IMTS ZERO TRUST ISOLATION - EDGE™

Proactive Endpoint Protection Powered by Revolutionary Isolation Technology.

IMTS Research Labs (IRL)

IMTS
INNOVATIVE MANAGEMENT & TECHNOLOGY
SERVICES

2024

1. Executive Summary

IMTS Zero Trust Isolation - Edge™ delivers industry-leading endpoint protection by proactively containing threats before they can execute. Built with **Zero Trust principles** at its core, this solution isolates untrusted files, applications, and processes in secure virtual environments, ensuring endpoints remain uncompromised.

As a critical element of the **IMTS Zero Trust Framework™**, it integrates seamlessly with the **IMTS SecureSOC™ SOC Platform** to enhance visibility, streamline response, and deliver a Unified Threat Management (UTM) experience.

---

2. Key Features

1. Revolutionary Containment Technology

- Runs untrusted processes in secure, virtualized environments, ensuring no harm to the endpoint or network.
- Stops threats like ransomware, fileless malware, and zero-day exploits before they can execute.

2. Comprehensive Endpoint Security

- **NexGen Anti-Virus (NGAV):** Detects and blocks known and unknown threats using heuristic and signature-based methods.
- **Endpoint Detection and Response (EDR):** Provides real-time monitoring and rapid response to endpoint threats.
- **Host Intrusion Prevention System (HIPS):** Prevents unauthorized changes to critical systems and files.
- **Integrated Firewall:** Blocks unauthorized network activity and enforces strict security policies.
- **Fileless Malware Detection:** Identifies and neutralizes advanced memory-based attacks.
- **IMTS ThreatIQ™ Integration:** Enriches detection with global threat intelligence.

3. Proactive Threat Isolation

- Automatically identifies and isolates suspicious files and processes.
- Ensures seamless productivity by protecting users from malicious activity without interruptions.

4. SOC Integration for Streamlined Operations

- Logs and alerts integrate with the **IMTS SecureSOC™ SOC Platform** to provide centralized monitoring and analysis.

- Supports automated workflows through SOAR, reducing incident response times.

5. Lightweight and Scalable Design

- Designed to minimize system resource usage for uninterrupted user experiences.
- Scales effortlessly across SMBs, enterprises, and hybrid environments.

---

3. Technical Highlights

Feature	Description
Dynamic Threat Containment	Runs suspicious processes in isolated virtual environments, preventing harm to endpoints or networks.
Behavioral Analysis	Monitors runtime activity to detect malicious patterns and stop threats.
Kernel-Level Protection	Secures endpoints at the OS level, blocking unauthorized modifications.
Advanced NGAV and EDR	Combines detection and response with heuristic, signature, and behavioral analysis.
SOAR-Enabled Integration	Automates response workflows within the **IMTS SecureSOC™ SOC Platform**.

---

4. Benefits of IMTS Zero Trust Isolation - Edge™

1. **Proactive Threat Containment**:
   Neutralizes threats before execution, reducing the risk of compromise.
2. **Holistic Endpoint Security**:
   Integrates NGAV, EDR, HIPS, firewall capabilities, and behavioral monitoring.
3. **Enhanced SOC Efficiency**:
   Provides enriched threat intelligence and streamlined workflows via the **IMTS SecureSOC™ SOC Platform**.
4. **Lateral Movement Prevention**:
   Blocks attackers from spreading across networks, ensuring threats are contained at the endpoint.
5. **Cost Efficiency**:
   Reduces incident response costs through proactive containment and seamless SOC integration.

---

5. Real-World Use Cases

1. Ransomware Mitigation

- An untrusted file attempting to encrypt data is automatically contained in a virtual environment.
- SOC teams leverage logs and insights from the **IMTS SecureSOC™ SOC Platform** to respond and remediate the incident.

2. Zero-Day Attack Defense

- Suspicious behavior from a newly introduced application triggers containment.
- Isolation ensures no harm to the endpoint while forensic analysis confirms the threat.

3. Insider Threat Neutralization

- Unauthorized USB activity is flagged, isolated, and logged for SOC investigation, preventing data exfiltration.

---

6. Integration with the IMTS Zero Trust Framework™

IMTS Zero Trust Isolation - Edge™ is a foundational component of the **IMTS Zero Trust Framework™**, delivering:

1. **Never Trust, Always Verify:** Proactively isolates all unverified processes.
2. **Least Privilege Access:** Ensures only trusted applications and processes execute.
3. **Continuous Verification:** Monitors runtime behaviors to detect and neutralize emerging threats.

By seamlessly integrating with the **IMTS SecureSOC™ SOC Platform**, this solution extends endpoint security to align with the broader Unified Threat Management (UTM) strategy.

---

7. Why Choose IMTS Zero Trust Isolation - Edge™?

1. **Revolutionary Containment Technology:**
   Proactively stops threats, delivering real-time protection for modern threats like ransomware and zero-day attacks.
2. **Comprehensive Endpoint Security:**
   Combines advanced NGAV, EDR, HIPS, and isolation technologies to secure every endpoint.
3. **Seamless SOC Integration:**
   Fully integrates with the **IMTS SecureSOC™ SOC Platform** for visibility, response, and automation.

4. **Cost-Effective Protection:**
   Reduces operational overhead and improves SOC efficiency by neutralizing threats at the endpoint.
5. **Scalable and Lightweight:**
   Designed to protect organizations of any size with minimal impact on resources.

---

8. Contact Us

To learn more about **IMTS Zero Trust Isolation - Edge™**:

- **Email**: info@IMTS.US
- **Phone**: 800-988-1939
- **Website**: IRL.IMTS.US