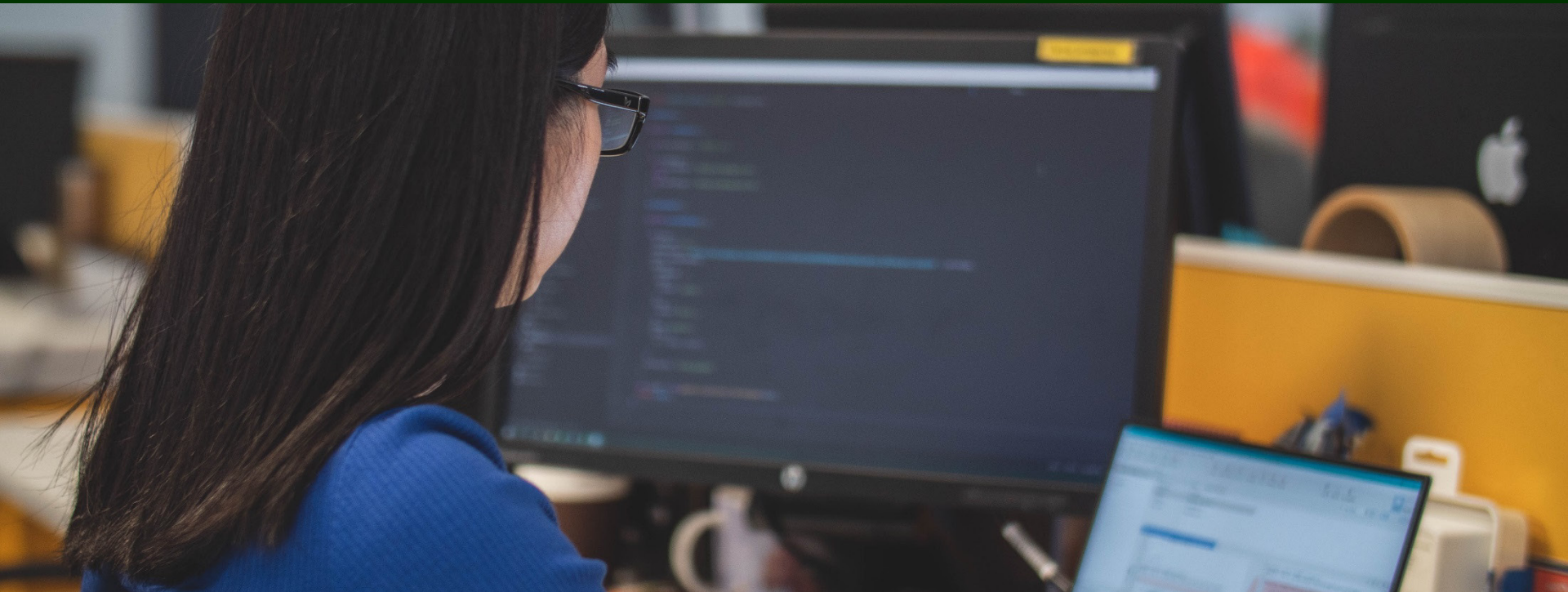


Forrester Opportunity Snapshot: A Custom Study Commissioned By McAfee | May 2019

Empower Security Analysts Through Guided EDR Investigation

Bridging The Gap Between Detection And Response

GET STARTED ►



Forrester Opportunity Snapshot: A Custom Study Commissioned By McAfee | May 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

EDR Must Evolve To Reduce Analyst Fatigue

Efficient and effective threat detection requires rapidly obtaining insights from collected data. Today, many EDR solutions are focused on providing investigation capabilities to the most sophisticated SOC analysts, a focus that hasn't proven effective or scalable. EDR products that enable triage by junior analysts through guided investigation open this superior level of detection to many markets that were previously unable to benefit from this technology.

In April 2019, McAfee commissioned Forrester Consulting to explore opportunities for guided investigation capabilities in enterprise endpoint detection and response (EDR) products. We found that security decision makers believe guided investigation will improve alert quality, drive efficiency in the security operations center (SOC), and ultimately help enterprises secure their endpoints at scale.



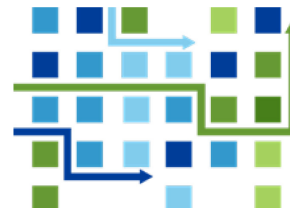
Country/region

- › US/Canada: **40%**
- › United Kingdom: **20%**
- › Germany: **20%**
- › France: **20%**



Position – 100% sec. IT roles:

- › C-level: **38%**
- › VP: **10%**
- › Director: **33%**
- › Manager: **19%**



Key industries

- › Tech/tech services: **19%**
- › Financial services: **18%**
- › Manufacturing: **12%**
- › Healthcare: **10%**



Company size - employees

- › 1,000 to 4,999: **46%**
- › 5,000 to 19,999: **28%**
- › 20,000 to 50,000+: **25%**

Note: Percentages may not total 100 because of rounding.

