IMTS SOC-AS-A-SERVICE, UTM-AS-SERVICE AND NOSC-AS-AS-SERVICE OVERVIEWS

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

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™, IMTS Threat360™, IMTS NOSC™ and IMTS iNOSC™—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™.

IMTS NOCIT-as-a-Service and NOSC-as-a-Service Overview

Introduction

IMTS delivers industry-leading IT operations and security solutions through **IMTS NOCIT-as-a-Service™** and **NOSC-as-a-Service™** offerings. These solutions address the challenges of IT infrastructure management, security operations, and insider threat detection within a seamless, scalable framework.

This overview introduces:

1. **IMTS NOC-IT™:** A standalone **NOCIT-as-a-Service™** solution providing proactive IT monitoring and support.
2. **IMTS NOSC™:** A **NOSC-as-a-Service™** offering combining IT operations and advanced security capabilities.
3. **IMTS iNOSC™:** A premium **NOSC-as-a-Service™** solution integrating **Threat360™** for unified threat management and insider threat detection.

For more details about SecureSOC™ Cyber and Threat360™, visit IRL.IMTS.US. For more details about SecureSOC™ Cyber and Threat360™, visit IRL.IMTS.US—We have included most details after the NOSC-as-a-Service™ section. The detailed competitor table at the end of this document illustrates how IMTS solutions surpass industry alternatives in both features and value, demonstrating our unique ability to meet and exceed modern IT and security demands.

IMTS NOCIT-as-a-Service

IMTS NOC-IT™ Features

IMTS NOC-IT™ delivers a robust suite of IT operations and support capabilities designed to ensure seamless network monitoring, infrastructure management, and end-user support. Built with scalability and efficiency in mind, IMTS NOC-IT™ empowers organizations to optimize their IT ecosystems while minimizing downtime. By integrating proactive monitoring, advanced troubleshooting, and responsive service desk support, IMTS NOC-IT™ provides comprehensive solutions tailored to meet modern IT demands. Below are the key features that distinguish IMTS NOC-IT™ as a leading NOCIT-as-a-Service offering.

Feature	Description
Workstation Issues and Maintenance	Troubleshooting and resolving workstation hardware and software issues.

Feature	Description
Virtual Server Maintenance	Maintenance and management of virtual servers.
Patch Management	Regular updates to maintain system security and software compliance.
Network and Server Notifications & Reports	Proactive monitoring and reporting on network and server health.
Account Unlocks	Assistance with unlocking user accounts.
AD User and Computer Setup/Domain Changes	Managing Active Directory accounts and domain-related changes.
Email Client Issue Resolution	Troubleshooting and configuring email client applications.
End-User Software Install/Uninstall	Installing, uninstalling, and activating software licenses for end users.
Office 365 User Setup and Troubleshooting	Assistance with setting up and resolving issues related to Office 365 accounts.
Monitors and Other Connected Devices	Setup and troubleshooting of peripherals like monitors, keyboards, and mice.
New Active Directory Accounts	Creating and configuring new AD accounts.
Password Resets	Assistance with resetting user passwords.
PC Troubleshooting and Maintenance	Resolving driver issues, updates, and general system optimization.
Phone Troubleshooting & Setup	Setting up and resolving issues with phone systems.
Printer Setup and Installation (PC Side)	Configuring printers and resolving connection issues.
Printer/Scanner Issues	Troubleshooting and resolving printer/scanner problems.
Server Software Install/Uninstall	Installing and uninstalling server-based applications.
Smartphone Email Troubleshooting	Configuring and troubleshooting email access on smartphones.
Support Center Ticket Resolutions	Resolving issues logged through the support center.
Wireless Networks	Managing and troubleshooting wireless network connectivity.

Additional Tier 3 Support:

- Advanced services, such as server migrations, firewall setups, and network switch configurations, are available upon request at **$175/hour**.

Price: $16.67 per device per month (working hours support: 9–5 M-F). For 24x7 monitoring and response add $10 per device per month.

Positioning:
IMTS NOC-IT™ is ideal for organizations seeking a foundational IT operations solution without integrated security capabilities.

IMTS NOSC-as-a-Service™

IMTS NOSC™ Features

IMTS NOSC™ combines the strengths of advanced IT operations and cybersecurity to deliver an integrated Network Operations and Security Center solution. Designed for organizations requiring comprehensive management of IT infrastructure and robust protection against evolving cyber threats, IMTS NOSC™ leverages state-of-the-art tools and methodologies. By uniting proactive network monitoring, IT support, and advanced SOC capabilities, IMTS NOSC™ ensures seamless operations, enhanced security, and business continuity. The following features highlight why IMTS NOSC™ stands out as a premier NOSC-as-a-Service solution.

