payback period (Section V)

ROI is the avoided loss net of what EmberNet costs, divided by what EmberNet costs: ((Expected Loss – Mitigated Loss) – EmberNet Cost) ÷ EmberNet Cost. The payback period runs the other way: it asks how much downtime has to be prevented to cover one year of the subscription.

> **Minutes to cover a year = Annual EmberNet Cost ÷ Downtime Cost per Minute**

At the Pro rate of $60,000 a year: $60,000 ÷ $38,333 = 1.57 minutes, or 94 seconds, for a large automotive plant; $60,000 ÷ $33,333 = 1.8 minutes (108 seconds) for semiconductors; and $60,000 ÷ $8,333 = 7.2 minutes for oil and gas. For energy, $60,000 ÷ $1,100 = 54.5 minutes, under an hour. For pharma and food and beverage, a single batch at $500,000 or $250,000 is worth more than a year of Pro, so the threshold is less than one batch.

Case studies (Sections 3.1 and VI)

The 3.1 scenario and Scenario A both price 4.5 hours of downtime at $2,300,000 an hour: $10.35M. In 3.1, adding the $2.1M penalty gives $12.45M. Each "Without EmberNet" total in Section VI is the sum of its line items, and Avoided Loss is that total minus the "With EmberNet" total. Scenario A: $10.35M + $2.1M + $0.8M = $13.25M, less $50K, is $13.2M. Scenario B: $1.8M + $0.4M + $3M = $5.2M, less $15K, is $5.185M. Scenario C: $200K + $1.2M + $300K + $180K = $1.88M, less $5K, is $1.875M, and $1.88M ÷ $8M = 23.5% of the utility's annual budget.

The salary comparison (Section 4.1)

The small market Value Case compares EmberNet to one entry-level IT technician's salary. Starter is $30,000 a year. The U.S. Bureau of Labor Statistics reports that the lowest-paid 10 percent of computer user support specialists earned less than $40,980 in May 2025, against a median of $61,860.[53] Starter costs less than even the bottom of that range.

Where the outside numbers come from

IBM Cost of a Data Breach Report. An annual study conducted independently by Ponemon Institute and sponsored, analyzed, and published by IBM. Each edition studies several hundred organizations that suffered a breach in the prior year (600 in the 2025 edition) and reports costs by industry and country. The global average is from the 2026 report page; industry costs and breach timelines are from the 2025 report, the most recent edition whose industry figures could be checked. Per-record healthcare cost and financial services churn are from 2019, and the zero trust savings from 2022, the latest editions that report them. Each figure in the paper is labeled with its year.

Downtime costs. Automotive and oil and gas downtime come from Siemens' True Cost of Downtime reports, semiconductors from Schneider Electric, warehouse logistics from FreightWaves' reporting of a Synergy Logistics study, pulp and paper from a Super Lube field service case study, SMT lines from a Minitab analysis, and trading-system downtime from Patterson's USENIX paper. Where a source measures something narrower than the paper's heading (a large automotive plant, an advanced fab, a warehouse), the text says so.

Regulations. Disclosure deadlines and penalty amounts are checked against the rule itself: the SEC's 2023 cybersecurity disclosure rule, the CMMC program rule and the DFARS clause that applies it, 21 CFR Part 11, the inflation-adjusted civil penalty tables for FERC (18 CFR 385.1602), HHS (45 CFR 102.3), and EPA (40 CFR 19.4), and Article 34 of the NIS2 Directive. Settlement examples come from the SEC's enforcement releases, reporting on NERC and HHS OCR actions, and a company's SEC filing.

Other costs. Recovery costs for small and mid-size companies come from the NetDiligence Cyber Claims Study, stock price effects from Comparitech's analysis of breached companies, outage length from Coveware's ransomware reports, re-qualification cost from DoD's own estimate in the CMMC rule, the recall figure from the Food Marketing Institute and Grocery Manufacturers Association study, the boil water notice cost from an ECONorthwest study for Portland, the pipeline cost from the NTSB, and the R&D example from a Justice Department case.