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2

Enterprises Seek Ways To Improve Detection While Increasing Efficiency

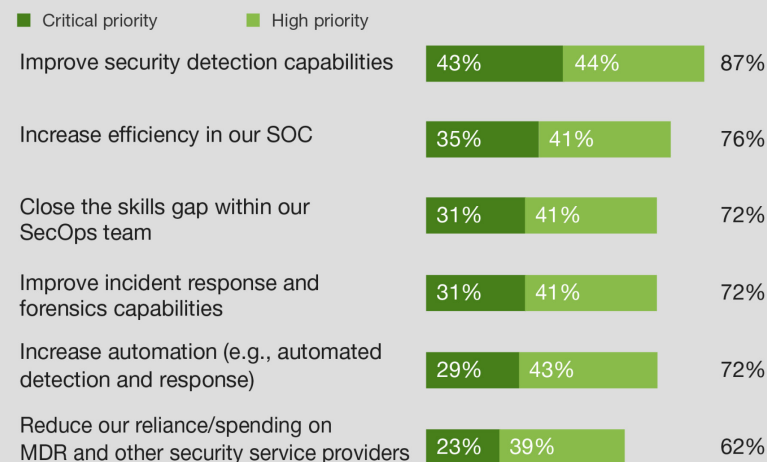
When considering their top security priorities, decision makers see threat detection as paramount: 87% of respondents consider this a high or critical priority.

As the volume and variety of threats continue to accelerate, security teams are also struggling with bandwidth constraints and skills gaps. Security decision makers are looking for ways to increase efficiency in the SOC and close skills gaps within their teams. Increased automation, including automated detection and response, is a goal that 72% of organizations are pursuing to ease the burden on security operations (SecOps) teams.

Security teams see detection as their No. 1 priority and seek to drive efficiency and close skills gaps to improve detection at scale.



“To what extent is your IT organization prioritizing the following endpoint security goals and initiatives for the coming year?”



Base: 258 security technology decision makers at enterprises that have implemented EDR solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, March 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

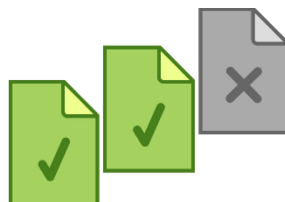
1 2

Current EDR Solutions Fall Short Of Business Expectations

Security teams rely on their EDR tools to provide many critical capabilities like automated detection, endpoint visibility, and threat hunting. However, current solutions fall short of meeting these needs. For example, 43% of security decision makers consider automated detection a critical requirement, but only 30% feel their current solution(s) completely meet(s) their needs in this area.

Many enterprises have enlisted managed detection and response (MDR) providers to close the gaps that their EDR solutions cannot fill, such as threat hunting and endpoint forensics. This requires decision makers to allocate security budget to support capabilities their EDR software should already provide.

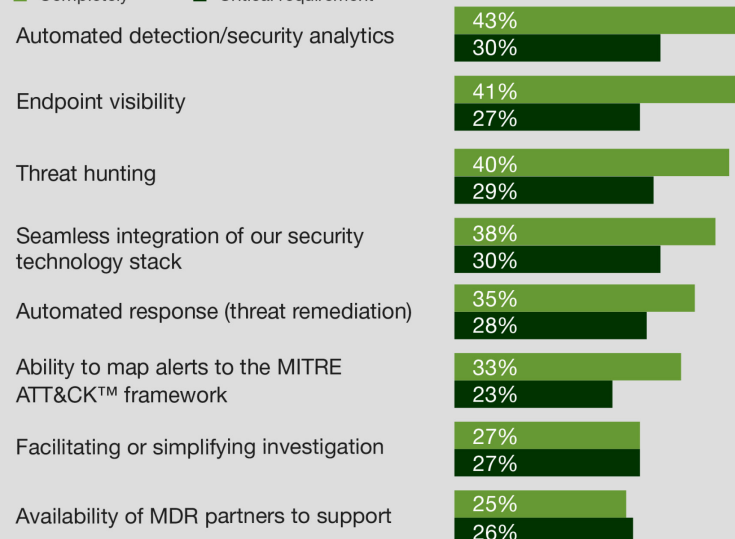
Many enterprises are spending money with MDR providers to support capabilities that their current EDR solutions fail to sufficiently deliver.



The biggest gaps in EDR capabilities are in automated detection, endpoint visibility, and threat hunting

"How important do you consider the following capabilities in selecting an EDR product?"
"To what extent do you feel your current EDR solution(s) meet(s) your organization's needs in the following areas?"

