ManageEngine

Take control of your IT

ManageEngine
Log360 MSSP

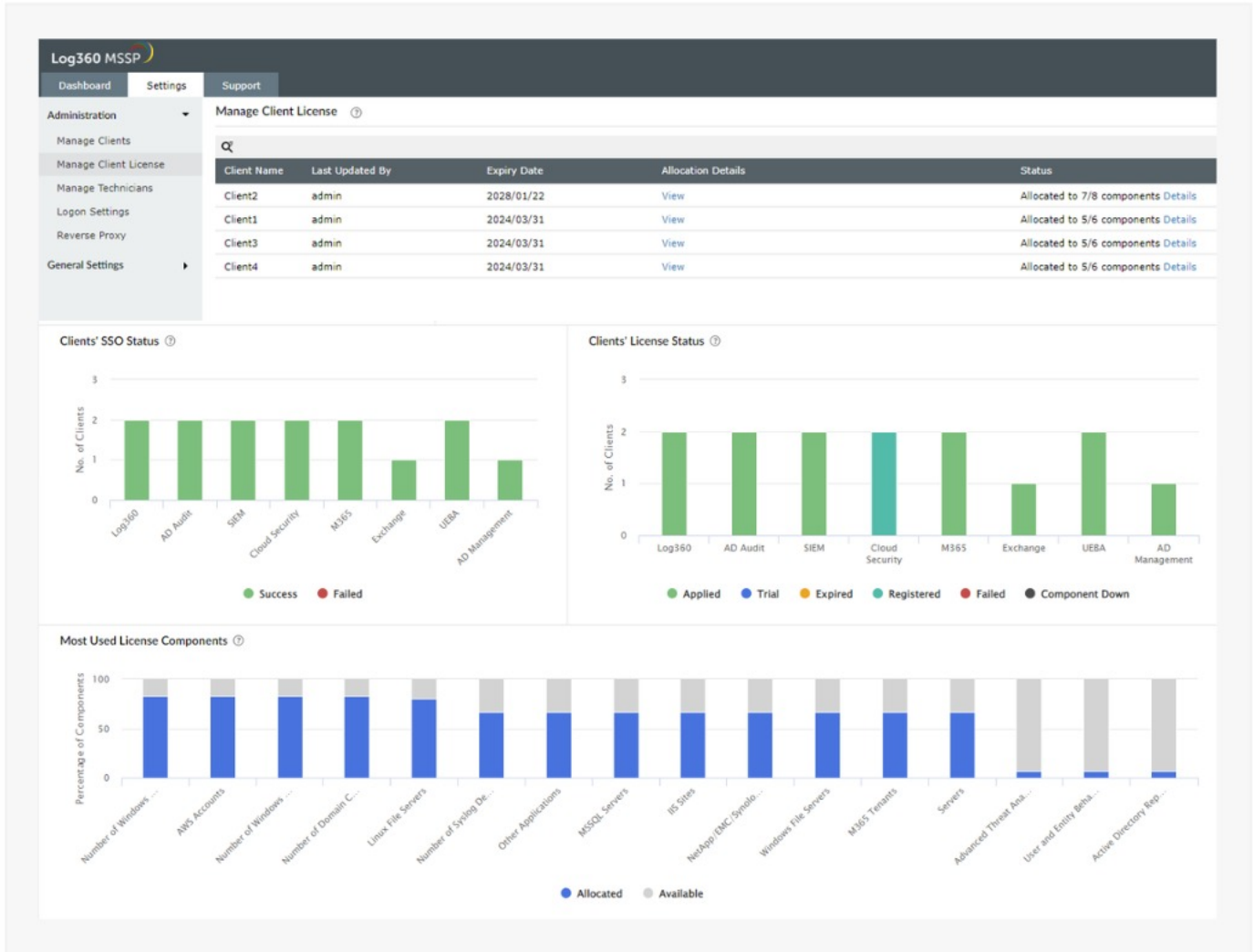
The unified SIEM for MSSPs

What does Log360 MSSP offer?

- Centralized license management
- Centralized technician management
- Single sign-on
- Client health monitoring

ManageEngine
Log360 MSSP

Centralized License management



ManageEngine
Log360 MSSP

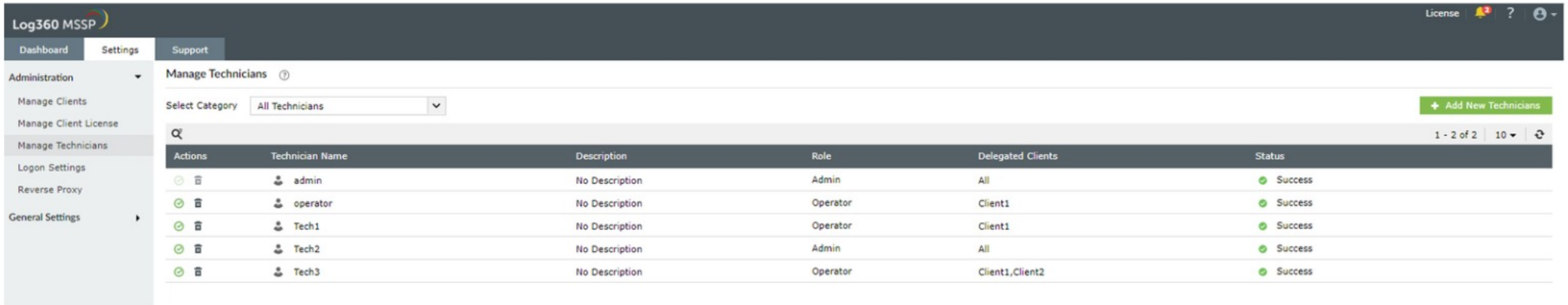
Centralized dashboard to monitor and manage licenses for all clients

- **License visibility:**
  Easily view clients' license status from the main dashboard or client management page

- **Detailed license information:**
  Access comprehensive license details for each client on the client management page (including expiration dates), enabling prompt action if licenses are nearing expiration

