Secureworks® | corelight

SOLUTION BRIEF

# Secureworks® Taegis™ and Corelight Drive Better Security Outcomes

Secureworks and Corelight help you outpace and outmaneuver adversaries with precision so you can focus on your business. A unique combination of Secureworks AI-powered insights and continuously updated Threat Intelligence, leveraging superior network evidence from Corelight, help SecOps teams experience improved visibility and rapid remediation.

## The Challenges

Organizations are experiencing an increase in both threat volumes and complexity, leaving corporate security teams with the ongoing challenge of balancing workloads across a broader attack surface. IT and security teams struggle to identify all their endpoints and are often unable to install Endpoint Detection and Response (EDR) software on every known endpoint device, leaving security gaps that increase business risk. Network visibility is crucial for multi-layer defense. Superior network evidence provides critical data to fill endpoint visibility gaps and to identify threats hiding in DNS and encrypted traffic.

In addition to visibility and endpoint protection gaps, security teams are burdened with manual processes, disparate or disconnected security tools and a lack of trained IT security staff. IT and security leaders are tasked with implementing security programs that reduce risk and show value, but often lack the technology and resources to do so. Prioritizing security objectives and improving threat detection and response capabilities to reduce risk is imperative.

### Security Challenges

- Limited visibility across endpoint, network, and cloud.
- Threat actors hide in DNS and encrypted traffic.
- Asset management challenges and gaps in EDR coverage result in security blind spots.
- Security teams pivot across too many consoles to find emerging threats.

## Simplify Security with Secureworks

Secureworks offers a wide range of security solutions informed by 20+ years of hands-on experience. We help you reduce business risk and identify more threats by applying automated analytics and correlating telemetry across your  security solutions. Our single console view helps your security team be more effective and efficient for better security outcomes and simpler security operations.

Secureworks Taegis XDR is a cloud-native SaaS solution that combines the power of human intellect with insights from security analytics to unify detection and response across endpoint, network, and cloud environments. XDR is an extended detection and response solution that consolidates best-of-breed security components into a holistic approach of proactive protection against complex cyber threats.

Our XDR Detectors are integrated with operationalized threat intelligence and automation capabilities to improve visibility, reduce alert fatigue, and accelerate investigation and response. The XDR "Ask an Expert" live chat feature provides access to Secureworks analysts so your analysts can ask questions during an investigation and enhance their security skills. Secureworks Taegis ManagedXDR is available for organizations without the ability to manage XDR themselves.

## Better Together - Secureworks and Corelight

Securing today's complex environments requires collecting and correlating evidence across endpoint, network and cloud. By combining the automated security analytics and threat detection capabilities of Taegis XDR with session-level network telemetry from Corelight, we deliver better security across your environment. Corelight Network Detection and Response (NDR) collects broad network evidence versus just sending an alert with limited context or packet-level data. Netflow, firewall and DNS data are important, but insufficient for full investigations to identify threats.

