Highlights

Our business is growing, along with our vineyard. Reach out and let us know how we can best serve your needs, from marketing to sales enablement, consulting, training, resource management. One of our strengths is writing – from all aspects of digital marketing, to white papers, research and competitive analysis, market reports, sales collateral. We can create resource collateral, edit existing documents, assist in cohesive messaging, implement processes, develop BOD and investor reports, highlight your strengths, differentiate you from your competitors, and create synergies to maximize value of your investments across all departments.

In the meantime, enjoy a relaxing summer, we will see you at Flash Memory Summit, and cheers to a culvating a fruitful harvest!

Mike Heumann

Managed Security Service Providers (MSSPs)

Posted by Mike Heumann, July 6, 2023

Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) are both third-party organizations that provide services to a company. Traditionally, MSPs deliver general network and IT support. MSSPs provide managed network and other security services. Services include 24/7 threat monitoring, firewall management, patch management, security audits, incident response.

An MSSP is intended to augment or replace an organization's internal security team. In North America, more than 80% of MSPs cite cybersecurity as a primary growth driver of their business.

The line between MSP and MSSP is disappearing as MSPs are picking up more and more security-related functions and MSSPs now serve all sized businesses, not just very large corporations. According to the 2023 State of the MSP report: "Cybersecurity is still a very large area for growth. While services for ransomware and phishing/email security remain the top focus for MSPs, others are finding further growth offering services around expanding reporting, auditing, training, and policy building for clients." This is likely to become a key business differentiator in the next decade. But packaging and reselling security products alone is not going to cut it. They need to transform into trusted security advisors. According to Gartner, "by 2025, 60% of organizations will use cybersecurity risk as a primary determinant in conducting third-party transactions and business engagements." By 2028, the value of the managed security services market is expected to be $56.6 billion.

	MSP	MSSP	In-House
Focuses on:	Technology	Security	Operations
Manages and monitors:	The health of technology	Network security 24x7x365	Technology and security during business hours
Visibility into:	No compliance reporting	Provides compliance reporting	No compliance reporting
Tech experts are trained to:	Fix technology and systems health	Detect and respond to security threats	Keep tech environment operating
SLAs around:	Response times, replacements, availability	Alerting, investigation, security systems, availability	Ensure operations is running

MSSP benefits:

- Partnering with an MSSP enables an organization to fill gaps within its internal security team or to replace it entirely. There is a cybersecurity workforce gap of 3.4 million people.
- Specialist Expertise
- Round-the-Clock Protection
- Increased Security Maturity
- Solution Configuration and Management
- Lower Cost: MSSP can use the same solution to support multiple clients, spreading the cost of a robust cybersecurity infrastructure across their client base.
- Compliance Support: An MSSP can help with collecting data and generating reports for demonstrating compliance during audits or after a potential incident.

Challenges that security leaders are facing today:

- How can I get full visibility into what is happening in my environment?
- How can I detect potential misconfigurations and vulnerabilities?
- How can I prioritize among the ever-growing list of priorities?
- How can I quickly and efficiently respond to threats in my organization?
- What threats are unique to my organization?

Categories of Managed Services in IT Security include on-site consulting, perimeter management of the client's network, managed security monitoring, penetration testing and vulnerability assessments, and compliance monitoring.

In finding a reliable managed security services provider, Robert Napoli highlights the importance of 1) evaluating a prospective MSSP's expertise and experience including factors such as their years of operation, track record, staff certifications and experience, and specialized knowledge in your industry or specific security challenges; 2) assess service offeringsto ensure they align with your specific security needs. Look for 24/7 monitoring capabilities, robust incident response procedures, vulnerability assessments, and other essential services tailored to your organization; 3) evaluate security technologies and infrastructure. They should have advanced threat detection and prevention tools and a robust infrastructure to protect your data and ensure service availability; 4) compliance and certifications relevant to your sector is crucial. Check if they hold certifications such as ISO 27001, SOC 2, or PCI DSS, demonstrating their commitment to security best practices and compliance standards; and 5) Incident response capabilities, among other recommendations.

