

MSSP Market Overview

Information Systems Security Association

Central Maryland Chapter

July 22, 2020



Speaker Bio



- **Name:** John Perkins
- **Title:** Principal and Founder of Threat Angler, LLC
- **Education:** MBA in Leading Organizational Change, Master of Science in Information Assurance
- **Certifications:** CISSP, CISM, ITIL, Azure, ServiceNow, Carbon Black, Tenable, Rapid7, Splunk
- **Employment:** Federal Reserve, Optiv, GuidePoint, Insight
- **Experience:** Serviced over 400 MSSP clients across 5 MSSPs

Topics

- Target Audience
- MSSP Defined
- Market Segments
- Services
- Platforms
- Service Models
- Market Disruptors

Target Audience

- Cybersecurity professionals prospecting for employment with an MSSP
- Cybersecurity professionals already employed with an MSSP and wondering if the grass is greener
- Businesses considering subscribing to MSSP
- Businesses questioning whether their current MSSP is the right fit
- New MSSPs still learning how they fit into the MSSP ecosystem
- The curious

Use this information as a guide and to generate new thoughts and ideas. It is not a perfect science.

MSSP Defined

MSSP

*"A managed security service provider (**MSSP**) provides outsourced monitoring and management of security devices and systems."*

- Gartner

MSSP vs MSP

MSP, or Managed Service Provider, delivers IT services that may or may not include cybersecurity related outcomes.

Managed Service

- Somewhere in between outsourcing and staff augmentation.
- Force multiplication is the expectation.
- Subscription based pricing often is the key differentiator from non-managed services.

Market Segments

Scraps

A wide variety of clients, often those the bigger players do not focus on (the "scraps")

- Sells via channel
- Bootstrapped
- White glove service

Metro

Clients mostly are in and around the same metropolitan area the MSSP operates from

- Sells directly
- Bootstrapped
- White glove service

Regional

Clients mostly fall within two to four regions of the US

- Sells direct and via channel
- Transitioning from white glove to commoditized

National

Strong presence across all 50 states and possibly some international as well

- Sells direct
- Multiple private investors
- Commoditized with VIP option

Global

Strong presence across three or more continents

- Sells direct; may whitelabel 3rd party
- Product vendors
- Commoditized or white glove options