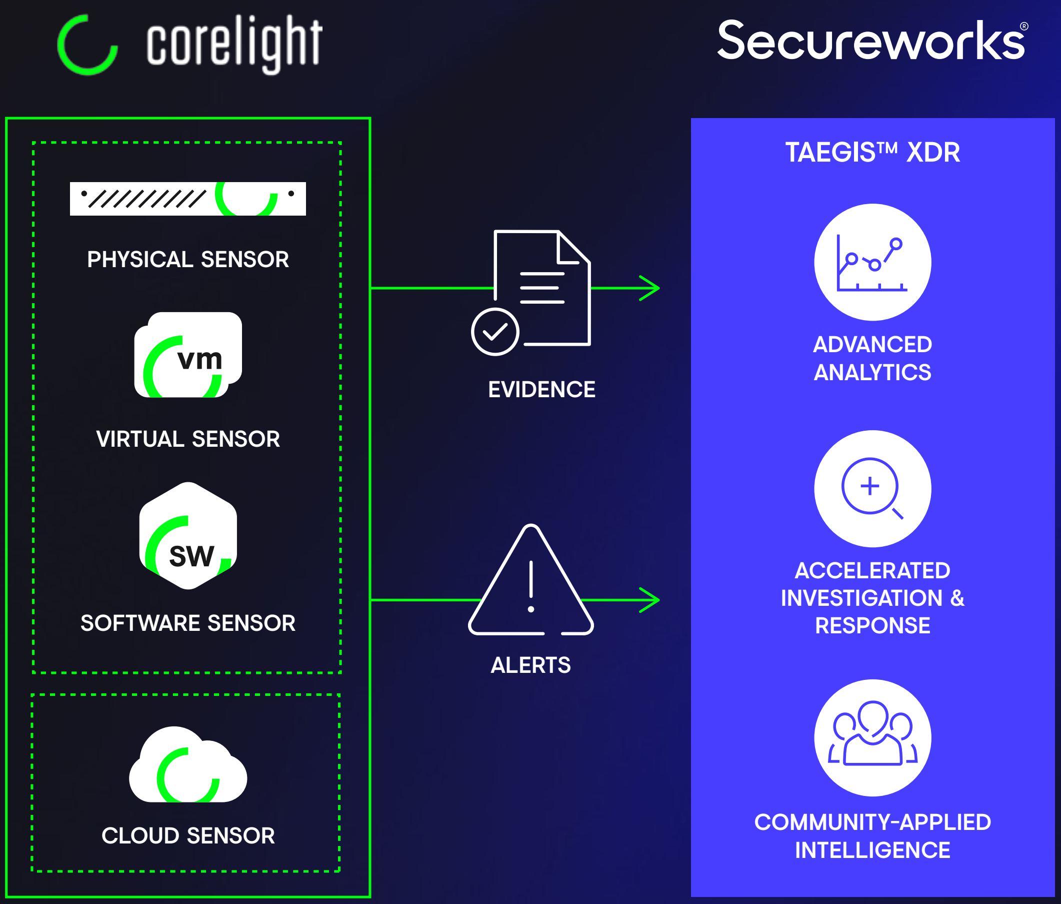
### Secureworks Differentiators

**20+**
Years of attack & threat data

**1,400**
IR engagements performed in the last year

**300+**
Expert security analysts, researchers & responders

**52,000**
Database of 52k unique threat indicators managed & updated daily



Taegis XDR includes a variety of Detectors that leverage Corelight evidence, correlated with telemetry across endpoint, network and cloud, to automatically identify malicious activity. XDR collects telemetry from Corelight's sensors to build rich security events using XDR Detectors.

- **IP Watchlist –**

This Taegis XDR Detector uses a Secureworks Counter Threat Unit™ Threat Intelligence curated list of suspicious IP addresses and compares them to Netflow telemetry collected via supported endpoint and syslog data sources. Endpoints that don't provide EDR telemetry result in metadata gaps. Corelight surpasses traditional Netflow data by monitoring network traffic to provide comprehensive network evidence that fills these endpoint data gaps and provides this XDR Detector with the required data to identify more suspicious IP addresses.

- **Domain Generation Algorithm (DGA) -**

In the past it was possible to block Command and Control (C&C) domains through proxies or content filters. However, with the evolution of DGA, malware authors use an algorithm to periodically generate many domain names to connect to. These domains change frequently, making it impossible for proxies and content filters to keep up. Corelight collects DNS requests off the network, which provide evidence leveraged by Taegis XDR. By evaluating DNS data from Corelight against known information on real and malicious domains, as well as your organization's streaming DNS data, XDR can identify domains that may indicate malicious activity.

- **Kerberoasting Detector**

Kerberoasting is a privilege escalation technique which proves to be very effective in extracting service account credentials in a domain environment. If an adversary/ penetration tester has domain credentials a domain can be compromised within a short period of time. Corelight provides Taegis XDR with the necessary network evidence to identify a possible Kerberos Ticket Granting Service (TGS) Service Ticket (ST) attack where a threat actor gathers, extracts, and cracks account password hashes offline in order to recover plaintext passwords.

- **Tactic Graph™**

Tactic Graph When countermeasures block or detect these, the adversaries are forced to modify their tactics in order to continue to operate. It's an arms race where threat actors and countermeasure developers are constantly iterating on their tactics and the countermeasures to stop them. The Secureworks Taegis XDR Tactic Graph™ Detector breaks this cycle through adversary behavior modeling. When tactics are identified in your environment Secureworks Taegis XDR generates alerts which are displayed in your Secureworks Taegis XDR tenant. When tactics are identified in your environment Secureworks Taegis XDR generates alerts which are displayed in your Secureworks Taegis XDR tenant.

Corelight network evidence contributes to several XDR Detectors, including:

- Tactic Graphs
- Domain Generation Algorithm
- Punycode
- Login Failure
- DDoS Source IP
- IP Watchlist
- Domain Watchlist
- Portscanning and Broadscanning
- Kerberoasting
- Network IDS

## Customer Benefits

- Save time with intuitive investigation workflows and single view across endpoint, network, and cloud.
- Fill endpoint visibility gaps with superior Network Detection and Response evidence.
- Avoid alert fatigue and understand which alerts are important with AI-based threat detection.
- Reduce blind spots with strong network evidence, even in DNS and encrypted traffic

## Conclusion

Together, Secureworks and Corelight deliver improved security, visibility, and time to remediation so you can reduce risk and more confidently run your business. For organizations without a SOC or enough skilled analysts, Secureworks can manage the solution for you with Secureworks Taegis ManagedXDR.

**About Secureworks**
Secureworks (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks Taegis, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

**About Corelight**
Corelight gives defenders unparalleled insight into networks to help them protect the world's most critical organizations and companies. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. The company has received investment support from Accel, General Catalyst, Insight Partners and Osage University Partners. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek, the widely-used network security technology. For more information, visit [https://www.corelight.com](https://www.corelight.com) or follow @corelight_inc.

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist **[secureworks.com](https://secureworks.com)**