Navigating the Noise

How to evaluate and select a MDR provider

Agenda

- Today’s Challenges
- Managed Detection and Response
- Choosing the Right MDR Provider
- How Analysts Define MDR
- Q&A/Discussion

Secureworks

Today's Challenges

Organizations Know Security is a Priority

But going it alone is not easy

Lack of Visibility

More attack surfaces. Hackers evade controls.

Too Much Complexity

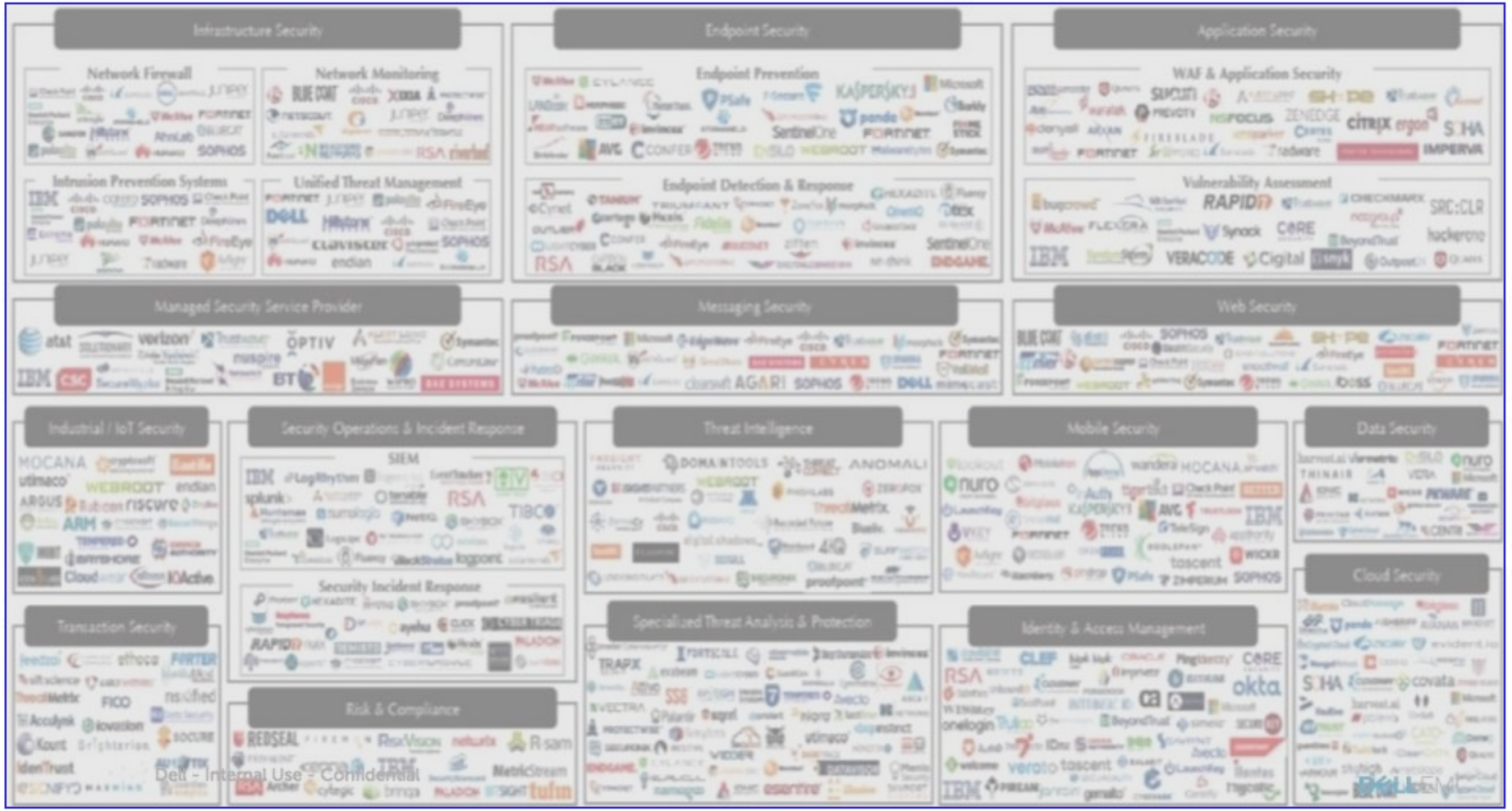
Thousands of signals. Which one matters?