ManageEngine
Log360 MSSP

Centralized technician management



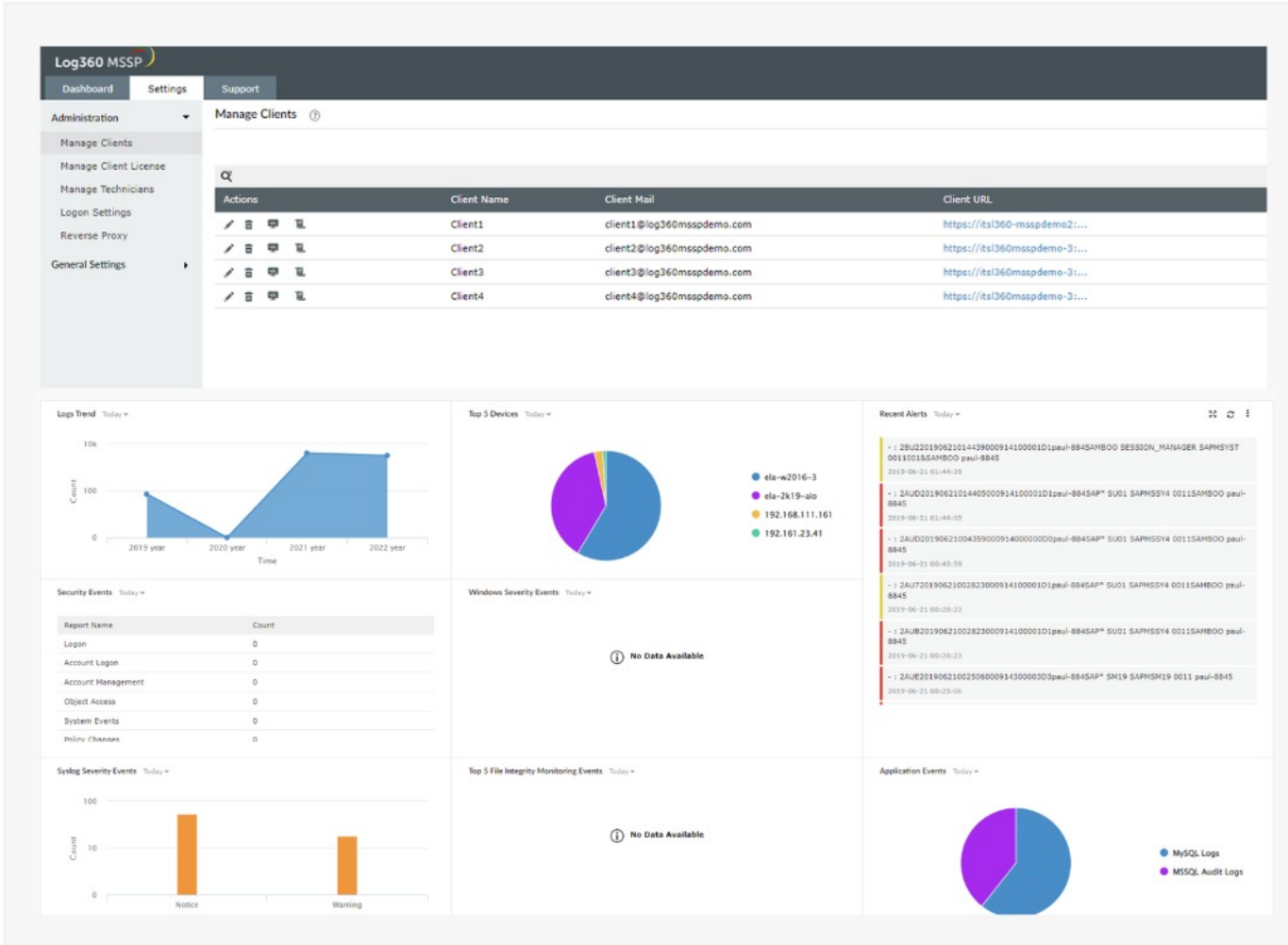
ManageEngine
Log360 MSSP

Centralized technician management and resource allocation

- **Create technicians**
  Easily onboard technicians with predefined roles and access levels

- **Delegate to clients**
  Assign technicians to clients based on expertise and workload

Single sign-on (SSO)



ManageEngine
Log360 MSSP

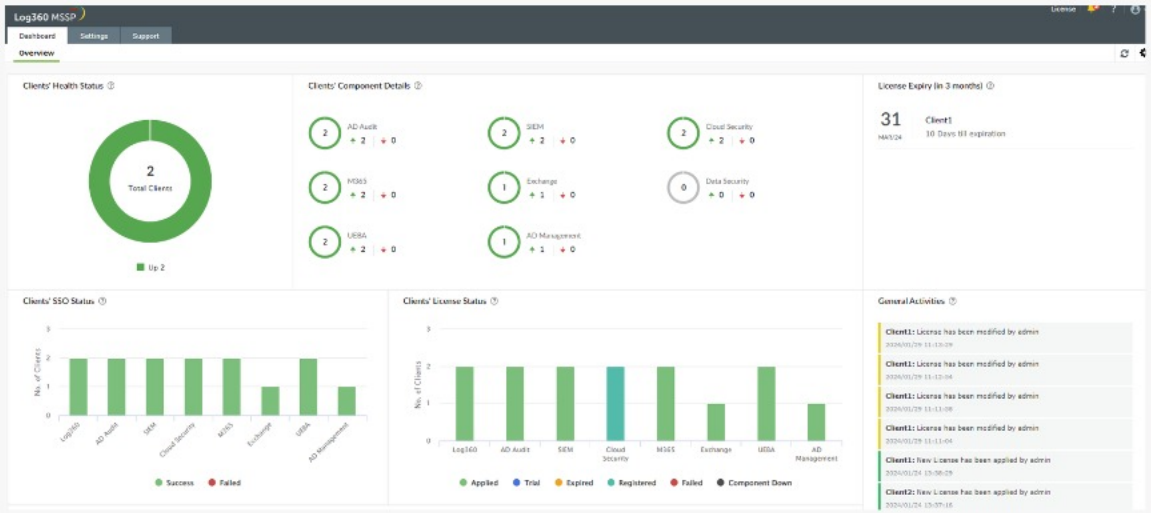
Integrated SSO functionality to allow technicians to seamlessly access client environments

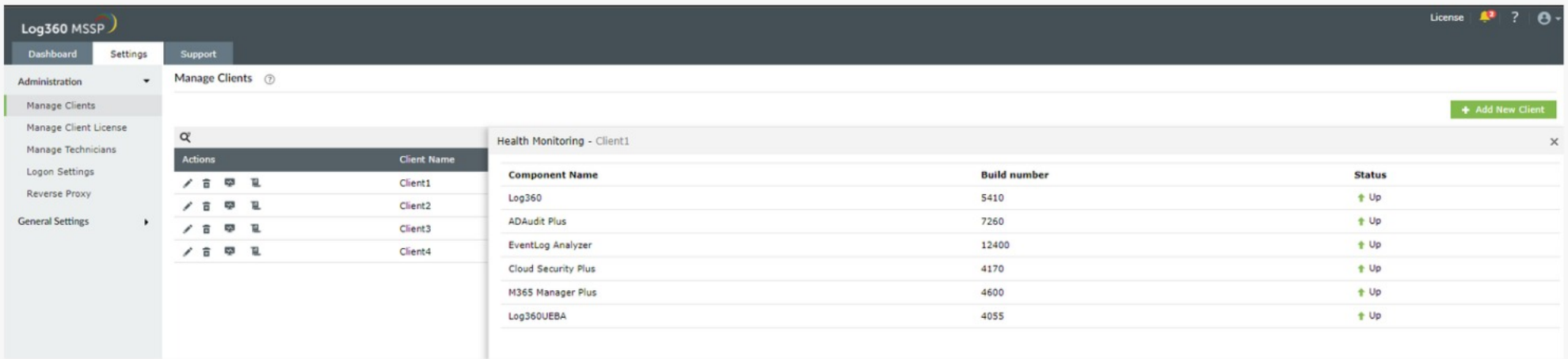
- **Streamlined access management:**
  Securely access multiple applications with one set of credentials

