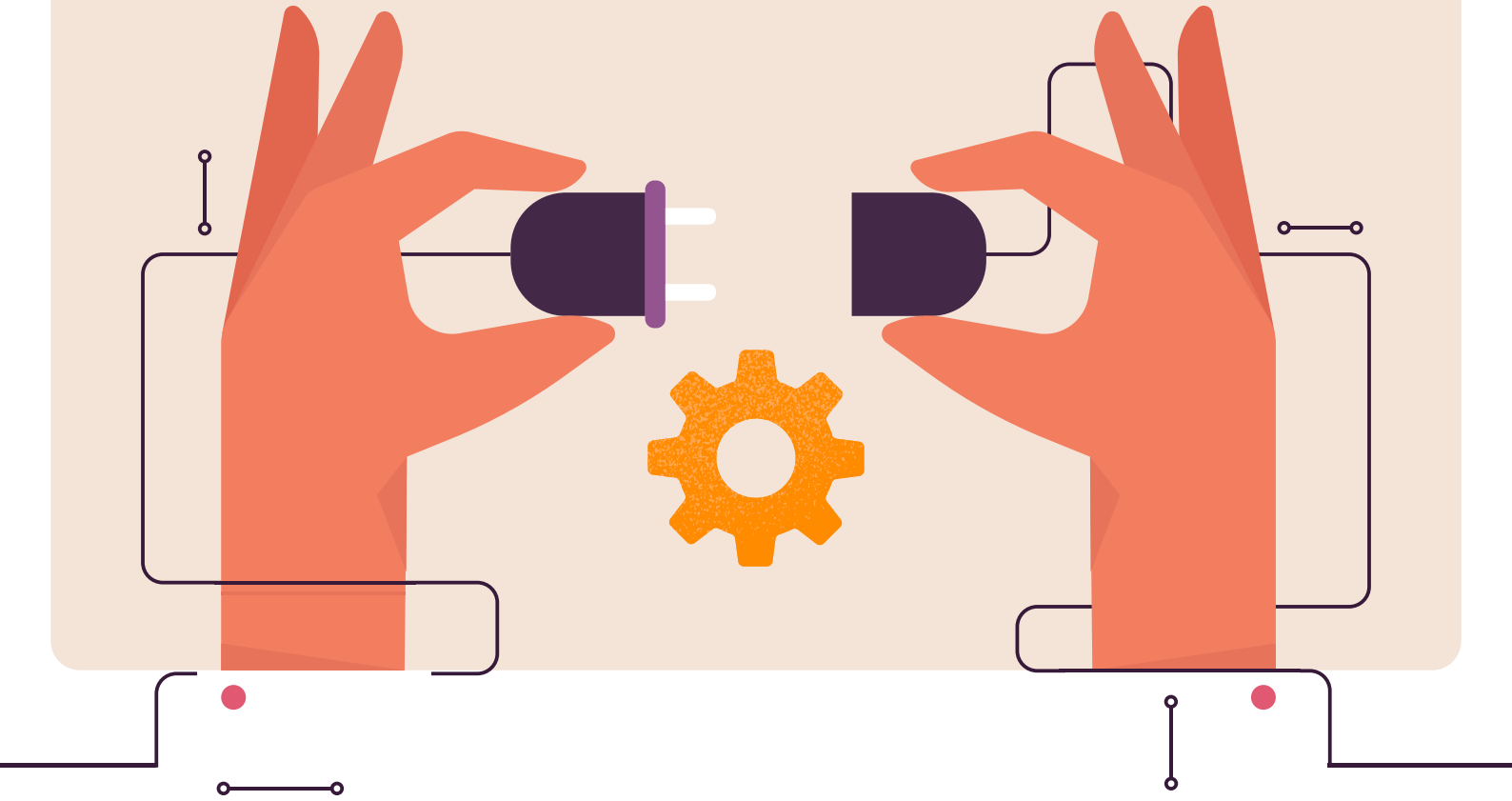
ManageEngine
Log360

DATASHEET

Unified security operation for effective threat detection and remediation

Log360's **integration with Endpoint Central**



Solving security silos challenges

A pressing security operations issue today is siloed security data points. Organizations manage an average of 45 security tools on their networks. Relying on an excessive number of tools could lead not just to difficulties in detecting, but also in defending against active attacks, according to ZDNet. This fragmentation often hinders visibility. Security teams spend an average of **277 days** to identify and contain a single breach, an Ponemon Institute determined.

The Log360 and ManageEngine Endpoint Central integration bridges this gap by fostering a **unified security environment.** This data sheet explores how this powerful integration addresses the challenges of data silos and empowers security teams with:

Contextual and enhanced threat detection:

Gain a holistic view of your security posture by ingesting security data points from Endpoint Central that adds visibility and non-event context for the effective correlation of network activities in Log360.This unified view enables pinpointing real threats amidst the noise, enriched with valuable endpoint context.