■ Completely ■ Critical requirement



Base: 258 security technology decision makers at enterprises that have implemented EDR solutions
 Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, March 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

EDR Alerts Are Noisy And Complex

Gaps in EDR capabilities have created pain points for 83% of enterprises. Security teams are struggling to achieve their endpoint security goals at scale because:

- **They worry about false negatives.** More than a third of decision makers (36%) worry that their EDR doesn't surface every threat that breaks through their barriers.
- **And yet, they are plagued by false positives.** On the flip side, the same proportion of decision makers feel that the alerts they *do* receive are frequently not worth investigating.
- **Alert triage requires advanced skill sets.** Security teams are already strapped for bandwidth and looking for opportunities to drive efficiency at every turn. EDR solutions have become a thorn in their side because the alerts are complex and difficult for junior analysts to triage without supervision.

It takes security staff an average of 2 hours and 10 minutes to close an EDR alert case.



"Which of the following pain points has your organization experienced with its current EDR product?"

We worry that our EDR product is not surfacing alerts for all threats that may exist.	36%
The alerts surfaced by our EDR product are frequently not relevant or not worth investigating.	36%
Many of our junior staff members lack the skill sets to triage and/or investigate alerts without the support/supervision of senior staff.	35%
We struggle to keep up with the volume of alerts generated by our EDR product.	31%
Alerts do not contain enough context/details, making them difficult to triage and investigate.	29%
N/A; we haven't experienced any pain points.	17%

Base: 258 security technology decision makers at enterprises that have implemented EDR solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, March 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

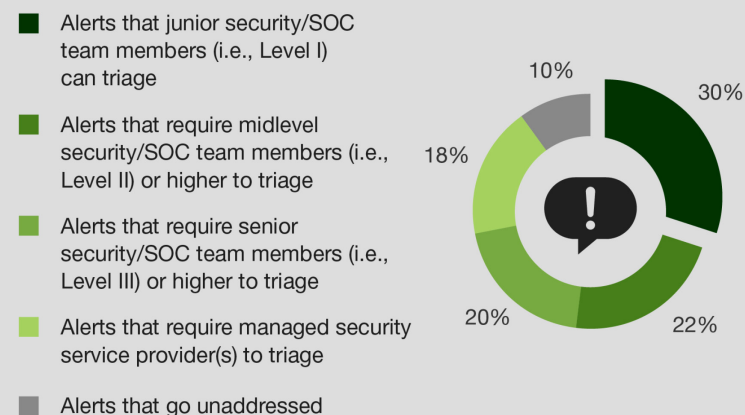
EDR Alerts Are Complex, Requiring Senior Analysts To Triage

Many EDR products rely on the security analyst to understand the collected telemetry while being provided limited context around generated alerts. This creates a situation where junior analysts can triage an average of just 30% of the alerts generated from EDR solutions. Sixty percent of alerts are complex enough to require the attention of more senior security analysts (e.g., Level II or Level III) or a service provider. And even with the time these skilled resources are dedicating to alert triage, an alarming 10% of EDR alerts still go unaddressed. This is a security incident waiting to happen.

Junior analysts can triage just 30% of alerts today. The remaining alerts require the skills of more senior analysts, or else they go unaddressed.



“Using your best estimate, what percent of alerts from your EDR solution can be triaged by junior analysts, compared to those that would require higher level or external resources?”



Base: 231 security technology decision makers at enterprises that have implemented EDR solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, March 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

1 2 3

Alert Triage Takes Too Much Time

When it comes to EDR alerts, security teams are likely to think in hours rather than in minutes. Just over half of enterprises (52%) report that it takes at least an hour to complete an investigation for a given alert and close the case. Five percent have found that the average case takes more than a full day to investigate. Overall, the average case takes 2 hours and 10 minutes to close.

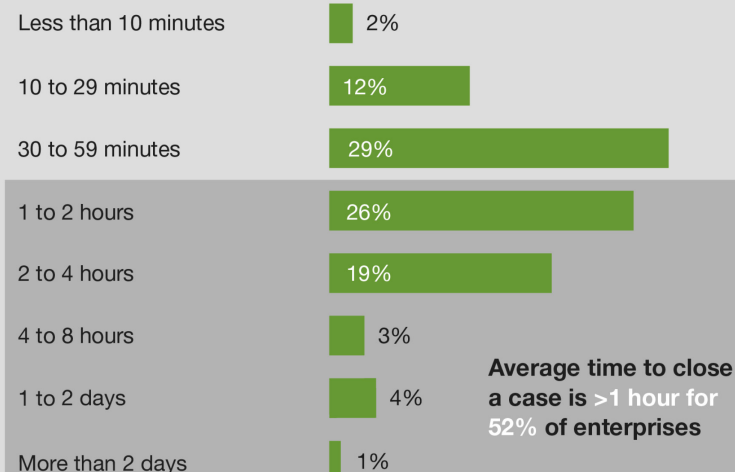
With 60% of alerts requiring the intervention of senior security analysts and/or managed service providers, and the fact that EDR solutions frequently produce false positives for 36% of companies, this is valuable time wasted.