- **Unified access:**
  Technicians seamlessly access client environments through a single portal

ManageEngine
Log360 MSSP

Client Health monitoring





ManageEngine
Log360 MSSP

Real-time health monitoring of each client's network and its network components

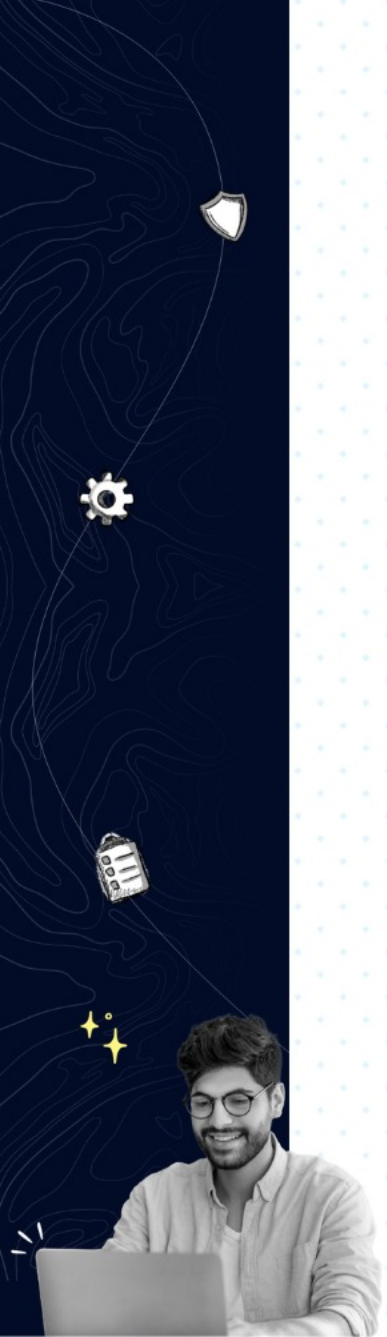
- **Proactive issue detection:**
  Detect and address potential issues in both client environments and network components

- **Real-time monitoring:**
  Ensure the health and stability of client environments and network components

