Gartner Security & Risk Management Summit
Summit 2018
04 – 07 June 2018 / National Harbor, MD

How to Become an MDR Provider

Sid Deshpande

MDR: Old MSSP in a New Bottle?

The problem with traditional MSS

MSSPs triage alerts (sometimes poorly) and the customer is expected to 'fix' the problem.

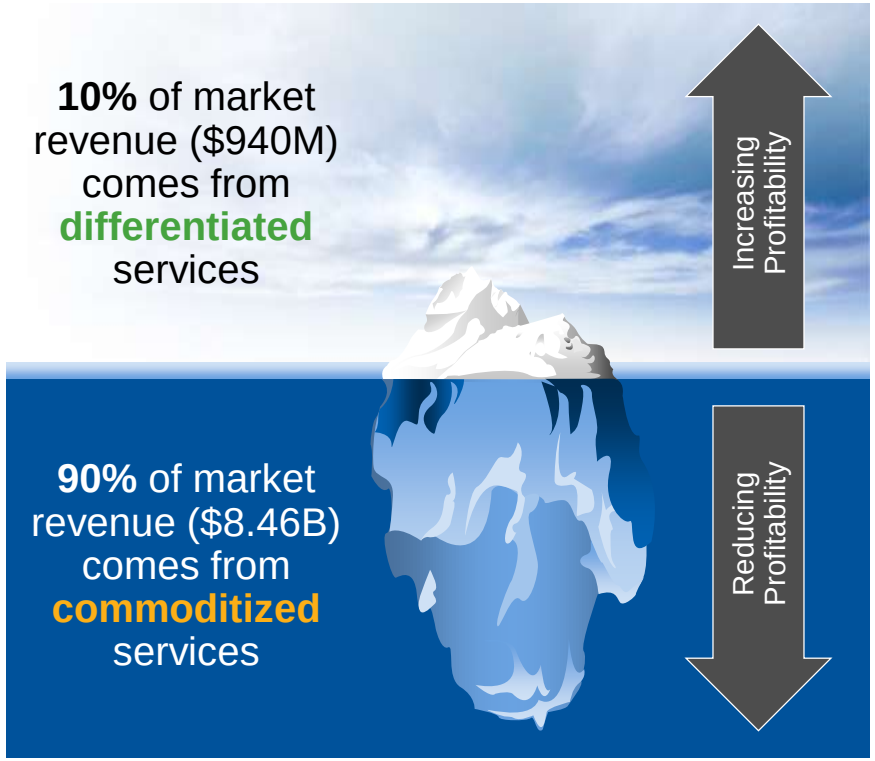
Degree of tuning and configuration required.

MSSP monitoring is based on preventative technologies like UTM and Firewalls.

Gartner

MSS Market Revenue in 2016: $9.4 Billion

MSS Market Revenue in 2016: $9.4 Billion



Emerging Services:
- **Managed detection and response**
- IaaS monitoring
- SaaS monitoring through CASB
- Managed network traffic analysis
- Threat intelligence platforms

Traditional Services:
- UTM/Firewall monitoring/management
- IPS monitoring management
- Managed secure web and email gateways
- Managed vulnerability scanning
- DDoS mitigation via remotely managed service

MDR was just a $100M market in 2017

MSSP is not going away!

Gartner

What MSSPs Need to Know About Offering MDR Services

Gartner

Technology Dependence

- Managed EDR (only) is a limited MDR service
- Broader support across different layers of the stack adds value
- Security technology vendors need MDR as much as the other way around

An MDR provider that positions itself as a specialist in data science has much more long-term viability than one that just offers a managed EDR or NTA service.

Gartner

The Importance of "Response"

- **Customers want:** Programmatic response, delivered remotely
- On-site incident response! = MDR
- Containment is a key part of response strategy
- Customers have different attitudes toward 'response' — flexibility is key

It is essential for the customer and the MDR provider to have a strong understanding of the IT asset management and identity context of the environment to deliver effective response

Architectural Considerations

- Primary Detection and Response Technology
- Secondary Detection Technology
- Log Collection, Filtering and Normalization
- Long-Term Data Store
- Batch Processing Component
- Streaming Analytics Component
- Portal, Workflow and Visualization

Workforce Management and Skill Sets

Typical 'Alternative' Skill Sets Required to Offer an MDR Service

- Incident Response and Remediation
- Threat Intelligence and Threat Research
- Penetration Testing
- Data Science

It's not only about the skills you have on your staff, it's about whether those skills are being made available to the customer!

Great so now you have an MDR service — but how do you talk to customers about it?