Competing Priorities

Not enough context to know which action to take.

There are Numerous Security Vendors

But how do you pick the right solution?



- Among larger clients, commonly see more than **50 different** security layers
- Disparate technology does not provide holistic solution
- What's needed? An easy-to-consume, simple solution

Secureworks

What is Managed Detection and Response (MDR)?

Improve detection & response times across network, endpoints and cloud

MDR is an end-to-end, outcome based solution designed to reduce your burden around

- Advanced threat detection
- 24x7 monitoring and alerting
- Emergency incident response

- Shifts the focus from compliance to detecting advanced threats and targeted attacks
- Helps identify new and existing Indicators of Compromise
- Delivers ongoing access to experts in research, investigation and incident response
- Leverages data from a wide range of security technologies and vendors
- Applies automated and human-driven advanced analytics to security tool output

Choosing the Right MDR Provider

Secureworks

Suggested Criteria for Making the Right MDR Selection

Call it what you want, but it's not MDR without satisfying these five points

- Endpoint Detection and Response
- Incident Response Capabilities
- Intellectual Property
- Beyond Endpoints
- Global Threat Visibility and Threat Intelligence

Endpoint Detection and Response

Not all EDR solutions are created equal

What to Know

- Many organizations cannot identify malicious activity
- Not all EDR products collect data analysis threat hunters need
- Some MDR solutions have difficulty transforming observed activity into actionable recommendations

What to Avoid

- Reliance on third-party EDR technology
- Technology that cannot absorb threat intel
- Solutions claiming to provide MDR with an endpoint plug-and-play approach

What Good Looks Like

- Detection of advanced threats at endpoint
- Application of threat intel and behavioral analytics

Incident Response Capabilities

Don’t be fooled … if there is no Incident Response, it’s not MDR

What to Know

- Ability to act upon discovery varies greatly across providers
- Detection is only part of the story. What do you do then?
- IR skillsets are in high demand, yet there is shortage of qualified personnel

What to Avoid

- Providers who lack depth and experience in response action
- MDR solutions claiming incident response, only to rely on inexperienced personnel
- Organizations lacking experience in malware analysis, digital forensics and complex incidents

What Good Looks Like

- Provable credentials (years of experience, engagements performed annually, credentials)
- The ability not only to contain a threat, but eradicate and prevent re-entry
- IR group that understands legal and compliance impacts

Intellectual Property

Whoever owns the components of your MDR solution holds the key to the kingdom

What to Know

- MDR components must work together seamlessly
- Mixing and matching technology from different providers does not always work

What to Avoid

- Siloed technologies developed by different vendors
- Organizations are at mercy of vendors to implement new methods to improve components
- Relying on a siloed approach leads to roadblocks and diminishes efficiency

What Good Looks Like

- Ensure telemetry and correlation are in place
- Provide intellectual property at every stage of the MDR process
- IP needs to be present throughout the network and endpoint layers, plus cloud, with ability to weave in threat intel and advanced analytics

Beyond Endpoints

Helping extend basic MDR to a higher, more-complete level

What to Know

- Some organizations focus on only EDR, lacking the ability to look at the network, the cloud, log data, etc.
- The more sources (network, cloud, IR), the better and more complete the solution

What to Avoid

- Endpoint visibility only is NOT a holistic MDR solution
- Be wary of providers who cannot provide visibility and action from log and network forensics

What Good Looks Like

- A fully powered solution absorbs information from variety of sources
- Ability to gain telemetry throughout the network
- The skill and experience to analyze data and turn into action

Global Threat Visibility and Threat Intelligence

The threat landscape is not static; updated intelligence drives more effective MDR