Comparison of Top MSSP Vendors

Posted by Karen Heumann, July 6, 2023

Comparison of Top MSSP Vendors

1. Cipher
   Cipher was established in 2000, has around 300 employees, annual revenue of $20-50M, and is based in Miami, Florida. Cipher was acquired by Prosegur in February 2019. Prosegur has 175k+ employees.
   Services Provided: Cybersecurity Monitoring, Incident Management & Cyber Defense, Security Asset Management, Vulnerability & Compliance Management, Managed Application Security
   Industries: Credit Unions, Financial Services, Hospitality, Manufacturing, Healthcare

2. ScienceSoft
   ScienceSoft was established in 1989, has 700+ employees, and $32M revenue.
   Services Provided: Network protection, cloud security, vulnerability management, security monitoring, threat detection, incident response, compliance management.
   ScienceSoft's team includes security and compliance consultants, cloud security specialists, certified ethical hackers, and SIEM/SOAR experts.

3. SecurityHQ
   SecurityHQ was established in 2003, has 300 employees, with office across the United Kingdom, the Middle East, Americas, India, and Australia.
   Services Provided: Managed Detection and Response (MDR), Managed Firewall, Managed Endpoint Detection & Response (EDR), Digital Risk & Threat Monitoring, Managed Endpoint Protection (EPP)
   Managed Network Detection & Response (MNDR), Managed Azure Sentinel Detection & Response, Vulnerability Management Service, Penetration Testing Service, Web Application Security Testing, Managed Data Security- Managed Data Security, powered by IBM Guardium, User Behaviour Analytics (UBA), Network Flow Analytics, Managed Microsoft Defender ATP

Service Trials: SecurityHQ offers a Free 30-Day trial (POC/POV) for its services.

4. Security Joes

   Security Joes was recently established, in 2020, and provides services including 24/7 Incident Response, Crisis Management & Follow-The-Sun MDR (Managed Detection & Response), Compromise Assessment, External Attack Surface, Red Team, Phishing Simulations, Malware Analysis, Threat Hunting, Threat Intelligence, Vulnerability Management

5. SecureWorks

   SecureWorks has 300+ employees, annual revenue of $4.3M, and was established in 1999.
   Services Provided: Advance threat protection, compliance management, critical asset protection, cybersecurity risk management, security operations, industries.
   SecureWorks provides the following solutions:
   Enterprise network monitoring: Comprised of Advanced Malware Detection & protection (AMDP), Managed Firewall, Managed IDS/IPS, iSensor
   Endpoint Security: Encompassed of Advanced Endpoint Threat Detection (AETD), Enhanced Endpoint Threat Prevention (AETP), Supervised Server Protection
   Vulnerability Management: Advanced Vulnerability Scanning, Managed Web application scanning, Managed policy compliance, PCI Scanning, Vulnerability threat prioritization
   Security Monitoring: Comprised of Log management
   Combined Solutions: Comprised of managed detection and response

6. IBM

   IBM has an annual revenue of $79B, locations in 170+ countries, and was established in 1911.
   Services Provided: Cloud Computing, Business Consulting, Technology services, financing, industry expertise, training & skills.
   IBM provides the following Managed Services: firewall management, vulnerability scanning from IBM Security, information event management, intelligent log management on cloud, intrusion detection and prevention system management, managed data protection services for Guardium, endpoint security services, IBM X-Force cloud security service, Amazon GuardDuty services, Security SD-WAN, Unified Threat Management, Technology Bundle, Security intelligence analyst, Security-rich web gateway management

7. Verizon

   Verizon has 155k+ employees, $129.6B+ annual revenue, and was established in 2000.

Products & Services Provided: Mobility, Internet of Things, Networks and Internet, IT solutions and Cloud, Business communications, Security

Services: Round the clock security expertise, review of incident information, data analysis with log management., In-depth inspection of incident trends, Intelligence-driven security monitoring and analysis.

8. Symantec

   Symantec was established in 1982, has 10k+ employees, and annual revenue of $2-5B.

   Products & Services Provided: Integrated Cyber Defense, Advanced Threat Protection, Information Protection, Endpoint Security, Email Security, Network Security, Cloud Security, Cybersecurity Services.

   Symantec solutions include: Continual 24/7 advanced threat monitoring, DeepSight intelligence, Incident response services, Indicators to detect advanced persistent threats, Retroactive log analysis.

9. Trustwave

   Trustwave was established in 1995, has 1-5k employees, and $190.4M annual revenue.

   Products: Network security, content & data security, endpoint security, security management, database security, application security.

   Trustwave provides the following services:

   Threat Management: This covers managed threat detection, managed SIEM, managed two-factor authentication, managed UTM, managed Email security, SSL service lifecycle management, incident response & readiness, etc.

