IMTS SECURESOC™ & IMTS THREAT360™ OVERVIEW

Innovation for Next-Generation Security Powered by IMTS Zero Trust Framework™

IMTS RESEARCH LABS (IRL)

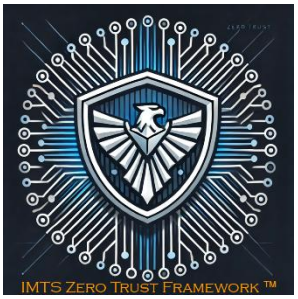
IMTS
INNOVATIVE MANAGEMENT & TECHNOLOGY
SERVICES

2024

Welcome to IMTS and IMTS Research Labs

IMTS Research Labs (IRL), founded in 2022, is the innovation arm of IMTS, dedicated to advancing solutions to meet our customers' most complex needs. Powered by the IMTS Zero Trust Framework™, our flagship offerings—IMTS SecureSOC™ and IMTS Threat360™—provide unparalleled endpoint, network, and cloud security. IRL is also responsible for the creation of and drives team readiness and operational excellence through platforms such as the IMTS Training Institute™ and its Government Training Center of Excellence™ and IMTS ThreatDetect™.

What is the IMTS Zero Trust Framework™ ?



The **IMTS Zero Trust Framework™** powers **IMTS SecureSOC™** and **IMTS Threat360™**, aligning with the three foundational principles of Zero Trust:

1. **Never Trust, Always Verify**: Applies **system-level validation** to files, applications, and devices through **Zero Trust Isolation™**, which blocks and isolates threats at the endpoint and host levels.
2. **Least Privilege Access**: Enforces strict user and system permissions, monitored continuously via **Zero Trust Visibility™**, to detect anomalies across networks, cloud platforms, and user behaviors.
3. **Continuous Verification**: Assumes threats may already exist and dynamically mitigates risks using **Zero Trust Containment™**, which facilitates rapid incident response and forensic analysis.

Core Features:

IMTS Zero Trust Isolation™

	Prevents and isolates threats at the endpoint, host, and network levels before they can spread or cause damage. By leveraging IMTS Zero Trust Isolation - Edge™, it proactively blocks threats and ensures system-level security, minimizing the attack surface.

IMTS Zero Trust Visibility™

Detects and monitors risks across networks, clouds, and user behaviors, providing actionable insights into potential vulnerabilities. Enhanced by IMTS ThreatIQ™ for global threat intelligence and Advanced Threat Hunting™, it delivers unparalleled real-time detection and risk assessment.	

IMTS Zero Trust Containment™

	. Ensures rapid containment of incidents to minimize downtime, mitigate data loss, and ensure compliance with regulatory standards. Enabled by effective SOAR workflows, it automates response actions and post-incident forensic analysis.

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.

Core Elements:

1. **IMTS Zero Trust Isolation™**

   - **Zero Trust Isolation - Endpoint™:** Powered by IMTS Zero Trust Isolation - Edge™, isolates threats at the endpoint to prevent lateral movement and compromises.
   - **Zero Trust Isolation - Host™:** Disconnects compromised hosts from network resources while maintaining SOC access for DFIR.

2. **IMTS Zero Trust Visibility™**

   - **Zero Trust Visibility - Network and Cloud™:** Monitors for anomalies across network traffic and cloud platforms like AWS, M365, and Azure AD.
   - **Zero Trust Visibility - IMTS ThreatIQ™:** Combines dynamic/static file analysis and integrated global intelligence to enrich IoCs and enhance threat response.
   - **Zero Trust Visibility - Advanced Threat Hunting™:** Proactively identifies vulnerabilities and attacker tactics using global telemetry and AI/ML-driven analytics.

3. **IMTS Zero Trust Containment™**

   - **Zero Trust Containment - DFIR™:** Facilitates post-incident analysis and rapid containment to minimize downtime and ensure compliance.

Why IMTS Zero Trust Framework™ is Unique

The number one source of compromise and security incidents is the **user**. While most frameworks focus on external threats, the **IMTS Zero Trust Framework™** uniquely addresses **insider risks**—trusted users who pose the greatest potential threat to an organization.

- **Foundation for Insider Risk Mitigation**: Enabled by **IMTS SecureSOC™ Base**, providing visibility into external and internal activity.
- **Enhanced Insider Protection**: Delivered through **SecureSOC™ Insider Edition**, with advanced tools like **IMTS ThreatDetect™** for UAM, UEBA, and DLP.
- **Fully Realized Zero Trust**: Achieved with **IMTS Threat360™**, combining internal and external threat management into a seamless **UTM-as-a-Service™** platform.

To learn more about how the IMTS Zero Trust Framework™ delivers comprehensive security for external and insider threats, read the full overview **here**.

What is IMTS SecureSOC™?

IMTS SecureSOC™ is a SOC-as-a-Service solution offering 24/7 threat detection and response with customizable tiers:

IMTS SecureSOC™ Base

- **Core Features**:

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.