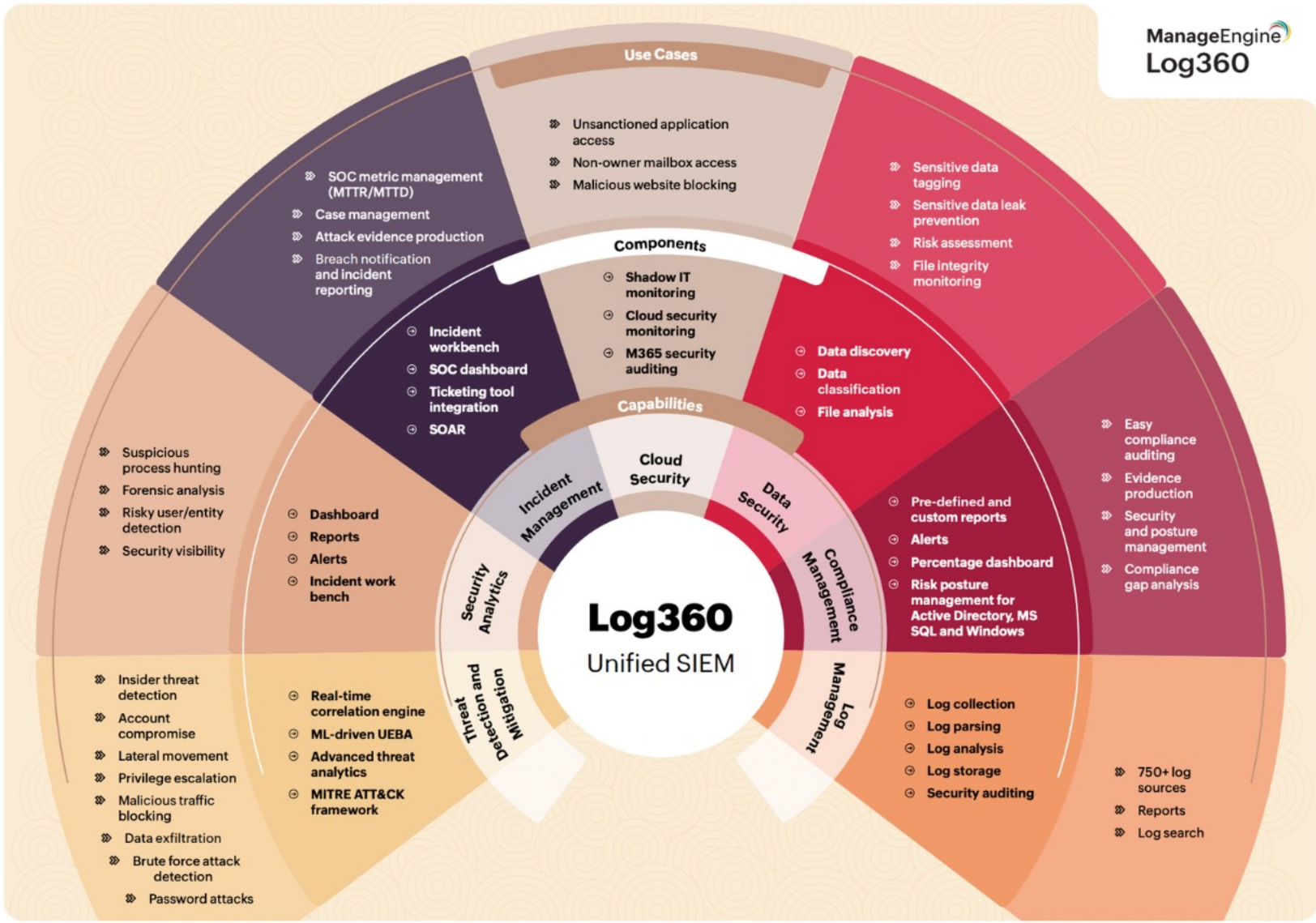
Core SIEM functionalities

of Log360 MSSP

ManageEngine
Log360 MSSP

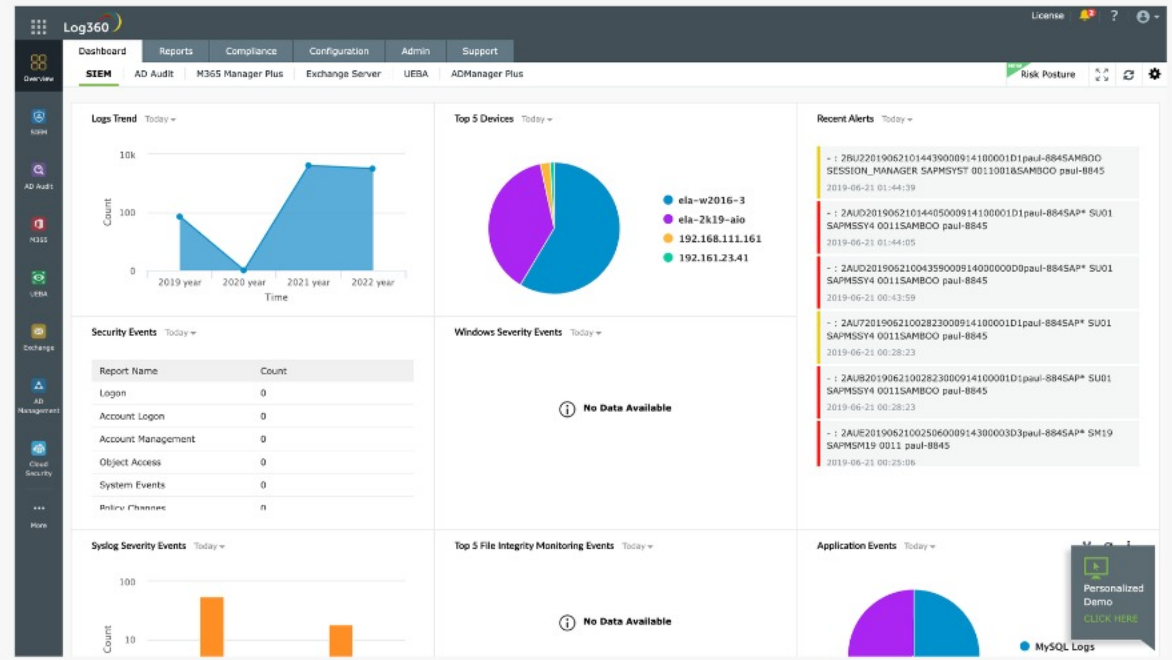


ManageEngine
Log360



ManageEngine
Log360 MSSP

A comprehensive SIEM solution for your network



ManageEngine
Log360 MSSP

Single console for network information

- Collect, analyze, and report events from more than 750+ log sources
- Get complete visibility into log data, network traffic, and security events
- Use advanced threat analytics to get valuable insights into the severity of threats with reputation-based scoring
- Leverage STIX/TAXII and AlienVault OTX threat feeds to discover malicious IPs, domains, and URLs
- Gain actionable insights with an intuitive dashboard that gathers the log data and assists you in developing an effective incident response plan

ManageEngine
Log360 MSSP

Threat detection and investigation

ManageEngine
Log360 MSSP

Correlation

- Powerful correlation engine equips you with 30 predefined attack patterns
- Custom correlation builder allows you to create custom correlation rules, specify time frames, and use advanced filters for detecting attacks