What to Know

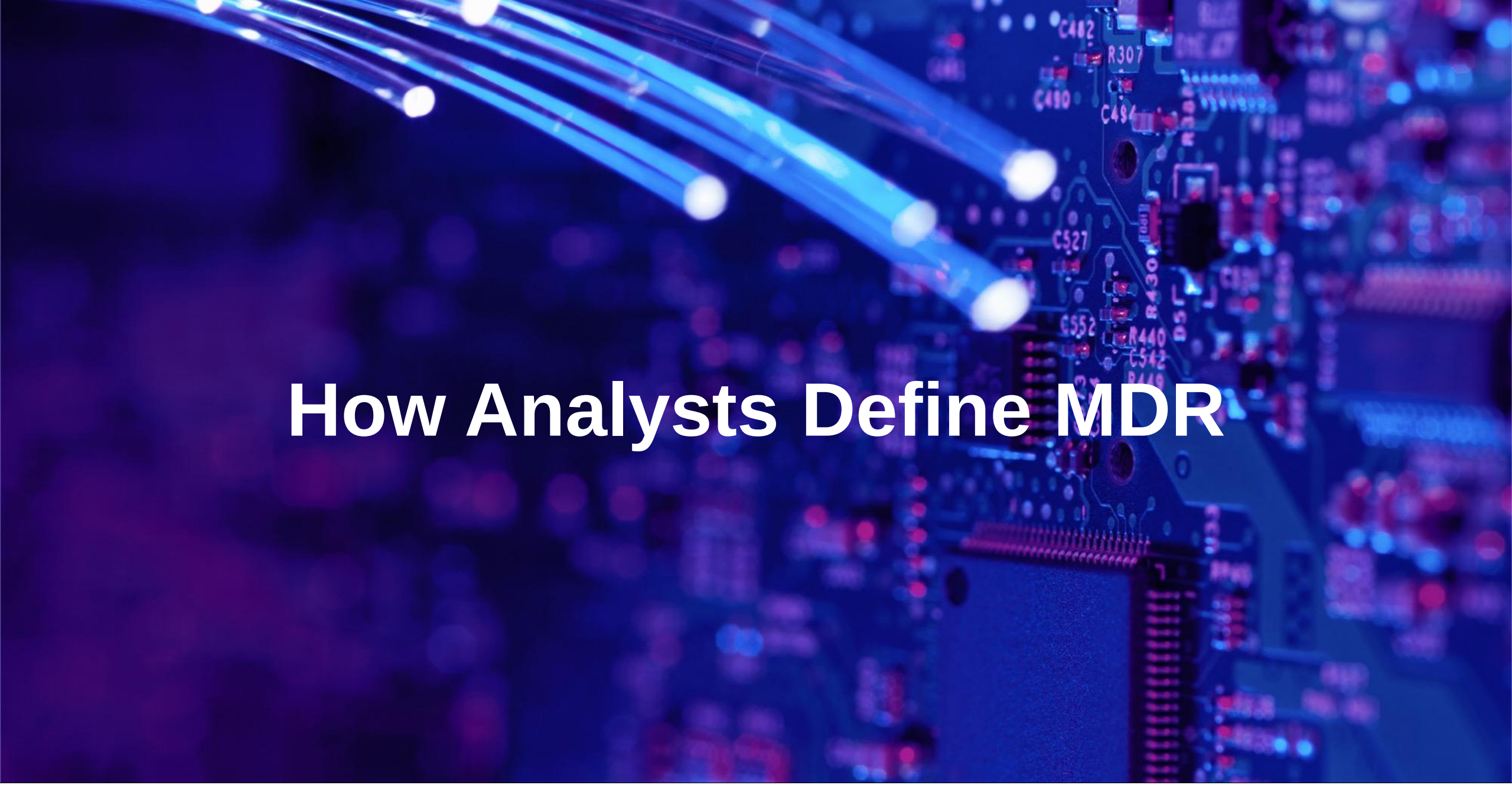
- Many MDR vendors do not possess impactful global threat visibility
- One major challenge is finding vendors who weave current threat intel into MDR

What to Avoid

- Those organizations who rely on old, outdated threat data
- MDR providers who cannot widen your view of the threat landscape

What Good Looks Like

- Providers who not only react to findings or research, but deliver it as part of day-to-day MDR
- Demonstration of ability the scope and depth of threat intel
- Threat intel and research expertise that accelerate MDR to stay head of evolving threats