- **Zero Trust Isolation - Endpoint™**: Enabled by **IMTS Zero Trust Isolation - Edge™**, part of our NextGen Endpoint Protection technology, it isolates threats at the endpoint to prevent system and network compromises, intrusions, incidents and lateral movement.
- **Zero Trust Isolation - Host™**: Cuts the host off from all other network resources while allowing SOC connectivity for DFIR.
- **Zero Trust Visibility - Network and Cloud™**: Provides anomaly detection and monitoring across network traffic and cloud platforms like AWS, M365, and Azure AD.
- **Zero Trust Visibility - IMTS ThreatIQ™:** Delivers dynamic and static analysis of unknown files, ensuring threats are neutralized before detection. Includes Integrated Global Intel—Leverages worldwide feeds to enrich IoCs and enhance threat response.
- **Zero Trust Visibility - Advanced Threat Hunting™:** Proactively identifies vulnerabilities and attacker tactics using global telemetry.
- **Zero Trust Containment - DFIR™ (Digital Forensics and Incident Response)**: Enables post-incident analysis and remediation aligned with compliance needs.
- **IMTS Service Desk™ (IMTS-SD™):** A centralized platform for case, ticket, and incident management, seamlessly integrated into the IMTS SecureSOC™ SOC Platform for end-to-end visibility and response coordination.
- **IMTS Remote Monitoring and Management™ (IRMM™):** enables **Zero Trust Isolation - Host™**, and t provides tools like remote desktop access, patch management, and system diagnostics to support advanced response and recovery actions.

IMTS SecureSOC™ Cyber

- **Includes all SecureSOC Base features**
- **Enhanced Features:**

1. **IMTS Secure Email Gateway (SEG)**:
    - Supports **Zero Trust Visibility™** by monitoring email traffic for anomalies.
    - Supports **Zero Trust Isolation™** by blocking phishing and email-based attacks.
2. **IMTS Secure Internet Gateway (SIG)**:
    - Extends **Zero Trust Visibility™** by monitoring web traffic for malicious sites and risky behaviors.
    - Implements **Zero Trust Isolation™** by and filtering web traffic and proactively blocking unsafe browsing activities.
3. **IMTS Mobile Device Management (MDM)**:
    - Integrates with **Zero Trust Isolation™** to lock, wipe, or reset mobile devices in response to potential threats.

IMTS SecureSOC™ Insider

- **Includes all SecureSOC Base features**
- Insider Threat UAM UEBA and DLP Powered by **IMTS ThreatDetect™**

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.

- **Advanced Features**:

    1. **Insider Threat Detection (UAM/UEBA):**

        - Enabling **Zero Trust Visibility™**, tracks user behavior and integrates with the SIEM to detect anomalies using **AI/ML-driven analytics** for advanced insights..

    2. **Insider Threat Mitigation (DLP, USB Control, Block Applications):**

        - Implements Zero Trust Containment™ to prevent unauthorized data transfers, insider disclosures, and risky device usage.

        - Uses **Zero Trust Isolation™** to proactively prevent unauthorized data transfers, insider disclosures, and risky device usage.

        - Enables **Zero Trust Containment™** by dynamically restricting actions during an unfolding incident to minimize its impact and prevent further escalation.

    3. **IMTS Mobile Device Management (MDM)**:

        - Integrates with **Zero Trust Isolation™** to lock, wipe, or reset mobile devices in response to potential threats.

    4. **Part of Unified Threat Management-as-a-Service™ (UTM-as-a-Service™):**

        - Leverages all aspects of the IMTS Zero Trust Framework™ to protect against insider and external threats while providing visibility, isolation, and containment across your organization.

What is IMTS Threat360™?

IMTS Threat360™ is an all-in-one UTM-as-a-Service™ combining the features of IMTS SecureSOC™ Cyber and IMTS SecureSOC™ Insider into a unified platform:

- **Mission Readiness Range (MRR) Silver Tier**: Includes 5 SaaS seats for training, labs, and compliance exercises. Additional seats available at discounted rates.
- **Complete UTM Coverage**: Seamlessly protects endpoints, networks, and clouds from internal and external threats.

Which option should I choose?

IMTS SecureSOC™ Base

- **Who It's For**:
    - Small to mid-sized businesses seeking affordable, foundational SOC services to defend against growing cyber threats.
    - Organizations with limited or no in-house IT security staff who need reliable 24/7 SOC monitoring and immediate threat response.

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.

- Companies taking their first steps toward adopting **Zero Trust Isolation** principles without the need for complex integrations.

IMTS SecureSOC™ Cyber

- **Who It's For**:
  - Businesses overwhelmed by the rise in external threats, including phishing, malware, and ransomware campaigns.
  - Teams needing secure internet browsing and email protection to safeguard communications and meet regulatory standards.
  - Companies looking to expand their security posture with enhanced XDR capabilities for **network and cloud monitoring**, gaining visibility into critical environments.