How correlation works

How correlation works for pass-the-hash attack

Event ID 10

Indicates that a process has accessed another process

Event ID4624 & 4672

An account was successfully logged on & special privileges have been assigned

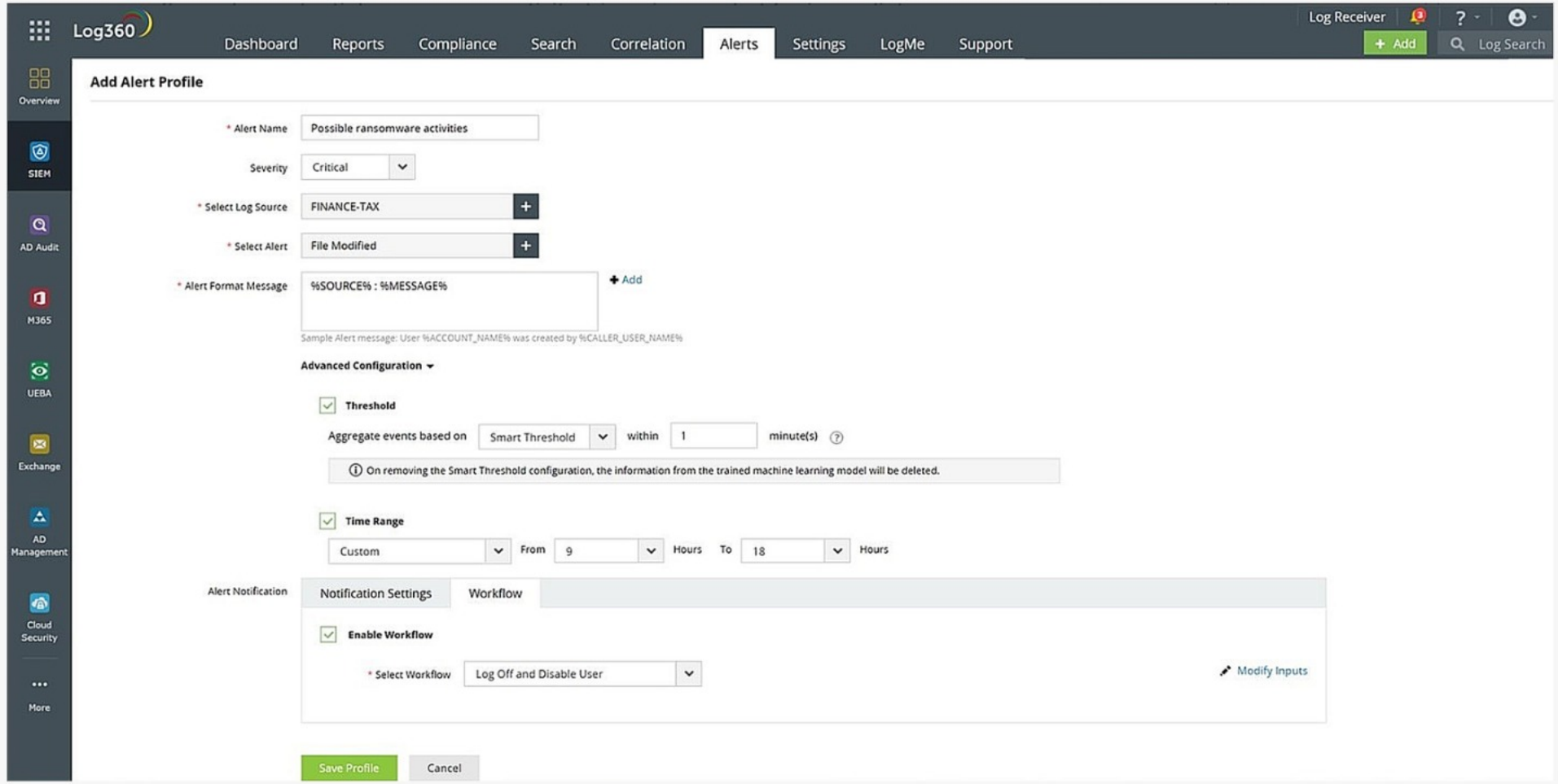
Attack suspected

ManageEngine
Log360 MSSP

Adaptive threshold

- Leverage a ML-based dual layered TDIR engine with smart threshold capability to eliminate false positives
- The adaptive threshold sets a baseline of normal activity to flag anomalous activity or suspicious correlation of events instantly

ManageEngine
Log360 MSSP

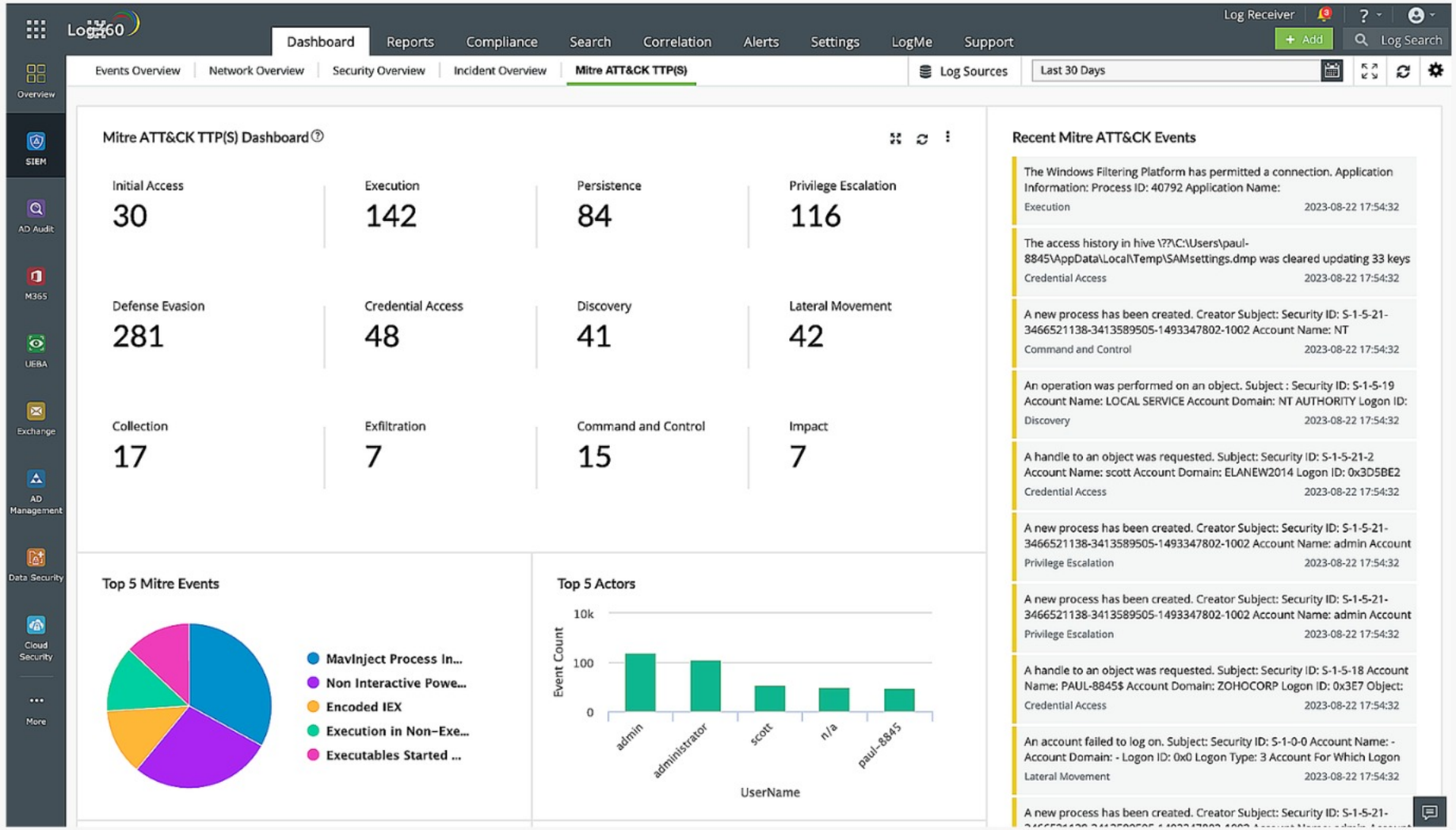


ManageEngine
Log360 MSSP

MITRE ATT&CK

- Stay up to date with the specific tactics and techniques used by threat actors when carrying out an attack
- Gain insights into the 12 ATT&CK tactics and their corresponding techniques through the security analytics dashboard

