CENTRALIZED LOG MANAGEMENT (CLM)

UNCOVER HIDDEN THREATS WITH FULL LOG DATA VISIBILTY

The Value of Log Analysis

Log analysis is a powerful tool for uncovering and analyzing suspicious system activities. System logs include network activities, system events, user actions, and more across the operating environment. Unfortunately, continuously accessing and analyzing log data from each individual system is tedious and simply impractical.

The Solution: Centralized Log Management

Cynet Centralized Log Management automatically collects the highest priority log data needed to quick and accurately uncover threats across your environment. Events and data are collected from network devices and applications, SaaS applications and all Cynet hosts. Log data is collected, integrated and normalized in the Cynet data lake, accessible directly from the Cynet console. You can also use Centralized Log Management to meet compliance requirements around log retention and quickly assess adherence to compliance requirements.

Key Benefits

- **Centralized Log Management analysis threat for critical**
- **Gain actionable insights using intuitive analysis and visualization tools**
- **Easily comply with log retention requirements**
- **Improve visibility to eliminate security gaps and oversights**
- **Outsource log collection and retention with Cynet SaaS**

Log Data Sources

Cynet 360 AutoXDR™ Windows Events and File Monitoring data are automatically displayed in the Centralized Log Management console with no license or configuration required. The following data sources are certified for Cynet CLM, with others continually being added:

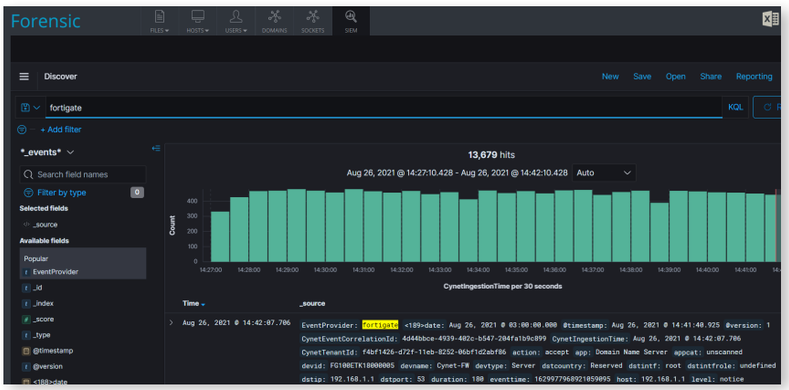
- SonicWall firewall
- FortiGate firewall
- Palo Alto Networks firewall
- WatchGuard firewall
- Office 365
- Azure Active Directory
- Zoom

Log Data Access

- 30 days of log data retention is included for instant search, query, and investigation
- 90 days of log data retention is optionally available for instant search, query, and investigation
- Unlimited cold retention is optionally available to help you meet various data storage compliance requirements

Leverage Existing Log Data for Actionable Insights

System logs contain a veritable goldmine of transaction and event history for uncovering and investigating security threats. Unfortunately, the time and effort required to mine this data leads to this data being underutilized or ignored. Harness the power of your existing system log data with Cynet Centralized Log Management by leveraging intuitive search, analysis, visualization and reporting tools.