Unfortunately, many EDR solutions have been designed for power users who are looking to manipulate and interpret complex data sets as part of an investigation. Enterprises need a better option to improve detection and secure their endpoints at scale.

It takes security staff an average of 2 hours and 10 minutes to close an EDR alert case.



“Approximately how much time, on average, does it take your security/security operations team to complete an investigation for a given alert and close the case?”



Base: 258 security technology decision makers at enterprises that have implemented EDR solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, March 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

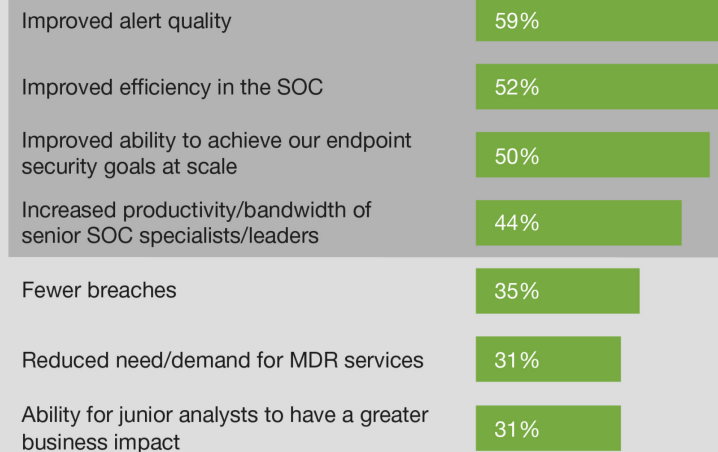
CONCLUSIONS

Guided Investigation Can Help

Enterprises are eager for solutions that drive efficiencies and close skills gaps in the SOC. EDR solutions that offer guided investigation, supporting alert triage and automated investigation, are a great example of such a solution. Security decision makers anticipate a wide range of benefits, including:

- **Improved efficiency and productivity.** Security decision makers recognize that guided investigation will help simplify alert triage and enable junior analysts to own more of the process. As a result, 44% believe that senior security analysts will be more productive and have more bandwidth. This will ultimately support the goal of improving efficiency in the SOC — a benefit that 52% anticipate.
- **Higher quality alerts.** Fifty-nine percent of respondents believe guided investigation capabilities will cut through the noise from their current EDR solutions and improve alert quality. A benefit of the improved SOC efficiency is that senior security analysts will be able to focus bandwidth on the most important alerts.
- **Increased endpoint security, at scale.** Increased efficiency and improved alert quality will ultimately help enterprises achieve their endpoint security goals at scale. Half of decision makers anticipate this benefit from guided investigation.

“What, if any, benefits do you anticipate these capabilities would deliver to your business?”



Base: 258 security technology decision makers at enterprises that have implemented EDR solutions
Source: A commissioned study conducted by Forrester Consulting on behalf of McAfee, March 2019

EDR vendors are beginning to introduce guided investigation capabilities, which support alert triage and automated investigation as a part of their core offering.

Forrester Opportunity Snapshot: A Custom Study Commissioned By McAfee | May 2019

Empower Security Analysts Through Guided EDR Investigation

OVERVIEW

SITUATION

APPROACH

OPPORTUNITY

CONCLUSIONS

Conclusion

Today's EDR solutions have left security teams feeling overwhelmed, at risk, and unfulfilled. Security decision makers seek greater automation, threat hunting, and endpoint visibility than what their current solutions deliver. Moreover, EDR alerts are complex, noisy, and require a significant amount of time and effort from senior security analysts and service providers. To sufficiently secure the enterprise, security teams need EDR solutions that are easier to use and support greater automation.

Guided investigation is an emerging EDR capability with significant promise. Security decision makers believe its automated investigation and guided alert triage features will yield higher quality alerts, drive greater efficiency in the SOC, and enable them to achieve their endpoint security goals at scale.

METHODOLOGY

This Opportunity Snapshot was commissioned by McAfee. To create this snapshot, Forrester conducted an online survey of 258 security technology decision makers at enterprises with 1,000 or more employees which have implemented EDR solutions. Respondents were based in the US, Canada, the UK, Germany, and France.

The survey was completed in March 2019.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2019, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. E-42268

Project Director:

Karin Fenty, Market Impact
Principal Consultant

Contributing Research:

Forrester's Security and Risk
research group