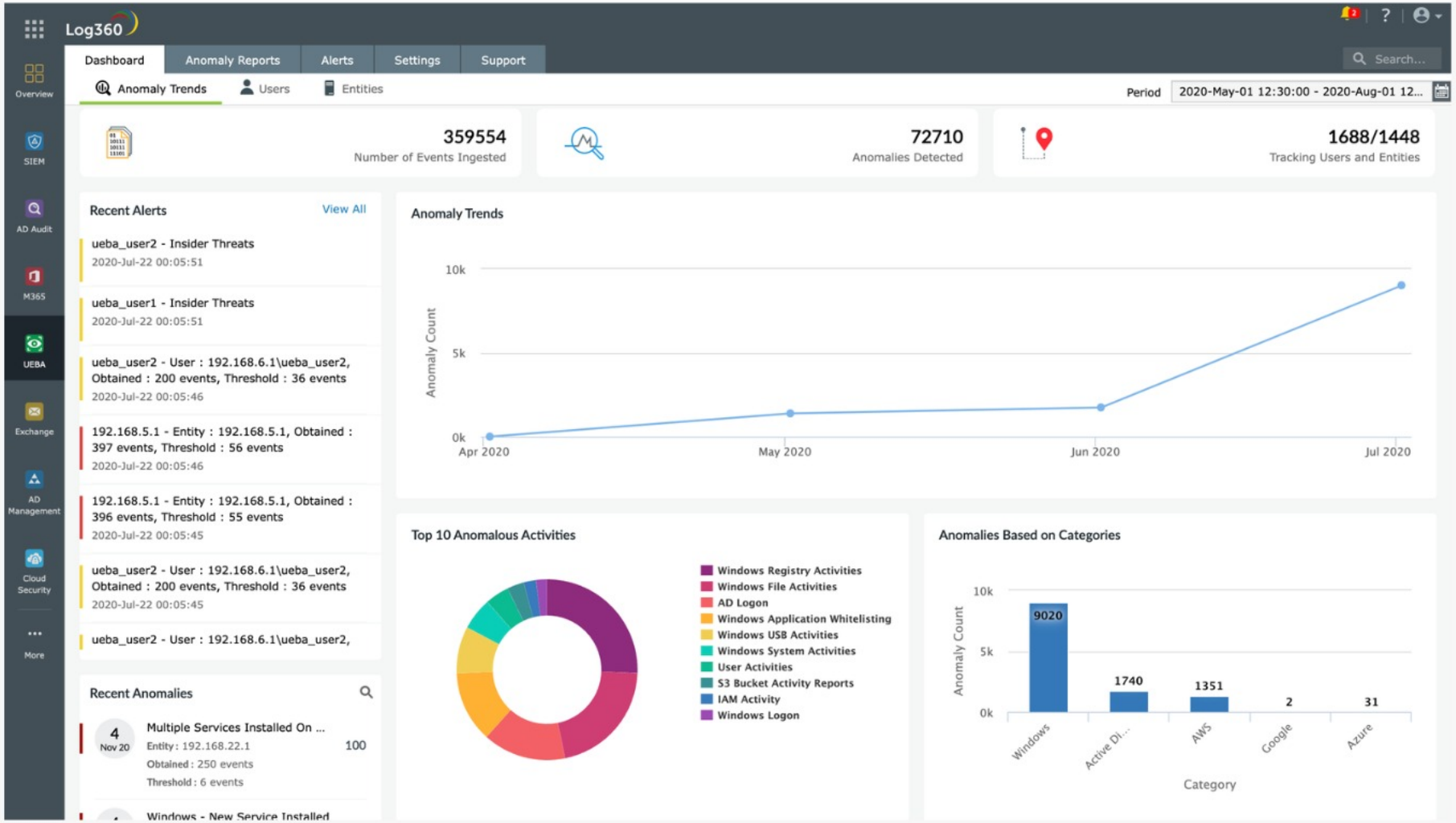
ManageEngine
Log360 MSSP



ManageEngine
Log360 MSSP

UEBA

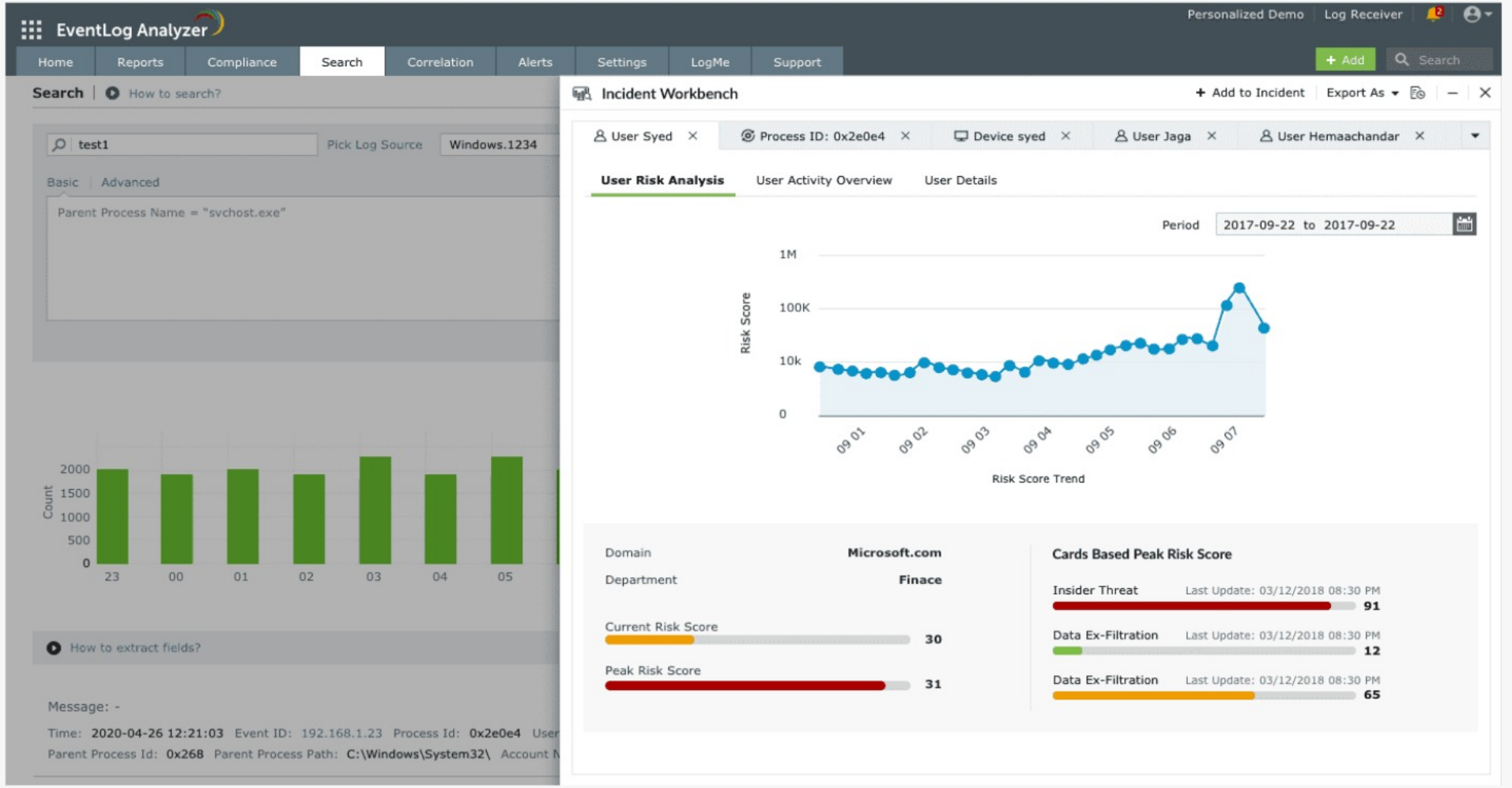
- Use machine learning to analyze patterns of users and other entities in the network to detect behavioral anomalies and anomalous activity
- Spot anomalies using time-based, count-based, and pattern-based detection techniques



ManageEngine
Log360 MSSP

Threat investigation workbench

- Add, compare, and analyze core digital artifacts like users, devices, and processes using Log360's threat detection workbench
- Analyze IPs with Log360's advanced threat analytics (ATA) integrations, including VirusTotal (one of the largest live threat feeds offering domain risk scores consolidated from multiple security vendors), Whois information of the threat source, and the associated files



