Joint solution brief

Corelight for Microsoft Defender

Accelerate investigations and prioritize alerts based on risk with integrated network, endpoint, and vulnerability data directly within the network sensor.

Security teams face challenges in maintaining a strong security posture because legacy tools often fall short in supporting today's modern infrastructures and countering increasingly sophisticated threats. This is further compounded by the limited visibility into unsecured and unknown endpoints—resulting in more data but a lack of insights.

SOLUTION HIGHLIGHTS

Extensive visibility into network traffic across all devices

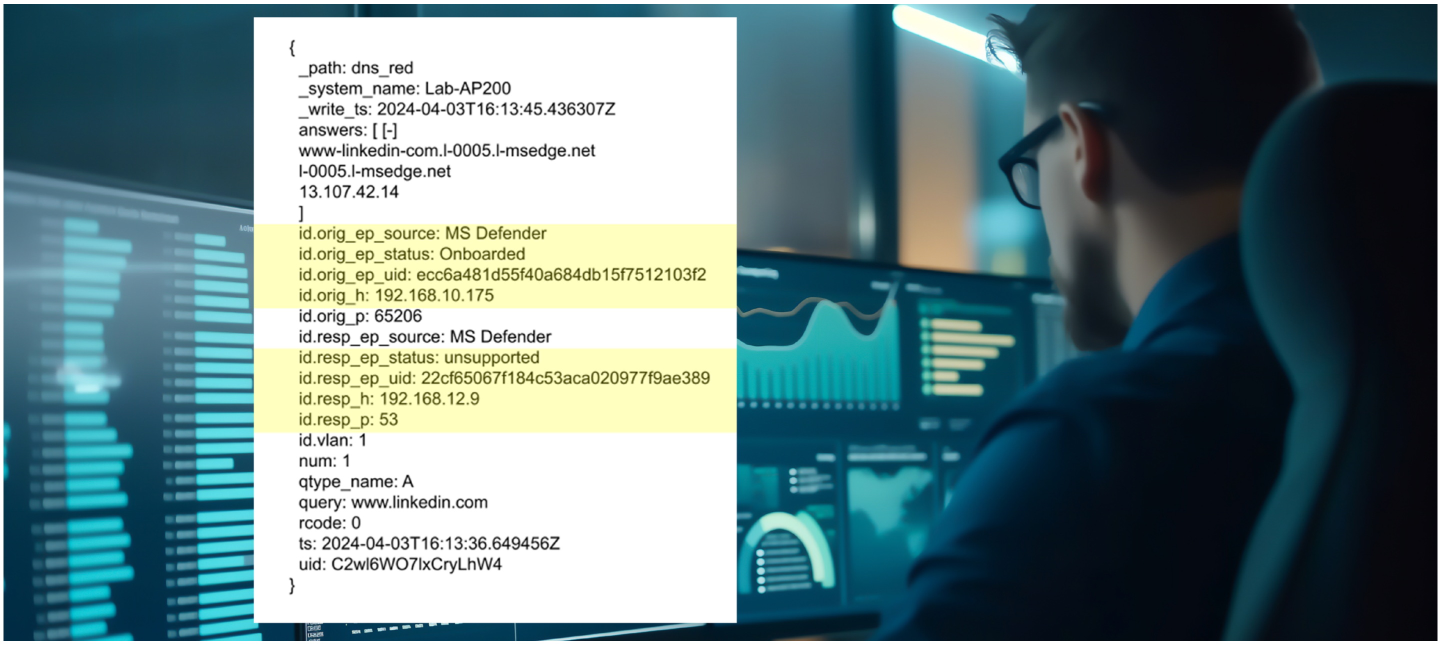
Faster investigations with risk-based alert prioritization

Higher analyst productivity with real-time contextualized alerts

1-click endpoint isolation directly through Corelight Investigator

Improved mean time to detection and remediation

Integrated Corelight and Microsoft Defender data in a single view.



```
{
  _path: dns_red
  _system_name: Lab-AP200
  _write_ts: 2024-04-03T16:13:45.436307Z
  answers: [ [-]
  www-linkedin-com.l-0005.l-msedge.net
  l-0005.l-msedge.net
  13.107.42.14
  ]
  id.orig_ep_source: MS Defender
  id.orig_ep_status: Onboarded
  id.orig_ep_uid: ecc6a481d55f40a684db15f7512103f2
  id.orig_h: 192.168.10.175
  id.orig_p: 65206
  id.resp_ep_source: MS Defender
  id.resp_ep_status: unsupported
  id.resp_ep_uid: 22cf65067f184c53aca020977f9ae389
  id.resp_h: 192.168.12.9
  id.resp_p: 53
  id.vlan: 1
  num: 1
  qtype_name: A
  query: www.linkedin.com
  rcode: 0
  ts: 2024-04-03T16:13:36.649456Z
  uid: C2wl6WO7lxCryLhW4
}
```

Accelerate investigations and prioritize alerts based on risk by enriching Corelight logs in real-time with Microsoft Defender endpoint and vulnerability data.

