Managed SD-WAN with Threat Monitoring and Response (TMR)

Agile enterprise connectivity with 24/7 cybersecurity protection

Product Sheet: SD-WAN Secure

COMCAST BUSINESS

MASERGY

What is TMR and why is it critical to SD-WAN?

Introducing SD-WAN connectivity into any environment increases the number of potential attack vectors into that network.

TMR provides 24/7 real-time security alert monitoring by certified security analysts via Masergy's SD-WAN Secure hardware endpoint with Unified Threat Protection (UTP), TMR deployed in tandem with Masergy's Managed SD-WAN service without any additional customer premise equipment. This includes full visibility of these new attack vectors as well as providing expanded monitoring coverage for both north/south and east/west network traffic throughout the enterprise.

Service Delivery Overview

- Masergy leverages security best practices for Incident Response (IR) workflow (including NIST 800-61)
- All UTP alerts follow pre-defined workflow as defined by a select catalog of IR playbooks
- These playbooks are supported within Masergy's Security Orchestration Automation and Response (SOAR) Platform to enable accelerate and optimize response effectiveness
- UTP alerts enter the SOAR platform via the event and alert management module, all alerts are correlated against Masergy's Global Threat Intelligence data and enriched with 100+ additional sources of threat intelligence data
- Masergy's tenured SOC analysts triage these alerts in real-time, 24/7, making expert assessments and taking any needed responses on your team's behalf, including pushing firewall blocking rules to stop any threats
- If additional customer action is needed, our analysts will contact you with actionable information and guide your team through any steps to fully mitigate the threat
- Risk metrics and alerts from the Incident Response (IR) workflow may be monitored via the Masergy customer portal

Deep Domain Expertise:

45B

security events analyzed annually

200+

full-time industry certified analysts

20+

years of network and threat data

3

SOCs & NOCs across three continents

FORTINET Network Security Expert

PCI Security Standards Council APPROVED SCANNING VENDOR

GIAC

CISSP

CEH Certified Ethical Hacker

CompTIA Security+

Contact Us: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com

Managed SD-WAN with Threat Monitoring and Response (TMR)

Product Sheet: SD-WAN Secure

COMCAST BUSINESS MASERGY

TMR Solution Requirements:

Masergy SD-WAN with Next Generation Firewall (NGFW) and Unified Threat Protection (UTP) included

Solution Capability Highlights

- UTP security is powered by Fortinet FortiGuard, an advanced analytics and artificial intelligence (AI) cybersecurity feature installed on FortiGate hardware endpoints which includes:
    - Up-to-the minute threat intelligence in real time to stop the latest threats
    - Insight into occurring threats anywhere in the world through a global network of more than three million sensors
    - Fast and comprehensive intelligence via automated and advanced analytics (such as machine learning) being applied to cross-discipline information
    - Prevention of exploitation of new avenues of attack with proactive threat research

- Fortinet UTP with Next-Generation Firewall (NGFW) and security processor technology provides comprehensive visibility and advanced layer 7 capabilities, including:

    - **Intrusion Prevention System (IPS)** – Powered by purpose-built hardware, the IPS functionality of Masergy SD-WAN with TMR is an industry-proven network security solution that includes:
        - Validated best-in-class security and capacity with proven coverage and high performance
        - Comprehensive protection provided by a signatures-based IPS engine, protocol anomaly scanning, and DDOS mitigation
        - IPS is kept up-to-date by research teams that work 24 hours a day worldwide, in order to detect and deter the latest known threats including zero-day attacks
        - Both signature and anomaly-based detection techniques are leveraged, with the latest threat intelligence updates pushed to the Masergy SD-WAN hardware in near real-time
        - Comprehensive IPS library with thousands of signatures, including the latest defenses against stealthy network-level threats