Services

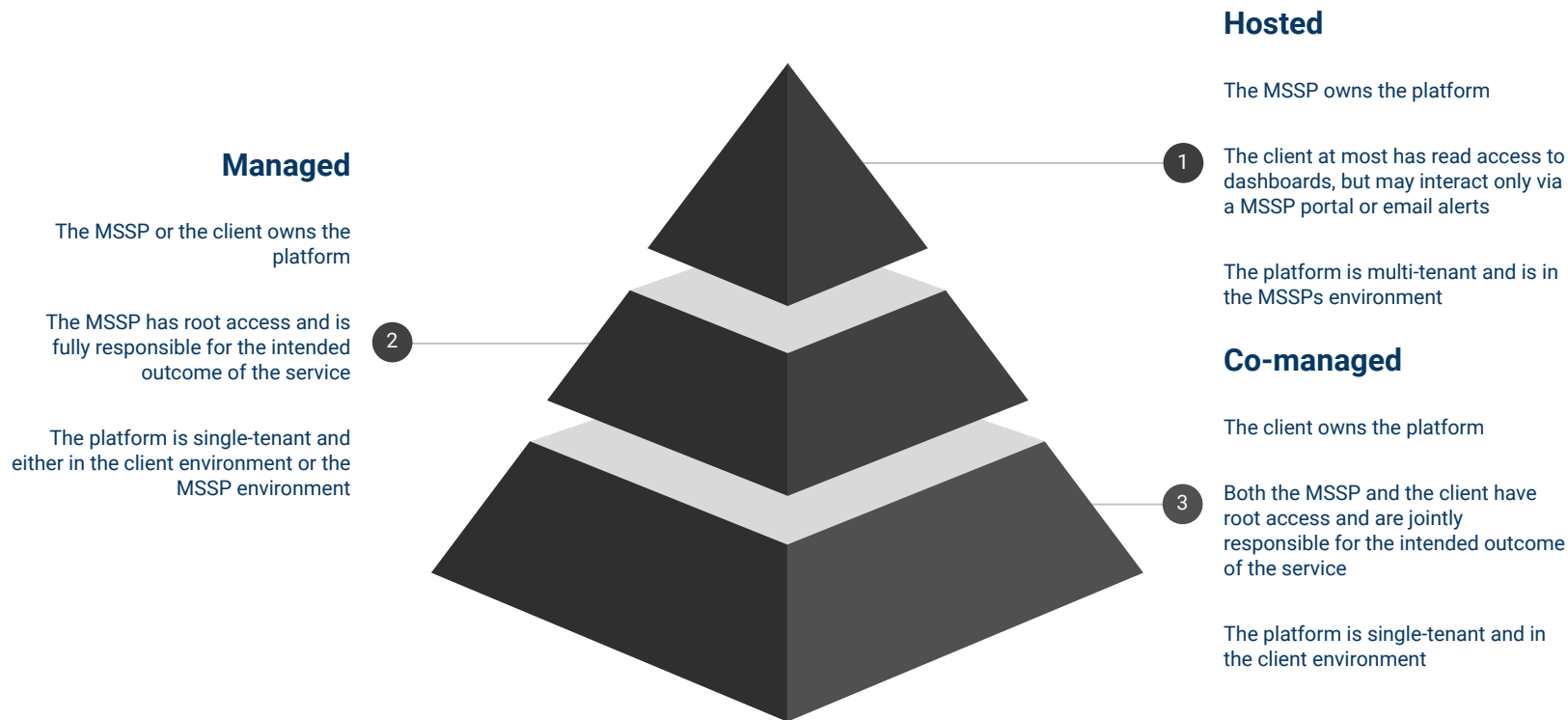


Platforms

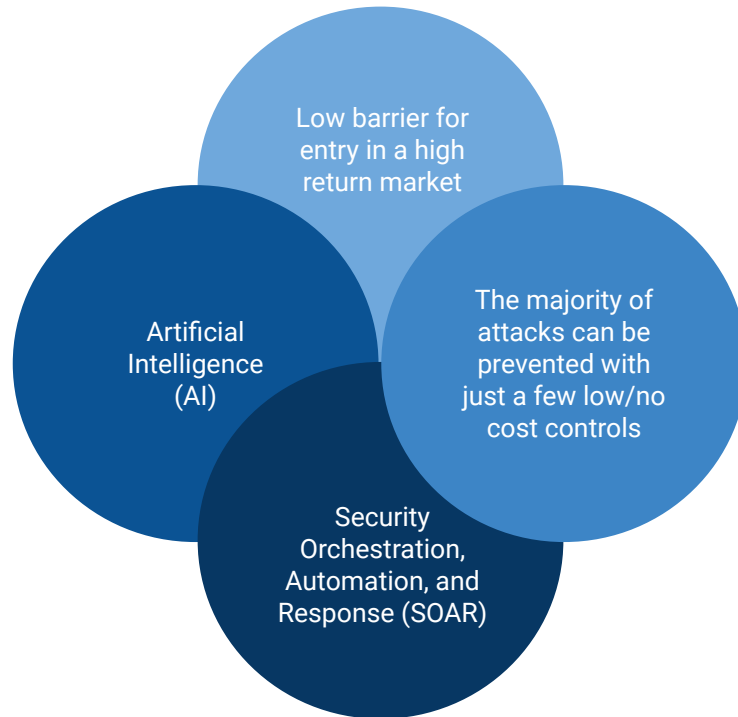
EPP	Endpoint Protection	<ul style="list-style-type: none">• Carbon Black• CrowdStrike	<ul style="list-style-type: none">• Cylance• Microsoft
SIEM	Security Information and Event Management	<ul style="list-style-type: none">• Microsoft• IBM• Splunk	<ul style="list-style-type: none">• Microfocus• AT&T• Elastic
NGFW	Next Generation Firewall	<ul style="list-style-type: none">• CheckPoint• Palo Alto	
VM	Vulnerability Management	<ul style="list-style-type: none">• Tenable• Rapid7• Qualys	

...and many other vendors

Service Models



Market Disruptors



How can Threat Angler help you?