Security architecture. The microsegmentation and zero trust lateral movement figures come from a 2025 journal article that compiles implementation data, the dark networking figure from NetFoundry, a zero trust networking vendor that publishes it without a methodology, and the Kubernetes misconfiguration finding from Red Hat's survey of Kubernetes users. The definition of zero trust is NIST's, from SP 800-207.

EmberNet documentation and results. The description of enrollment and access comes from the EmberNet product documentation, and the real-time numbers from the published EmberRTOS hardware results.

Figures without a reference number are the author's benchmarks and are used as stated. The results in "Proof from EmberNet" are EmberNet's own measurements and engineering events, not industry benchmarks, and the case study companies in Section VI are hypothetical.

APPENDIX

References

All URLs were checked on October 5, 2026.

1. The True Cost of Downtime 2024. Siemens, 2024. https://assets.new.siemens.com/siemens/assets/api/uuid:1b43afb5-2d07-47f7-9eb7-893fe7d0bc59/TCOD-2024_original.pdf ($2.3 million an hour in a large automotive plant, more than $600 a second.)
2. SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Press Release 2023-139). U.S. Securities and Exchange Commission, 2023. https://www.sec.gov/newsroom/press-releases/2023-139 (The four business days run from the company's determination that an incident is material.)
3. 18 CFR 385.1602, Civil monetary penalty inflation adjustments. Federal Energy Regulatory Commission, Electronic Code of Federal Regulations, 2025. https://www.ecfr.gov/current/title-18/chapter-I/subchapter-X/part-385/subpart-P/section-385.1602 (Federal Power Act 16 U.S.C. 825o-1(b): $1,584,648 per violation, per day.)
4. 32 CFR Part 170, Cybersecurity Maturity Model Certification (CMMC) Program. U.S. Department of Defense, Electronic Code of Federal Regulations, 2026. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
5. 45 CFR 102.3, Penalty adjustment and table (HIPAA penalties under 45 CFR 160.404). U.S. Department of Health and Human Services, Electronic Code of Federal Regulations, 2024. https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-A/part-102/section-102.3 (Per violation: $145 minimum and $73,011 maximum in the lowest tier; $2,190,294 calendar-year cap.)
6. 21 CFR 11.10, Controls for closed systems. U.S. Food and Drug Administration, Electronic Code of Federal Regulations, 2026. https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11/section-11.10
7. 40 CFR 19.4, Statutory civil monetary penalties, as adjusted for inflation. U.S. Environmental Protection Agency, Electronic Code of Federal Regulations, 2025. https://www.ecfr.gov/current/title-40/chapter-I/subchapter-A/part-19/section-19.4 (Clean Water Act 33 U.S.C. 1319(d): $68,445 per day per violation; Clean Air Act 42 U.S.C. 7413(b): $124,426 per day per violation.)
8. Directive (EU) 2022/2555 (NIS2 Directive), Article 34. Official Journal of the European Union, EUR-Lex, 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/oj
9. Cost of a Data Breach Report 2025. IBM and Ponemon Institute, 2025. https://www.ibm.com/downloads/documents/us-en/131cf87b20b31c91 (Healthcare $7.42M, the highest for the 12th consecutive year; financial $5.56M; energy $4.83M; pharmaceuticals $4.61M; 181 days to identify and 241 days to identify and contain.)
10. Recall: The Food Industry's Biggest Threat to Profitability. Food Safety Magazine, 2012. https://www.food-safety.com/articles/2542-recall-the-food-industrys-biggest-threat-to-profitability (Reports the Food Marketing Institute and Grocery Manufacturers Association finding of $10M average direct cost per recall, not limited to Class I.)
11. Abbott Laboratories Fined. Infection Control Today, 2000. https://www.infectioncontroltoday.com/view/abbott-laboratories-fined (A $100 million FDA consent decree payment.)
12. The True Cost of Downtime 2022. Siemens, 2023. https://assets.new.siemens.com/siemens/assets/api/uuid:3d606495-dbe0-43e4-80b1-d04e27ada920/dics-b10153-00-7600truecostofdowntime2022-144.pdf (Oil and gas downtime at almost $500,000 an hour, 2021/22. The 2024 edition reports 2023 back near 2019 levels without a published figure.)
13. Enbridge Incorporated Hazardous Liquid Pipeline Rupture and Release, Marshall, Michigan (DCA10MP007). National Transportation Safety Board, 2012. https://www.ntsb.gov/investigations/Pages/DCA10MP007.aspx (Line 6B cleanup costs exceeding $767 million.)
14. Enforcement Streamlining Update and Key Compliance Trends, Board of Trustees Compliance Committee presentation. North American Electric Reliability Corporation, 2011. https://www.balch.com/files/upload/BOTCC%20Presentation%20(5-2011).pdf

(Six-month rolling average of 269 days from discovery to a validated mitigation plan, all standards. Copy hosted by Balch & Bingham.)