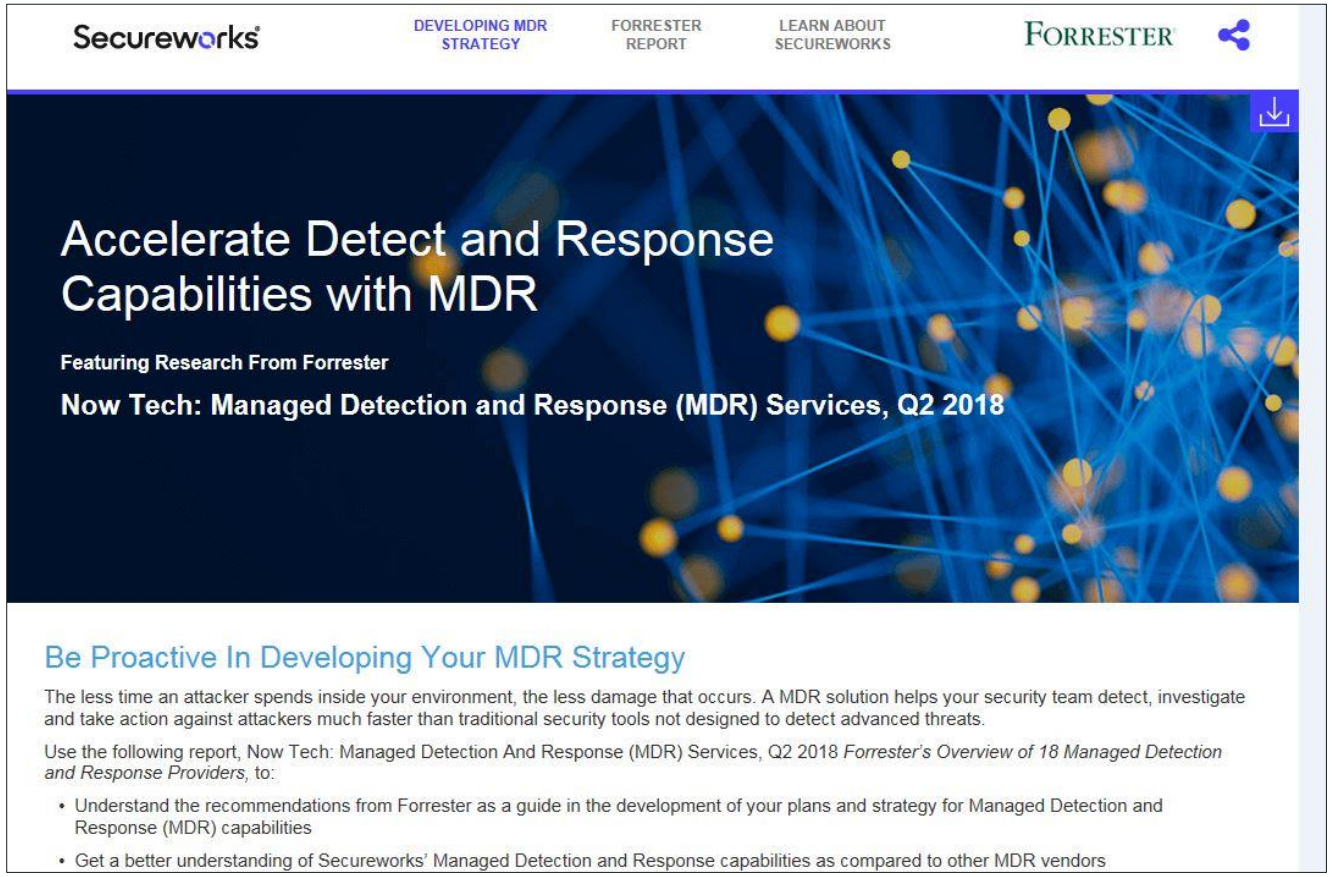


How Analysts Define MDR

Secureworks

Forrester Viewpoint: Endpoint, Incident Response, IP

Secureworks cited as full-scale forensics provider in latest Forrester report



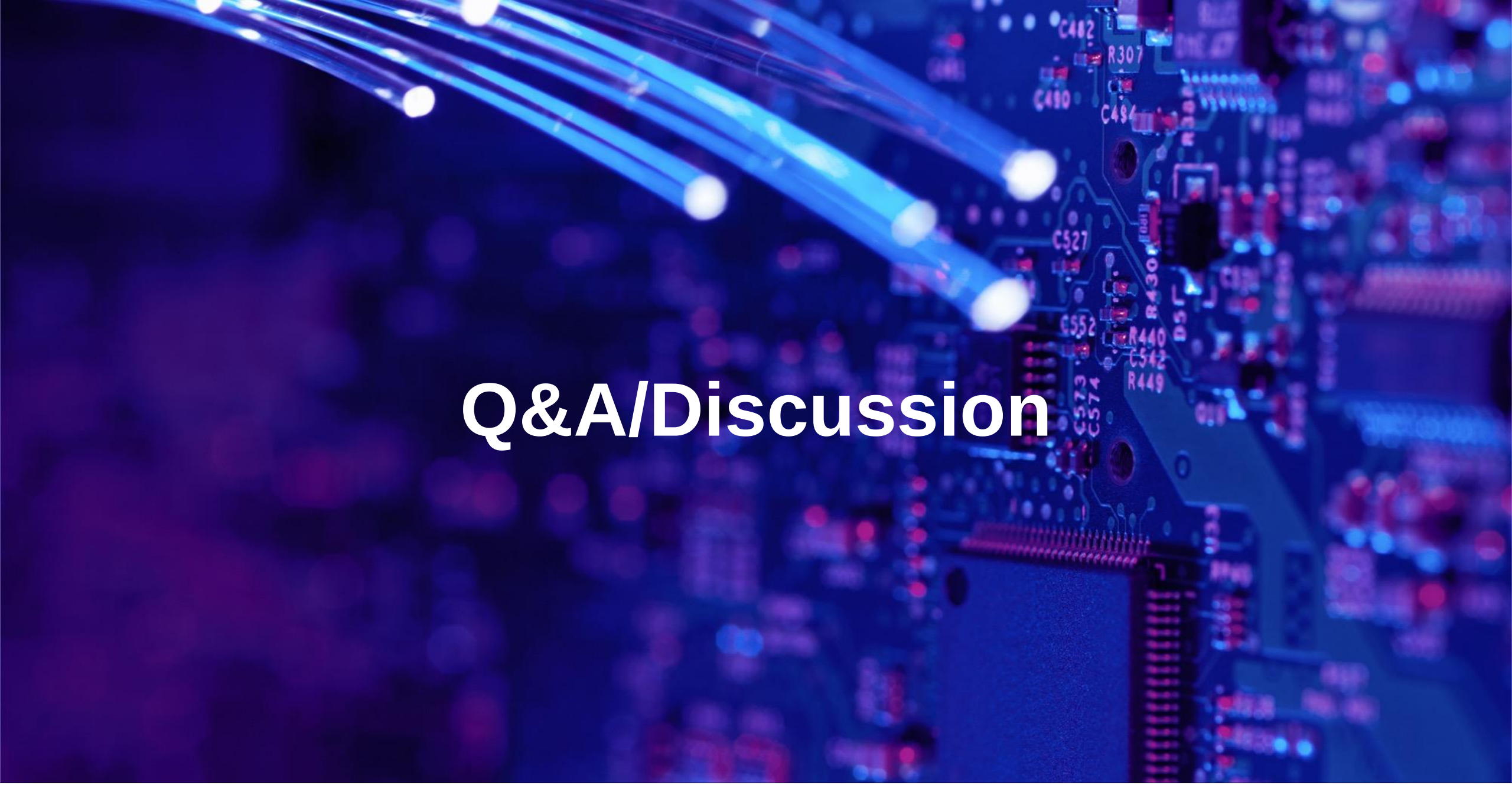
Finding the right provider:

- Evaluate EDR capabilities (Red Cloak)
- Choose IR pedigree (Decade-plus experience, 900-plus engagements annually)
- Prioritize those who own MDR intellectual property (Red Cloak, iSensor, CTU, CTP, threat intelligence)

Use the report to:

- Understand Forrester's recommendations as a guide for clients to develop MDR strategy
- Acquire better understanding of Secureworks MDR capabilities as compared to other MDR vendors

https://www.secureworks.com/resources/rp-mdr-solution-cited-by-forrester-2018


Q&A/Discussion