Gartner

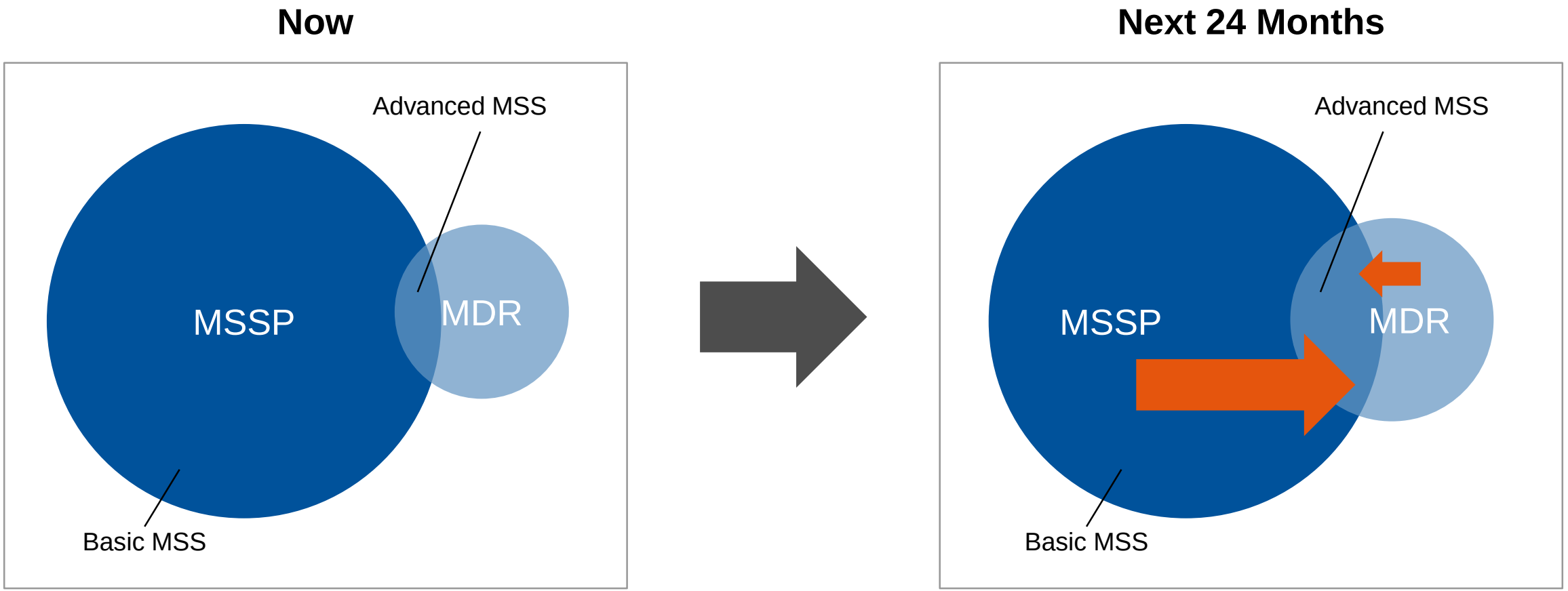
Articulating MDR Value to Customers

Security Operations Maturity Level	Description of Customer Security Operations Maturity	MDR Value
1 (Lowest)	Fully decentralized, no SIEM, no MSSP, no analytics	MDR allows quick introduction of detection and response capabilities where none exists.
2	Heavily reliant on an MSSP, no SIEM, no analytics or other on-premises security operations	MDR does what an MSSP cannot do (detect threats that bypass traditional controls managed by MSSPs), and thus is complementary. The MDR provider brings in new sensors to aid better detection.
3	Using an MSSP and also small part-time in-house centralized security operations	MDR brings specialized skill sets and technologies that in-house team cannot hire/retain/afford.
4 (Highest)	Significant investment in on-premises dedicated SOC	MDR improves business metrics around security operations (time to detect and time to respond).

How is the MDR market going to evolve in relation to MSSP?

Gartner

MDR Service Providers in Relation to MSSPs



Recommendations

- ✓ Focus on cultural aspects of offering MDR — doesn't happen overnight!
- ✓ MDR is one part of a broader security operations approach.
- ✓ Focus on customer experience as a strategic service delivery area.
- ✓ Pursue a strategy that leads to the least amount of disruption for customers' security architecture.
- ✓ Remote response delivered programmatically.
- ✓ Flexibility in service delivery — customers have varying degrees of security operations maturity.

Recommended Gartner Research

- **Market Insight: What MSSPs Need to Know About Offering MDR Services**
  Sid Deshpande, Craig Lawson and Others (G00342443)
- **Market Guide for Managed Detection and Response Services**
  Toby Bussa, Craig Lawson and Others (G00308991)
- **Magic Quadrant for Managed Security Services, Worldwide**
  Toby Bussa, Kelly M. Kavanagh and Others (G00325535)

For information, please contact your Gartner representative.

Gartner