15. US Energy Firm Fined $10 Million for Security Failures. SecurityWeek, 2019. https://www.securityweek.com/us-energy-firm-fined-10-million-security-failures/ (A record NERC penalty; the previous year's was $2.7 million.)
16. Cost of a Data Breach Report 2019. IBM Security and Ponemon Institute, 2019. https://web.archive.org/web/20200308185647/https://www.ibm.com/downloads/cas/ZBZLY7KL (Archived copy; IBM's original link no longer resolves. Healthcare at $429 per record and financial services customer turnover of 5.9% are from this edition.)
17. 48 CFR 204.7502, Policy (DFARS Subpart 204.75, Cybersecurity Maturity Model Certification). Electronic Code of Federal Regulations, 2026. https://www.ecfr.gov/current/title-48/chapter-2/subchapter-A/part-204/subpart-204.75/section-204.7502
18. Fiber Laser Expert Convicted by Federal Jury of Economic Espionage and Theft of Trade Secrets. U.S. Department of Justice, Office of Public Affairs, n.d. https://www.justice.gov/opa/pr/fiber-laser-expert-convicted-federal-jury-economic-espionage-and-theft-trade-secrets (An example inside the range: a 5-year, $11.4 million research project.)
19. Why is power quality so critical in semiconductor fabs. Schneider Electric Blog, 2026. https://blog.se.com/energy-management-energy-efficiency/2026/07/30/why-is-power-quality-so-critical-in-semiconductor-fabs/ (More than $1 million to $2 million per hour in advanced fabs.)
20. Automation Reduces Contamination and Costs within Semiconductor Fab Cleanrooms. Semiconductor Digest (Chrisos and Horan), n.d. https://sst.semiconductor-digest.com/?p=43390 ($20,000 to well over $500,000 per 25-wafer lot.)
21. Warehouses face $100K-hour downtime risk as cloud outages mount. FreightWaves, 2026. https://www.freightwaves.com/?p=571723 (Citing a Synergy Logistics report: $5,000 to $100,000 per hour.)
22. Economic Effects of a 2-Day and 2-Week Boil Water Notice. ECONorthwest for the Portland Water Bureau, 2017. https://www.portland.gov/sites/default/files/2021/econw_economic-effects-bwn_final_2017-1025.pdf (A 2-day citywide notice: about $13 million for households plus $3.6 million in lost food-service output.)
23. Kroil and Super Lube Help Triosim Service the Pulp and Paper Industry. Super Lube, 2024. https://www.super-lube.com/news-insights/kroil-and-super-lube-help-triosim-service-the-pulp-and-paper-industry/ ($80,000 to $150,000 per hour.)
24. What Downtime Actually Costs You. Minitab Blog, 2025. https://blog.minitab.com/en/what-downtime-actually-costs-you ($500 to $2,000 per hour for a mid- to high-volume SMT line.)
25. A Simple Way to Estimate the Cost of Downtime (Table 1). David A. Patterson, USENIX LISA Conference, 2002. https://www.usenix.org/legacy/event/lisa02/tech/full_papers/patterson/patterson_html/index.html (Brokerage operations at $6,450,000 per hour, about $107,500 per minute; the table's data dates from 2000.)
26. SEC Charges Pearson plc for Misleading Investors About Cyber Breach (Press Release 2021-154). U.S. Securities and Exchange Commission, 2021. https://www.sec.gov/newsroom/press-releases/2021-154 ($1 million.)
27. SEC Charges Software Company Blackbaud Inc. for Misleading Disclosures About Ransomware Attack That Impacted Charitable Donors (Press Release 2023-48). U.S. Securities and Exchange Commission, 2023. https://www.sec.gov/newsroom/press-releases/2023-48 ($3 million.)
28. SEC Charges Four Companies With Misleading Cyber Disclosures (Press Release 2024-174). U.S. Securities and Exchange Commission, 2024. https://www.sec.gov/newsroom/press-releases/2024-174 (Unisys $4 million, Avaya $1 million, Check Point $995,000, Mimecast $990,000; the last two sit just under $1 million.)
29. Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million (Press Release 2018-71). U.S. Securities and Exchange Commission, 2018. https://www.sec.gov/newsroom/press-releases/2018-71
30. Cost of a Data Breach Report 2026 (report page). IBM, 2026. https://www.ibm.com/reports/data-breach (Global average cost of a data breach: USD 4.99 million.)