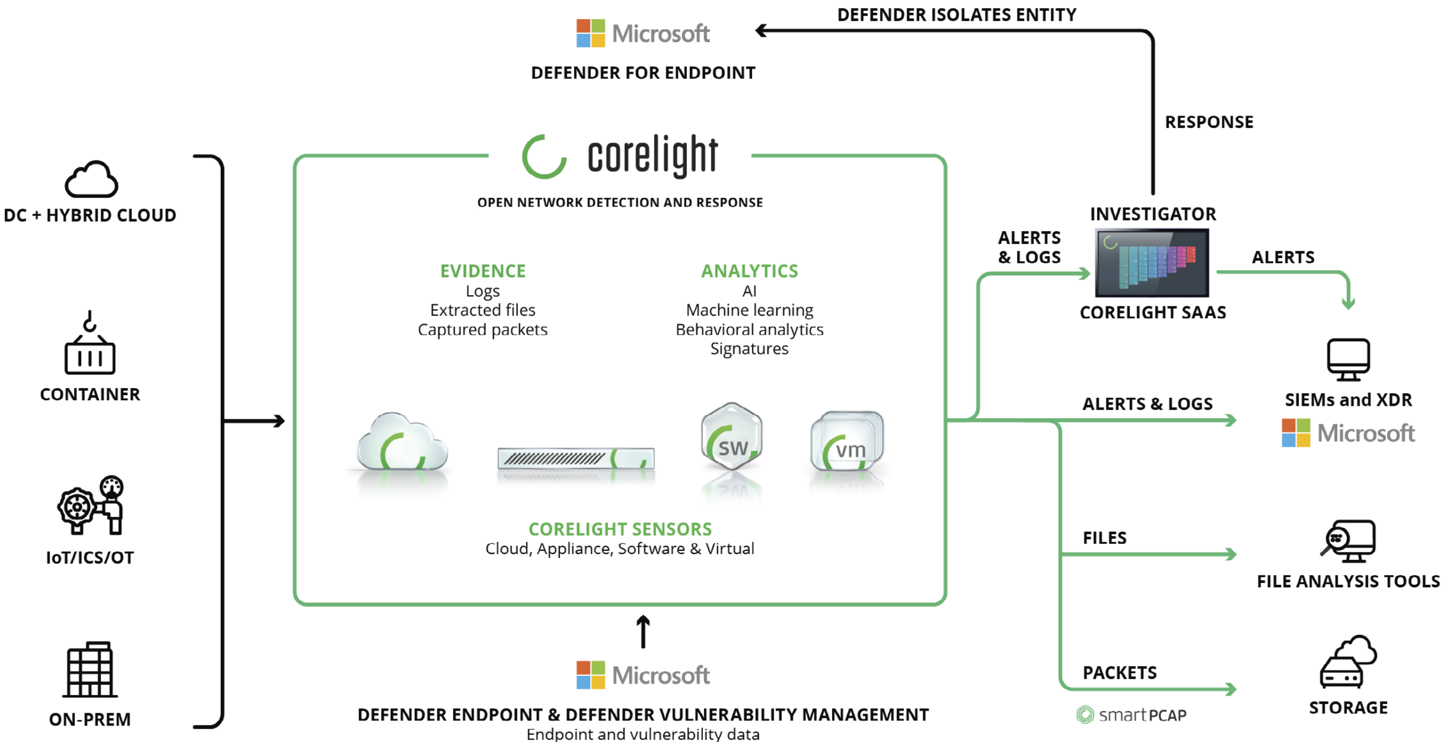
STREAMLINE INCIDENT RESPONSE WITH ENRICHED NETWORK EVIDENCE

Native Corelight integration with Microsoft Defender for Endpoint and Microsoft Defender Vulnerability Management can address these common problems. By enriching Corelight logs with timely and relevant Defender endpoint and vulnerability data at the point of observation directly in Corelight sensors, customers can streamline investigations, accelerate responses, and remediate incidents faster and easier than ever.

In addition to providing the correlated network and endpoint data that helps organizations better understand and prioritize the vulnerable endpoints across the enterprise, this unique integration enables fast and easy isolation of those endpoints that show signs of compromise. When Corelight detects a compromise, for example, analysts can use Corelight Investigator to quickly assess the threat and isolate devices with a single click. If further investigation shows that the endpoint is no longer a threat, analysts can just as easily release it from isolation directly within the Investigator interface.

In addition to helping Security Operations Center (SOC) analysts easily identify and isolate compromised endpoints, prioritizing alerts and detections with integrated network and endpoint telemetry can also greatly reduce the ongoing challenge of alert fatigue. Additionally, Corelight's extensive visibility of all network activity helps identify unmanaged and unknown systems across the environment that can then be inventoried and managed by Microsoft Defender.

Native integration streamlines and accelerates investigations



Simplify investigations and prioritize alerts according to actual risk to the enterprise with integrated network, endpoint, and vulnerability data.

SOLUTION BENEFITS

With full contextual and integrated endpoint, vulnerability, and network data now available directly from Corelight network sensors, analysts can simplify and accelerate their investigations for a more secure posture across the enterprise.

GET COMPLETE VISIBILITY

Detect early, mid, and late-stage indicators of network compromise with comprehensive visibility into all network traffic across the enterprise, including support for unmanaged and unknown devices, as well as those that can't accommodate endpoint agents.

IMPROVE NETWORK DETECTION AND COVERAGE

Enhance detections with prioritized alerts based on verified environmental risks by enriching Corelight network telemetry with Microsoft Defender endpoint and vulnerability data, all at the point of observation within the network sensor.

ACCELERATE RESPONSE

By enriching Corelight logs with unique device IDs from Microsoft Defender for Endpoint, SOC teams can pivot seamlessly between NDR and EDR telemetry to accelerate investigations and streamline incident response. One-click endpoint isolation through Corelight Investigator helps streamline workflows.

INCREASE OPERATIONAL EFFICIENCY

Corelight consolidates multiple legacy tools—including network monitoring, IDS, and intelligent packet capture—into a unified NDR platform that can reduce SOC complexity across on-premise, hybrid, and multi-cloud environments, while enabling higher analyst productivity.

corelight

To learn more about Corelight for Microsoft, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497