Feature	**Description**
IMTS NOC-IT™	Includes all features of the IMTS NOC-IT™ solution.
IMTS SecureSOC™ Cyber Features:	
Zero Trust Isolation - Endpoint™	Enabled by IMTS Zero Trust Isolation - Edge™, 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 intelligence feeds to enrich IoCs.
Zero Trust Containment - DFIR™	Enables rapid containment of incidents and post-incident analysis and remediation aligned with compliance needs.
Secure Email Gateway (SEG)	Monitors email traffic for phishing attempts and email-based attacks, proactively blocking malicious messages.
Secure Internet Gateway (SIG)	Filters unsafe web traffic and proactively blocks risky browsing behaviors and malicious websites.
Mobile Device Management (MDM)	Integrates with Zero Trust Isolation™ to lock, wipe, or reset mobile devices in response to detected threats.
Advanced Threat Hunting	Uses AI/ML-driven analytics and manual techniques to identify vulnerabilities, suspicious activities, and attacker tactics.
Digital Forensics and Incident Response (DFIR)	Provides post-incident analysis to identify root causes, mitigate future risks, and streamline remediation efforts.

Price: $48 per device per month.

Positioning:
IMTS NOSC™ integrates IT operations and security to deliver a unified solution for enterprises requiring combined NOC and SOC capabilities.

IMTS iNOSC™ Features

IMTS iNOSC™ represents the pinnacle of integrated IT and cybersecurity services, merging advanced Network Operations and Security Center capabilities with insider threat detection and response. Tailored for organizations that demand comprehensive IT management, robust cybersecurity, and proactive threat mitigation, IMTS iNOSC™ leverages the power of unified threat management to protect assets and ensure operational excellence. With its premium feature set, IMTS iNOSC™ offers unparalleled visibility, control, and protection for critical IT environments. Below are the key features that establish IMTS iNOSC™ as a cutting-edge NOSC-as-a-Service solution.

Feature	Description
IMTS NOC-IT™	Includes all features of the IMTS NOC-IT™ solution.
IMTS SecureSOC™ Cyber Features:	Includes all features listed above under IMTS NOSC™.
Insider Threat Detection and Response Features:	
User Activity Monitoring (UAM)	Tracks user behaviors and detects anomalies using AI/ML.
User and Entity Behavior Analytics (UEBA)	Identifies risky user actions and potential insider threats.
Data Loss Prevention (DLP)	Prevents unauthorized transfers of sensitive data.
USB and Device Control	Restricts risky device usage to prevent data leaks.

Price: $58 per device per month.

Positioning:
IMTS iNOSC™ is the premium solution for enterprises requiring seamless IT operations, advanced security integration, and insider threat management.

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.

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.

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.

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**:
    - **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 as well as** Insider Threat UAM UEBA and DLP**.**
- **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.

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.

Expanded Competitor Comparison Table

Feature/Capability	IMTS SecureSOC™ Base	IMTS SecureSOC™ Cyber	IMTS SecureSOC™ Insider	IMTS NOSC™	IMTS iNOSC™	CrowdStrike Falcon Complete	SentinelOne Singularity Commercial	Teramind UAM + DLP	SentinelOne Vigilance MDR + DFIR	Everfox UAM + UBA
NOC-IT: Infrastructure Monitoring	✗	✗		✓	✓	✗	✗	✗	✗	✗
NOC-IT: Infrastructure Operations	✗	✗		✓	✓	✗	✗	✗	✗	✗
NOC-IT: Desktop Support	✗	✗		✓	✓	✗	✗	✗	✗	✗
NOC-IT: Helpdesk Support	✗	✗		✓	✓	✗	✗	✗	✗	✗
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)	✗	✗	✓	✗	✓	✗	✗	DLP Only	✗	✗
Secure Email Gateway (SEG)	✗	✓	✓	✓	✓	Integration	Integration	✗	✗	✗
Secure Internet Gateway (SIG)	✗	✓	✓	✓	✓	✗	✗	✗	✗	✗
Mission Readiness Range (MRR)	Add-On	Add-On	Add-On	Add-On	Add-On	✗	✗	✗	✗	✗
Pricing (Per Device/Month)	$16.67	$30.00	$32.00	$48.00	$58.00	$16.67	$17.50 + Add-On	$32.00	$48.00	~$32.00

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.

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):

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