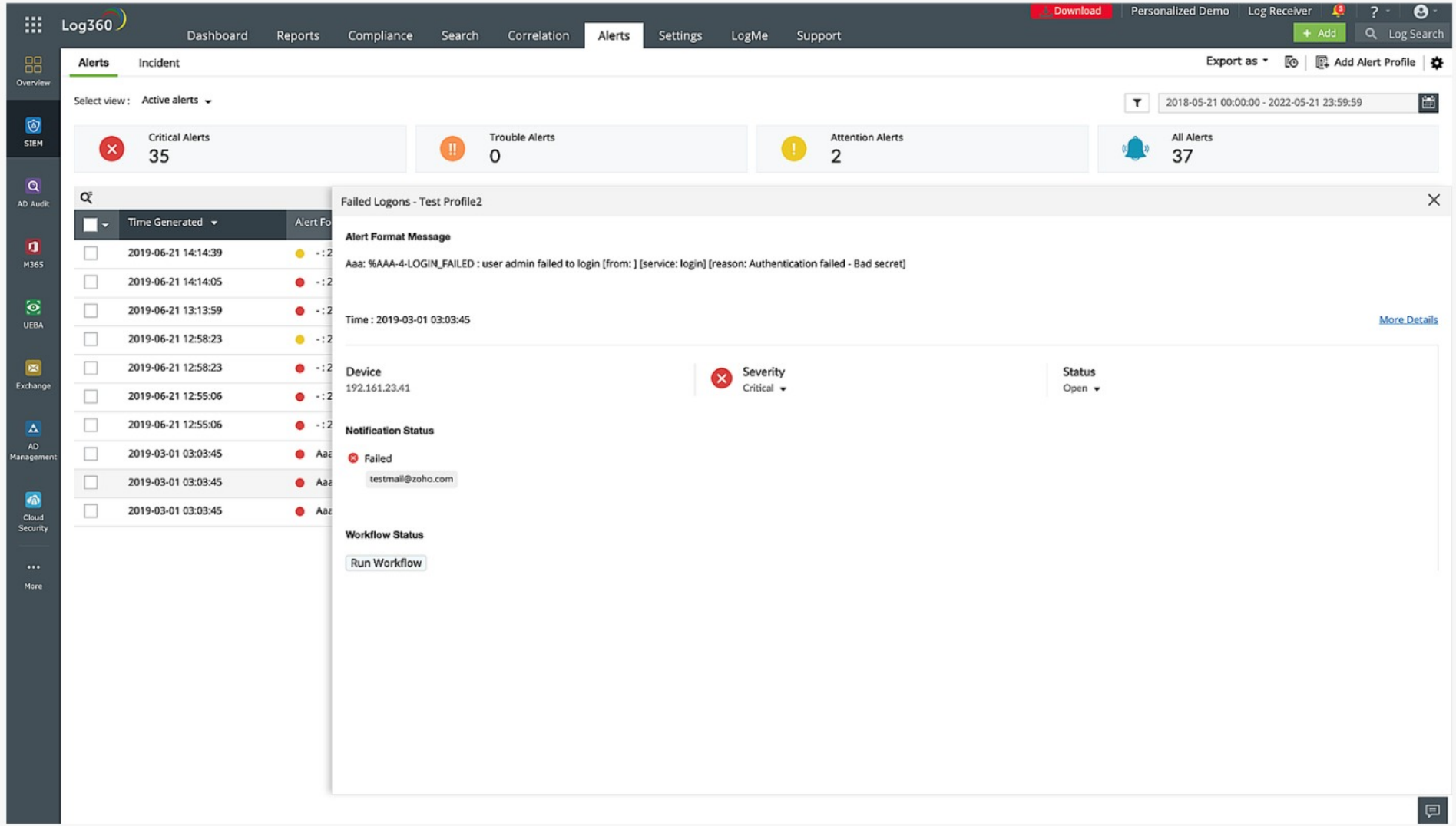
ManageEngine
Log360 MSSP

Incident response and management

ManageEngine
Log360 MSSP

Single console for network information

- Strengthen your incident management with Log360's dedicated incident overview dashboard
- Gain insight into incidents that are active, unresolved, recent, or critical to manage and prioritize incident resolution
- Reduce the mean time to detect (MTTD) and the mean time to resolve (MTTR) an incident by quickly detecting, categorizing, analyzing, and resolving an incident accurately with a centralized console
- Get instant alerts (categorized into three severity levels: Attention, Trouble and Critical) to prioritize and remediate the threat accordingly



ManageEngine
Log360 MSSP

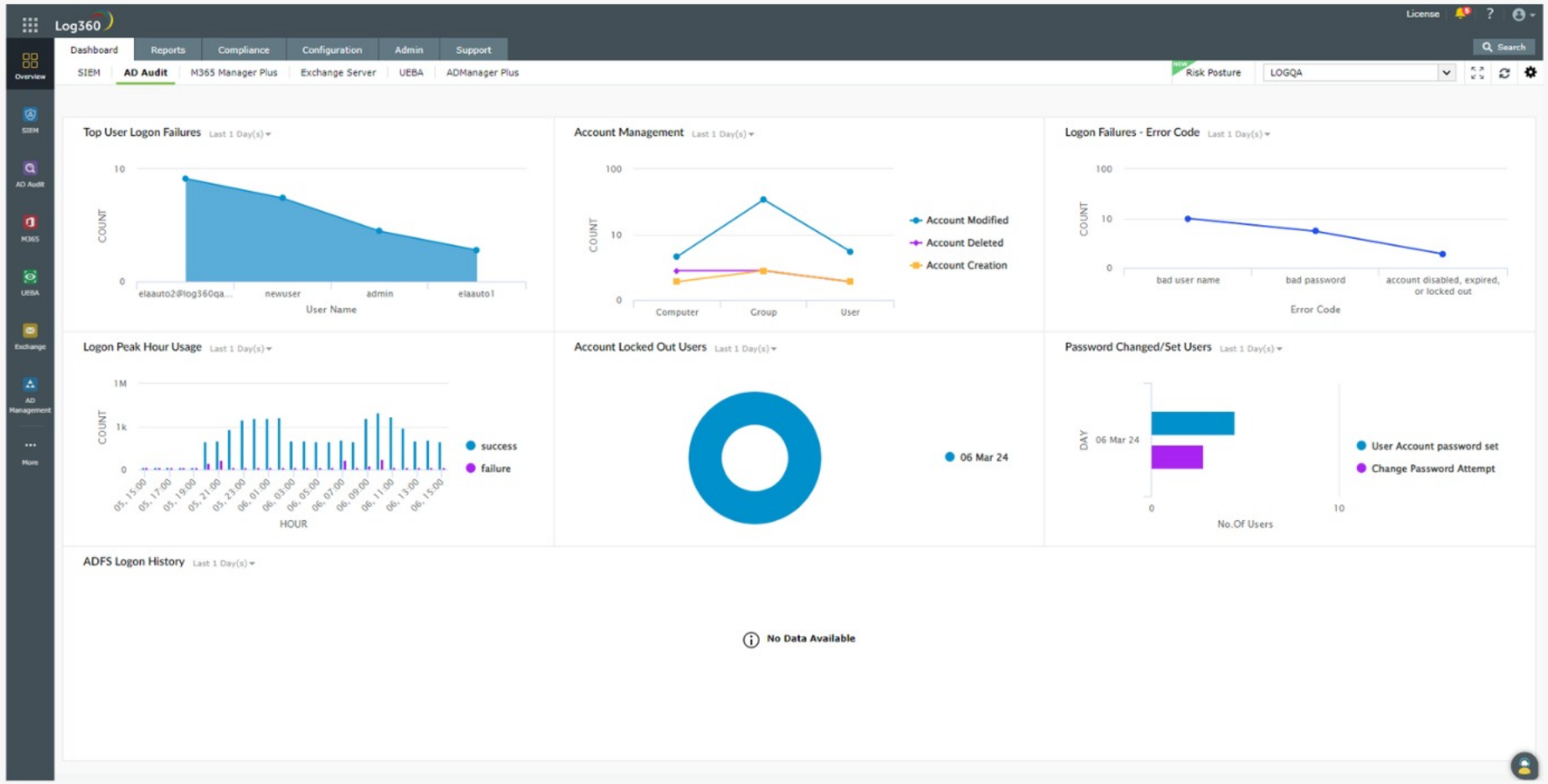
Active Directory (AD) auditing and reporting