   Vulnerability Management: Managed security testing, application scanning, managed Web application firewall, network vulnerability scanning, database & big data scanning.

   Compliance Management: This covers Risk Assessment, PCI compliance, security awareness, and security awareness education.

10. AT & T

    AT&T has 10k+ employees, $10B+ annual revenue, and was established in 1983.

    Products & Services Provided: Mobility Services, Network services, Internet of things, voice & collaboration, cybersecurity services, cloud services, Wi-Fi, DIRECTV for Business. AT&T Security Services aid in identifying, preventing and alleviating the loss caused by cyber-attacks and business interruptions.

AT&T security services include: Internet protection, DDoS Defense, private intranet protect, mobile security, firewall security, network-based firewall, web application firewall, Intrusion detection/prevention service, secure email gateway, endpoint security, web security service, premises-based firewall, encryption services, token authentication services, security analysis and consulting solutions.

How to Stand Out as an MSSP

Posted by Mike Heumann, July 6, 2023

5 ways MSSPs can differentiate themselves in the market

1. Use Automation to Address the Cybersecurity Skills Gap
2. Provide a Holistic Approach to Cybersecurity: a wider range of cybersecurity services, consult on policy creation and enforcement, conduct training sessions, showcase advanced and easy-to-consume reports, become an expert in compliance, offer bundled services, take a consultative approach, provide both strategic and hands-on services (vCISO), customize your offerings, focus on providing solutions to their problems, rather than just delivering products.
3. Focus on Prevention- Conduct risk assessments to identify potential security risks and vulnerabilities, provide security awareness training to avoid common security threats, continuous reporting and monitoring, and update the security strategy based on changing clients' business needs and the network.
4. Deliver a Good Customer Experience- Clearly define the scope of services, set expectations with customers regarding the expected level of service, keep clients informed, have a skilled staff or resources, and use the latest security technologies. Provide regular, consistent and objective reports about system and strategy status and effectiveness. Select vendors that will help you provide such high-quality services and will naturally expand on your existing capabilities to help you deliver superior service and show the value of your services consistently.
5. Offer Competitive Pricing- To offer competitive pricing without compromising on quality, leverage automated solutions, as well as AI and ML, to reduce manual processes and improve

operational efficiency. Automation and AI can automate routine tasks like data entry or administration, assist with data analysis, and provide insights that help with decision-making.

G2M Research Multi-Vendor Webinar Series

Our webinar schedule is below. We are offering a Cybersecurity series and an Enterprise Storage & Technology multivendor series.

"The Need for Speed: NVMe™, NVMe-oF™, and Data Processing Accelerators" webinar featured Tony Afshary, Vice President, Products and Marketing at Pliops; Rob Davis, Vice President of Storage Technology at NVIDIA; and Peter Onufryk, Intel fellow for NVMexpress. Companies are focused on storage/networking/processing acceleration. Higher-level networking protocols and custom protocols for specific workloads require "offloads" to lower CPU utilization and increase application performance. Advanced storage capabilities such as those offered by NVMe and NVMe-oF can also tax CPUs, reducing cycles available for workloads. And then there is security, data resilience, and other very real needs that take CPU cycles away from workloads. This webinar explored where non-hyperscalers go to accelerate their workload in the same way hyperscalers do. The webinar video is available to view and a copy of the slidedeck is available here.

Interested in a custom webinar? Contact **G2M** for a prospectus. We can create a custom webinar, custom webinar series, and add or modify topics to specifically appeal to your target audience. View our webinars and access slide deck presentations on our website.

Upcoming Conferences

July 14-19	School Transportation Network Expo, Reno, NV
August 5-10	Black Hat USA, Las Vegas
August 8-10	Flash Memory Summit, Santa Clara, CA
August 28-31	VMWare Explore, San Francisco, CA
August 30-Sept 1	Security Expo, Sydney, Australia
September 11-13	Gartner Security & Risk Management, London
September 11-13	Global Security Exchange, Dallas, TX
September 18-20	Crowdstrike fal.con, Las Vegas
September 18-21	SDC 2023, Fremont, CA
October 2-4	DattoCon, Miami, FL
October 3-4	CyberTech Europe, Rome
October 16-19	Gartner IT Symposium/Xpo, Orlando, FL
November 15-16	Microsoft Ignite, TBD
Nov 27- Dec 1	AWS re:Invent, Las Vegas