31. Cyber Threats Continue to Target SMEs, While Large Firms Face Greatest Costs: Report. Carrier Management, reporting the NetDiligence 2025 Cyber Claims Study, 2025. https://www.carriermanagement.com/news/2025/09/25/279803.htm (SME averages: $152,000 for crisis services, $264,000 per incident.)
32. Ransomware Marketplace Report Q4 2020. Coveware, 2021. http://coveware.com/2021/02/ransomware-marketplace-report-q4-2020/ (Average ransomware downtime of about 21 days in Q4 2020, across all company sizes; supports the top of the range.)
33. TISAX Participant Handbook. ENX Association, 2026. https://portal.enx.com/handbook/tisax-participant-handbook.html
34. Cybersecurity Maturity Model Certification (CMMC) Program, final rule, 89 FR 83092. U.S. Department of Defense, Federal Register, 2024. https://www.govinfo.gov/content/pkg/FR-2024-10-15/html/2024-22905.htm (Three-year Level 2 certification assessment cost: $104,670 for a small entity, $117,768 for others.)
35. How data breaches affect stock market share prices. Comparitech, 2024. https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/
36. Incident Response Retainer vs. On-Demand: A CFO's Guide to Breach Response. TrustedSec, n.d. https://trustedsec.com/resources/business-resources/incident-response-retainer-vs-on-demand (On-demand incident response at $300 to $600 per hour; page is undated.)
37. Zero Trust API Security. NetFoundry, 2026. https://netfoundry.io/api-security/ (Vendor figure; no published methodology.)
38. Zero Trust and Microsegmentation: An Integrated Framework for Robust Network Defense in Government Organizations, European Journal of Computer Science and Information Technology 13(47), Table 3. R. Tavva, 2025. https://eajournals.org/ejcsit/vol13-issue47-2025/zero-trust-and-microsegmentation-an-integrated-framework-for-robust-network-defense-in-government-organizations/ (The table draws on ColorTokens and Zero Networks implementation data.)
39. The State of Kubernetes Security. Red Hat, 2021. https://www.redhat.com/en/blog/state-kubernetes-security
40. Cost of a Data Breach Report 2022. IBM Security and Ponemon Institute, 2022. https://web.archive.org/web/20221227193727/https://www.ibm.com/downloads/cas/3R8N1DZJ (Archived copy; IBM's original link no longer resolves. The USD 1.51 million figure compares mature zero trust deployments with early-stage ones.)
41. SP 800-207, Zero Trust Architecture. National Institute of Standards and Technology, 2020. https://csrc.nist.gov/pubs/sp/800/207/final
42. Zero-Trust Networking. EmberNet Docs, Fireball Industries, 2026. https://docs.embernet.ai/docs/networking/zero-trust
43. Flux zero-trust networking. EmberNet Docs, Fireball Industries, 2026. https://docs.embernet.ai/docs/services/flux
44. Installation Guide. EmberNet Docs, Fireball Industries, 2026. https://docs.embernet.ai/docs/deployment/installation
45. EmberNet Endpoint. EmberNet Docs, Fireball Industries, 2026. https://docs.embernet.ai/docs/embernet-endpoint/overview
46. SSO Integration. EmberNet Docs, Fireball Industries, 2026. https://docs.embernet.ai/docs/platform/sso
47. EmberRTOS overview. EmberNet Docs, Fireball Industries, 2026. https://docs.embernet.ai/docs/emberrtos/overview
48. EmberRTOS: the real-time edge OS (hardware results). Fireball Industries, 2026. https://embernet.ai/emberrtos.html
49. About Fireball Industries: how a project runs. Fireball Industries, 2026. https://www.fireballz.ai/about
50. Solutions. Fireball Industries, 2026. https://www.fireballz.ai/solutions
51. OCR Active with Settlements and Enforcement Actions in November and Early December. Robinson+Cole Data Privacy + Security Insider, 2024. https://www.dataprivacyandsecurityinsider.com/2024/12/ocr-active-with-settlements-and-enforcement-actions-in-november-and-early-december/ (OCR actions of $100,000, $250,000, $325,581, $548,265, and $1.19 million.)
52. Genzyme Corporation, Current Report on Form 8-K (FDA consent decree). U.S. Securities and Exchange Commission, EDGAR, 2010. https://www.sec.gov/Archives/edgar/data/0000732485/000110465910030445/a10-9595_158k.htm ($175 million disgorgement under a cGMP consent decree, not specifically Part 11.)
53. Occupational Outlook Handbook: Computer Support Specialists, Pay. U.S. Bureau of Labor Statistics, 2026. https://www.bls.gov/ooh/computer-and-information-technology/computer-support-specialists.htm