ManageEngine
Log360 MSSP

Audit critical changes

- Monitor all security group membership changes, unauthorized logon attempts, account lockouts, OU permission changes, and any other security event of interest occurring in AD with extensive, predefined audit reports
- Get real-time alerts on user activities, AD object changes, account lockouts, and more, helping you to instantly detect changes that pose a threat to security

ManageEngine
Log360 MSSP



ManageEngine
Log360 MSSP

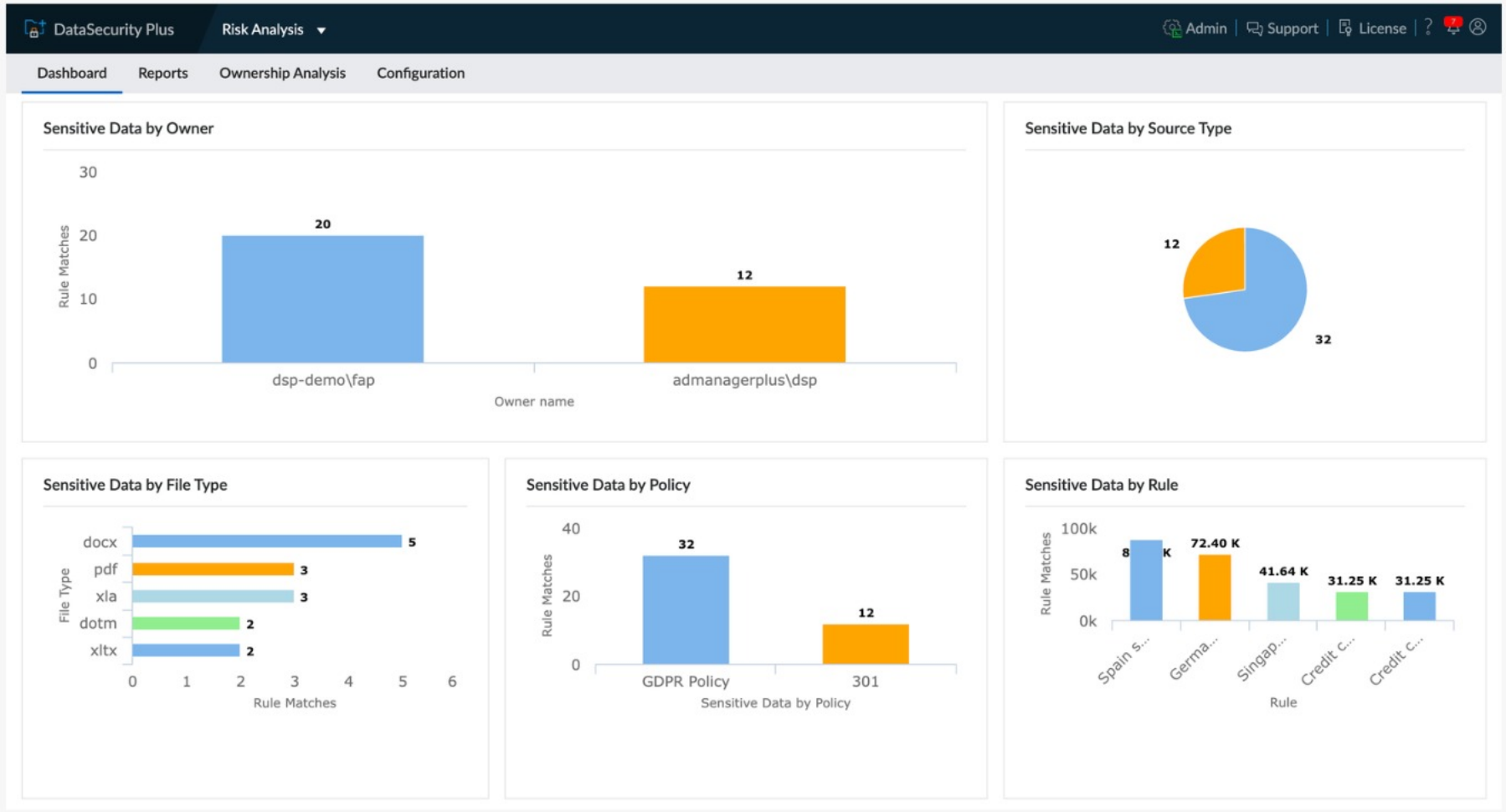
Data security monitoring

ManageEngine
Log360 MSSP

Monitor access to sensitive data

- Discover sensitive data (PII, PHI, etc.) across your network using predefined and custom policies
- Ensure integrity of confidential files and folders with file integrity monitoring
- Get real-time alerts for unauthorized file accesses, permission changes, and modifications

ManageEngine
Log360 MSSP



ManageEngine
Log360 MSSP

ManageEngine
Log360 MSSP

Thank you!

Contact

log360-support@manageengine.com