    - **Anti-Malware/Antivirus** – Built into the Masergy SD-WAN with TMR hardware, this high-performance network detection engine stops advanced malware before it even enters your enterprise network. Using industry-leading detection engines to prevent both new and evolving threats from gaining a foothold in the network including viruses, spyware, worms, Trojans, and other malware.
        - Automated content updates & latest malware and heuristic detection engines
        - Proactive threat library protects against all known threats and variants.
        - Content Pattern Recognition Language with patented code recognition software protects against unknown variants

Solution Capability Highlights (continued)

- **Web Content Filtering:** Web filtering is designed to restrict or control the content a reader is authorized to access, delivered over the Internet via the web browser.
    - Masergy TMR leverages Fortinet's massive web-content rating databases power one of the industry's most accurate web filtering services
    - Granular blocking and filtering provide web categories to allow, log, or block based on internet usage policies
    - Wide choice of web filtering technologies - Various web filtering technology options are available to provide each organization the most suitable implementation
    - Integrated secure web proxy blocks and alerts by employee username on inappropriate and insecure web usage, such as: adult, gambling, hacking, discriminatory sites
    - Comprehensive URL database provides rapid and comprehensive protection against all active malicious URLs
- **Application Control:** Application control technologies detect and take action against network traffic based on the application that generated the traffic. Application control uses protocol decoders with signatures that analyze network traffic to detect application traffic, even if the traffic uses nonstandard ports or protocols.
    - Protects your organization better by blocking or restricting access to risky applications via blacklists and whitelists
    - Gives you visibility and control of thousands of applications and lets you add custom applications
    - Enables you to fine-tune your policies based on application type via application categories
    - Optimizes bandwidth usage on your network by prioritizing, de-prioritizing, or blocking traffic based on application
    - Flexible policies enable full control of attack detection methods
- **Data Leak Prevention (DLP):** The Fortinet-powered data leak prevention (DLP) system allows you to prevent sensitive data from leaving your network. You configure the DLP system by creating individual filters based on file type, file size, a regular expression, an advanced rule, or a compound rule, in a DLP sensor and assign the sensor to a security policy, data matching these patterns will be blocked, or logged/allowed when passing through the Fortinet-powered Masergy Managed SD-WAN endpoint hardware.

  Although the primary use of the DLP feature is to stop sensitive data from leaving your network, it can also be used to prevent unwanted data from entering your network and to archive some or all of the content passing through the Masergy SD-WAN Secure endpoint hardware.

Managed SD-WAN with Threat Monitoring and Response (TMR)

Product Sheet: SD-WAN Secure

COMCAST BUSINESS MASERGY

Solution Capability Highlights (continued)

- **SSL Content Scanning & Inspection:** Secure Sockets Layer (SSL) content scanning and inspection allows you to apply antivirus scanning, web filtering, FortiGuard Web Filtering, and email filtering to encrypted traffic. To perform SSL content scanning and inspection, the FortiGate unit does the following:
  - Intercepts and decrypts HTTPS, IMAPS, POP3S, SMTPS, and FTPS sessions between clients and servers
  - Applies content inspection to decrypted content, including:
  - HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and DLP archiving
  - HTTPS web filtering and AI-powered web filtering powered by FortiGuard Labs
  - IMAPS, POP3S, and SMTPS email filtering
  - Encrypts the sessions and forwards them to their destinations

Additional Service Benefits

- Masergy's implementation of Fortinet's UTP security combines industry leading security capabilities with Masergy's high performance Secure SD-WAN networking into a single appliance for low total cost of ownership (TCO) and simple deployment
- All Masergy SD-WAN network deployments includes Shadow IT detection and alerting. All high-risk Shadow IT alerts are incorporated included into the TMR security monitoring service which includes appropriate incident response and/or active blocking of unwanted suspicious activity
- Masergy Threat Monitoring and Response solution retains privacy-protected log files, security tickets, and alerts for a period of one year to provide rich, historical data used by our proprietary machine learning algorithms for detailed forensic threat analyses and response. All supporting security event data is retained for 30 days

FortiGuard Labs

Contact your Masergy representative for more information

Contact Us: USA +1 (866) 588.5885 | UK +44 (0) 207 173 6900 | sales@masergy.com