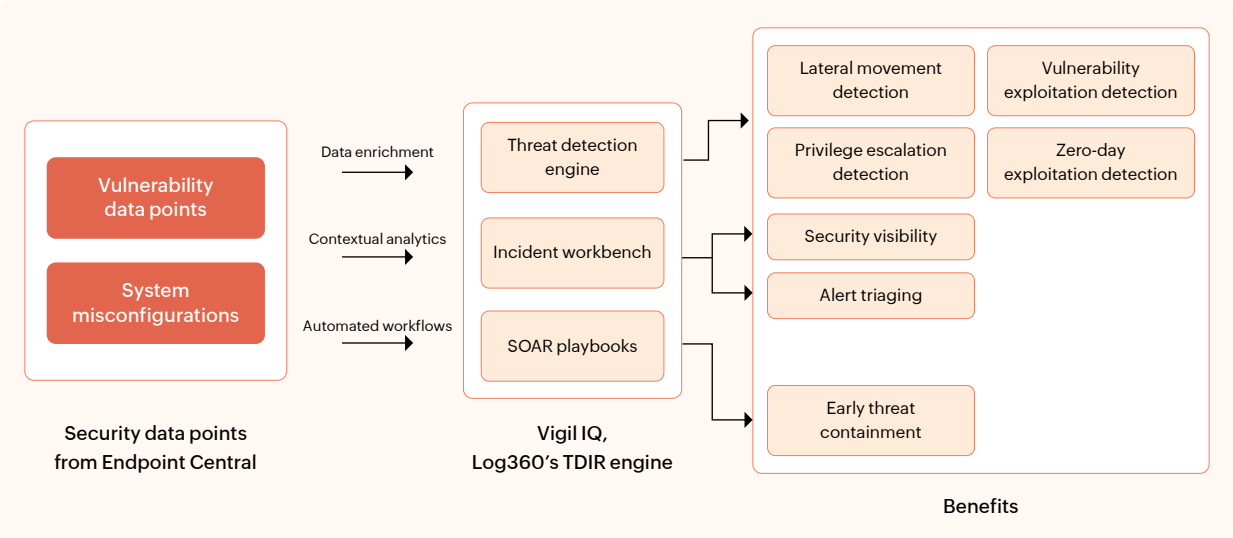
Streamlined investigation:

Investigate potential threats faster and more effectively with all relevant security data. The Incident Workbench of Log360 stitches together the suspicious security events in the form of an incident timeline for effective investigation.

Accelerated incident detection and response:

Reduce the time from security event to containment. Log360 leverages advanced analytics to detect high-fidelity threats. When a threat is identified, Log360 triggers automated workflows that initiate predefined actions within Endpoint Central to patch vulnerabilities. This translates to faster mean time to response (MTTR) and improved mean detection and response (MDR) capabilities.

How it works



Security operations challenges addressed by this integration

Use cases and challenges	How Log360 and EndPoint Central integration helps
Early threat detection	Automatically ingests security data points such as vulnerabilities and misconfigurations from Endpoint Central and contextually sweeps those entities for relevant traces of attacks. This enables you to detect the early indicators of compromises thus minimizing potential damage.
Lateral movement and privilege escalation detection	Ingests user account management misconfigurations and checks for lateral movement and privilege escalation attempts with an out-of-the-box threat detection rule. Endpoint Central provides visibility into endpoint health and behavior, aiding in identifying compromised machines that attackers may use as footholds.
Zero-day exploitation detection	Identifies the vulnerabilities instantly from the Endpoint Central and finds the zero-day exploits through anomaly detection.
Alert triaging	Prioritizes security alerts based on threat context and endpoint data. This reduces security analyst fatigue by focusing on the most critical alerts first. Endpoint context helps distinguish genuine threats from false positives.
Faster incident resolution	Automates incident response workflows. Upon threat detection, Log360 triggers actions within Endpoint Central to isolate endpoints, patch vulnerabilities, or contain threats. This reduces manual intervention and speeds up resolution times.

Additional benefits

- **Reduced security complexity:**
  Consolidate security data from disparate sources into a single pane of glass for simplified threat detection and investigation.

- **Improved security visibility:**
  Gain a holistic view of your IT infrastructure, including user activity, endpoint health, and network traffic.

About Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.
For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download

About Endpoint Central

Endpoint Central is a UEM and EPP solution that manages and secures today's digital workplace across diverse device types and OSs. Acclaimed by industry analysts like Gartner®, Forrester and IDC, it employs a single, lightweight agent to offer end-to-end device life cycle management, consolidated with security capabilities like attack surface management, threat detection and response and compliance. Robust remote troubleshooting, self-service capabilities and proactive analytics help reduce downtime and improve the overall end-user experience. Available both on-premises and as a SaaS solution, Endpoint Central is used by more than 25,000 enterprises globally, fitting perfectly into their existing IT infrastructures and enabling interoperability. For more information, visit manageengine.com/endpoint-central.