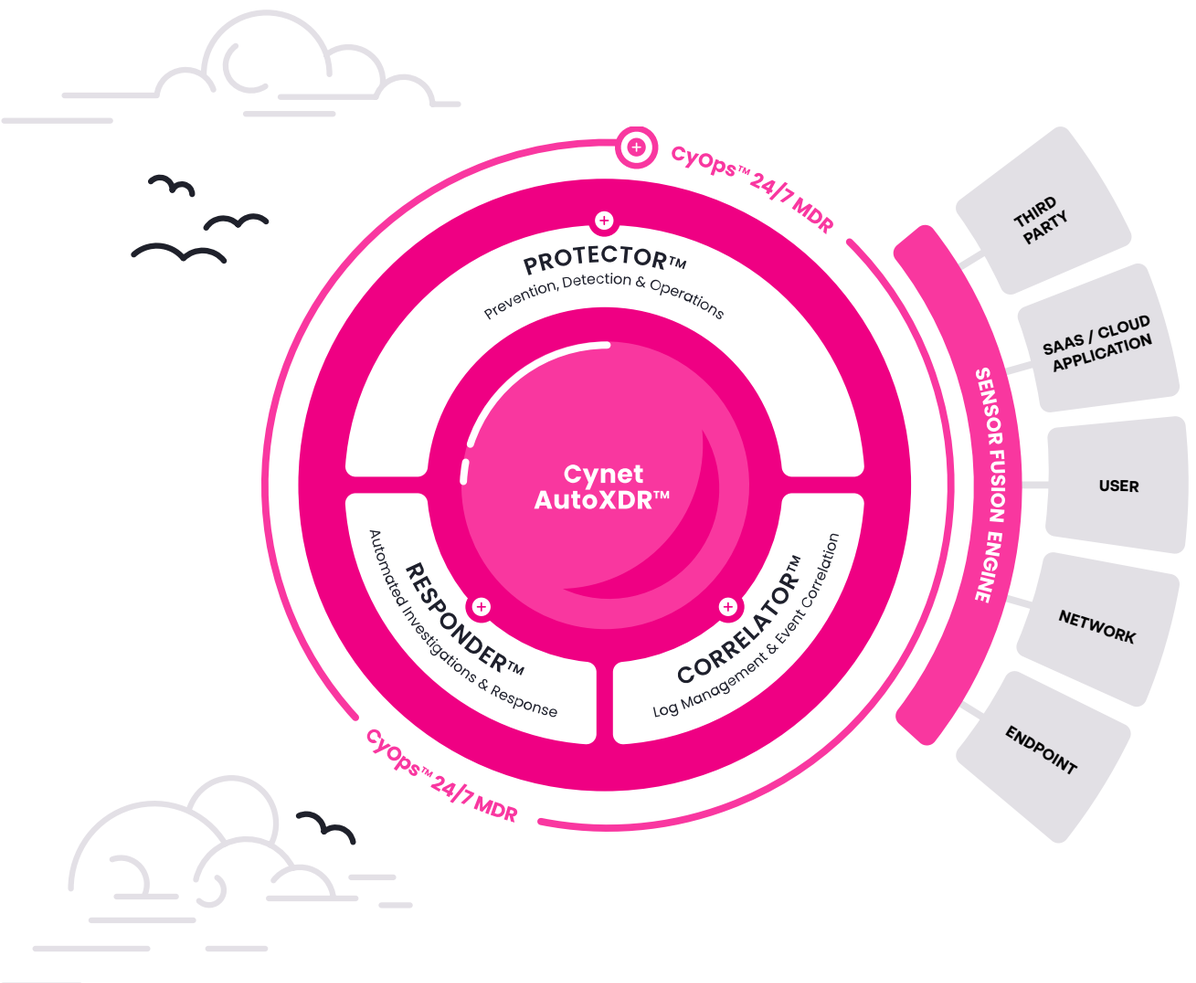
Easily Connect the Dots

- The ability to view, query and correlate events from firewalls, AD, endpoints in one forensic investigation experience enables you to connect the dots regarding a security incident.
- Example showing the distribution of firewall provider security events by time.

ABOUT US

Cynet's end-to-end, natively automated XDR platform, backed by a 24/7 MDR service was purpose-built to enable lean IT security teams to achieve comprehensive and effective protection regardless of their resources, team size or skills.

Cynet delivers the prevention and detection capabilities of EPP, EDR, NDR, Deception, UBA rules and CSPM, together with alert and activity correlation and extensive response automation capabilities.



Our vision is to enable security teams to put their cybersecurity on autopilot and focus their limited resources on managing security rather than operating it.

Bring sanity back to cybersecurity with a fresh approach that makes protecting your organization easy and stress-less.

FIPCO

Contact: Rob Foxx
FIPCO Director - InfoSec and IT Audit Services
rfoxx@fipco.com 800-722-3498, ext 249