WORK WITH FIREBALL

Start with a conversation.

Bring your cost per minute if you have it. If you don't, that is the first thing we will build together.

Fireball Industries designs and builds industrial automation, commissions it digitally before it reaches your floor, and supports it after startup. EmberNet is our platform for running and reaching that automation without opening the plant to the internet. Tell us what runs on your floor today and what keeps stopping it.

Email sales
info@fireballz.ai

Fireball Industries
fireballz.ai

EmberNet
embernet.ai

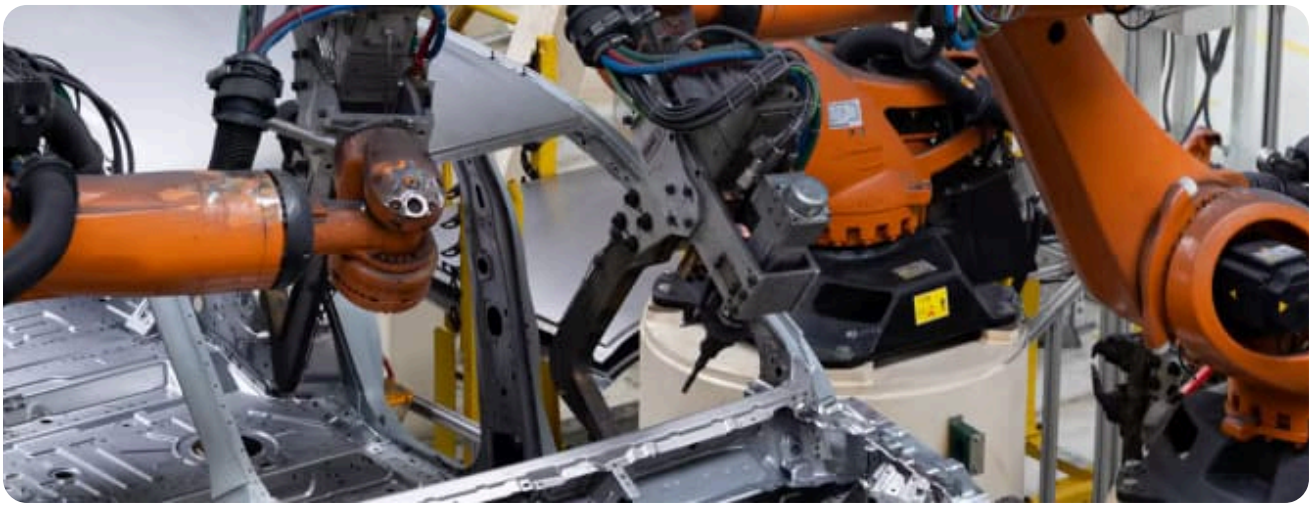

Figure 8. Robotic arms on a production line.

© 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 research, including IBM Security, Ponemon Institute, Gartner, Siemens, and regulatory agency publications. Specific company scenarios are hypothetical and intended for illustrative purposes only.