IMTS SecureSOC™ Insider

- **Who It's For**:
  - Organizations with insider risk concerns, such as **data exfiltration, unauthorized access**, or **misuse of sensitive data**.
  - Industries operating in **highly regulated environments** (e.g., finance, healthcare, government) requiring compliance with DLP and behavior-based analytics.
  - Teams looking for proactive insider threat management with tools like **UEBA, UAM**, and **USB Device Control**, integrated seamlessly with mobile device protection.

IMTS Threat360™

- **Who It's For**:
  - Enterprises needing comprehensive, **all-in-one security** for endpoints, networks, and clouds to manage both internal and external threats.
  - Organizations ready to consolidate fragmented tools into a single platform for unified threat management, saving costs and improving efficiency.
  - Security teams prioritizing **operational readiness** and compliance with access to **MRR.**

Why IMTS?

- Backed by **IMTS Research Labs**, our solutions leverage cutting-edge innovation to provide holistic security for organizations of all sizes.
- Our flexible pricing and advanced features outperform competitors, offering more capabilities at competitive costs for superior return on investment.

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.

Competitor Comparison Table

Feature	IMTS SecureSOC™ Base	IMTS SecureSOC™ Cyber	IMTS SecureSOC™ Insider	IMTS Threat360™	CrowdStrike Falcon Complete	SentinelOne Singularity Commercial	Teramind UAM + DLP	SentinelOne Vigilance MDR + DFIR	Everfox UAM + UBA
Zero Trust Isolation - Endpoint	✔	✔	✔	✔	✘	✘	✘	✘	✘
Zero Trust Isolation - Host	✔	✔	✔	✔	✘	✘	✘	✘	✘
Zero Trust Isolation - Mobile	✘	✔	✔	✔	Add-On	Add-On	✘	Add-On	✘
Zero Trust Visibility - Network	✔	✔	✔	✔	✘	✘	✘	✘	✘
Zero Trust Visibility - Cloud	✔	✔	✔	✔	✘	✘	✘	✘	✘
Endpoint Protection (EDR)	✔	✔	✔	✔	✔	✔	✘	✔	✘
Insider Threat Detection (UAM/UEBA)	✘	✘	✔	✔	✘	✘	✔	✘	✔
Insider Threat Mitigation (DLP, USB Control)	✘	✘	✔	✔	✘	✘	DLP Only	✘	✘
Secure Email Gateway (SEG)	✘	✔	✔	✔	Integration	Integration	✘	✘	✘
Secure Internet Gateway (SIG)	✘	✔	✔	✔	✘	✘	✘	✘	✘
Mission Readiness Range (MRR)	Add-On	Add-On	Add-On	**Silver Tier (5 Seats)**	✘	✘	✘	✘	✘
Pricing (Per Device / Month)	**$16.67**	**$30.00**	**$32.00**	**$40.00**	**$16.67**	**$17.50 + Add-On**	**$32.00**	**$48.00**	**~$32.00**

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.

How do you get started and what happens next?

1. Email us with any questions
2. We Schedule a call at your convenience
3. We do a discovery and consulting meeting
4. We prepare a proposal

Contact Us

- **Website**: IRL.IMTS.US | IMTS.US
- **Email**: info@IRL.IMTS.US | info@IMTS.US
- **Phone**: 800-988-1939
- **Address**: 7764 Armistead Rd, STE 160, Lorton, VA 22079

Trademark Notice

All trademarks, including the following, are the trademarks of Innovative Management and Technology Services, LLC (LLC):

- IMTS Zero Trust Framework™
- IMTS Zero Trust Isolation™
    - Zero Trust Isolation - Endpoint™
        - Powered by Trust Zero Trust Isolation - Edge™ (ZTIE™)
    - Zero Trust Isolation - Host™
- IMTS Zero Trust Visibility™
    - Zero Trust Visibility - Network™
    - Zero Trust Visibility - Cloud™
    - Zero Trust Visibility - IMTS ThreatIQ™
    - Zero Trust Visibility - Advanced Threat Hunting™
- IMTS Zero Trust Containment™
    - Zero Trust Containment - DFIR™
- IMTS SecureSOC™
- IMTS Threat360™
- IMTS ThreatDetect™
- IMTS Training Institute™
- Unified Threat Management-as-a-Service™
- UTM-as-a-Service™
- Government Training Center of Excellence™ (GT-COE™)
- IMTS Secure Email Gateway™ (ISEG™):
- IMTS Secure Internet Gateway™ (ISIG™):
- IMTS Mobile Device Management™ (IMDM™)
- IMTS Remote Monitoring and Management™ (IRMM™)
- Mission Readiness Range™ (MRR™)
- IMTS Service Desk™ (IMTS-SD™)

© 2024 Innovative Management and Technology Services, LLC. All rights reserved.