Endpoint vs Network Visibility: Where to Invest Your Budget

Security teams frequently ask: If I can only invest in one kind of visibility solution, should it be network or endpoint security? Each of these platforms gives value to an organization in different capacities—and that capacity can vary depending on the organization itself.

	Endpoint Visibility	Network Visibility
What you can collect	• Process information • Network connections • Dns requests • File modifications • Registry changes • Binary files • Memory content and structures • User information	• Artifacts of communication to feed other investigative processes from logs, NetFlow, and full-packet data • Exfiltration reconstruction (damage assessments) • C2 protocol decoding
What you can detect	• Malware installation • Advanced attacker techniques • File creation/modification events • Registry edits • Misuse of legitimate applications • File-based attacks • Unwanted software • Insider threats • Suspicious user activity • Suspicious application behavior	• Known command and control • Payloads • Evidence of communication with systems that are confirmed or believed to be malicious • Anomalies from baseline activity that suggests short- or long-term investigation may be needed
Benefits	• Broader detection coverage across the attackers' kill chain; identifies advanced attacks and threatening behaviors • Faster, more resolute detection reduces attackers' dwell time • IR teams can quickly go back in time to an event or time period of interest to establish a high-resolution picture of what occurred and whether it was malicious	• Can provide immediate value and is often inexpensive to start • Fast to query and can quickly scope a compromise or identify additional sources of evidence during an investigation • Network security monitoring (NSM) platforms like Bro provide long-term network visibility that aids in IR actions (preferable to traditional IDS and other signature-based tools/platforms)

red canary

	Endpoint Visibility	Network Visibility
Challenges	Building a full operational capability requires additional investments in technology and expertise	• Encryption limits visibility • Legality of collection and retention • Lack of visibility into endpoint activity limits detection capabilities and ability to accurately determine specific events
Requirements	Either an in-house SOC and robust IR processes or a skilled MEDR partner to run endpoint analysis, threat triage, and investigation	Streamlined investigative workflow; legal coordination

WHAT IF YOU HAVE TO PICK ONE?

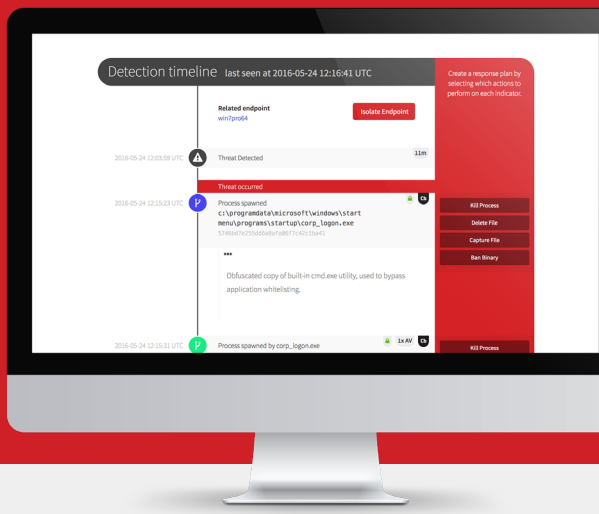
Network-based detection, while invaluable, generates questions that almost always lead to endpoints because the endpoint is the most conclusive place to look. Only 5% of organizations have a traditional network perimeter. No one is attacking the perimeter; they're trying to get through it to an organization's endpoints. Thus, detecting and responding to threats at the endpoint provides a more effective defense.

While cost-conscious security leaders may be tempted by offerings that cover both the network and endpoint, selecting broad "all-in-one" coverage often means sacrificing quality and expertise where it matters most: at the endpoint.

About Red Canary

Red Canary helps customers secure their endpoints and stop attacks before they result in breaches. The Managed Endpoint Detection and Response solution quickly and accurately identifies threats on customers' endpoints ranging from compromised credentials to lateral movement to crimeware. Every threat is investigated by a Red Canary Analyst to remove false positives and provide the context required for remediation.

Red Canary's customers extend all over the world and face the breadth of threats. With customer concentrations in banking, legal, technology, and manufacturing, Red Canary understands the challenges enterprises face securing their data and brand.



red canary

Secure Your Endpoints

www.redcanary.com