



ManageEngine

**Take control
of your IT**



ManageEngine
Log360 MSSP

The unified **SIEM for MSSPs**

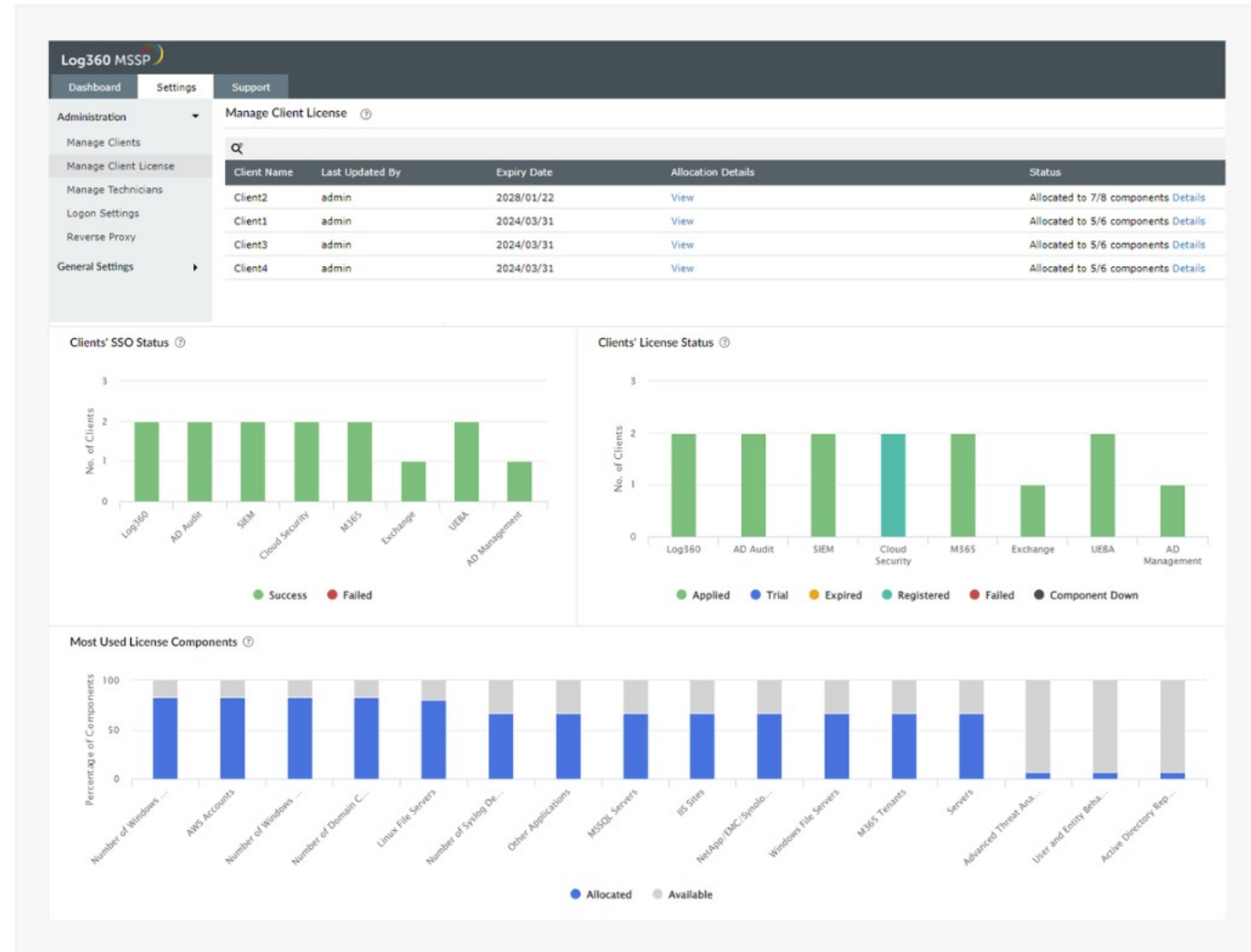


What does Log360 MSSP offer?

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



Centralized License management



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



Centralized technician management

Log360 MSSP

License [icon] [icon] [icon]

Dashboard Settings Support

Administration

- Manage Clients
- Manage Client License
- Manage Technicians
- Logon Settings
- Reverse Proxy

General Settings

Manage Technicians ⓘ

Select Category: All Technicians

[+ Add New Technicians](#)

1 - 2 of 2 10

Actions	Technician Name	Description	Role	Delegated Clients	Status
	admin	No Description	Admin	All	Success
	operator	No Description	Operator	Client1	Success
	Tech1	No Description	Operator	Client1	Success
	Tech2	No Description	Admin	All	Success
	Tech3	No Description	Operator	Client1,Client2	Success



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)

The screenshot displays the Log360 MSSP dashboard. The top navigation bar includes 'Dashboard', 'Settings', and 'Support'. The left sidebar lists 'Administration' (Manage Clients, Manage Client License, Manage Technicians, Logon Settings, Reverse Proxy) and 'General Settings'. The main content area is titled 'Manage Clients' and features a search bar and a table with the following data:

Actions	Client Name	Client Mail	Client URL
[edit] [delete] [refresh]	Client1	client1@log360msspdemo.com	https://its360-msspdemo2:...
[edit] [delete] [refresh]	Client2	client2@log360msspdemo.com	https://its360msspdemo-3:...
[edit] [delete] [refresh]	Client3	client3@log360msspdemo.com	https://its360msspdemo-3:...
[edit] [delete] [refresh]	Client4	client4@log360msspdemo.com	https://its360msspdemo-3:...

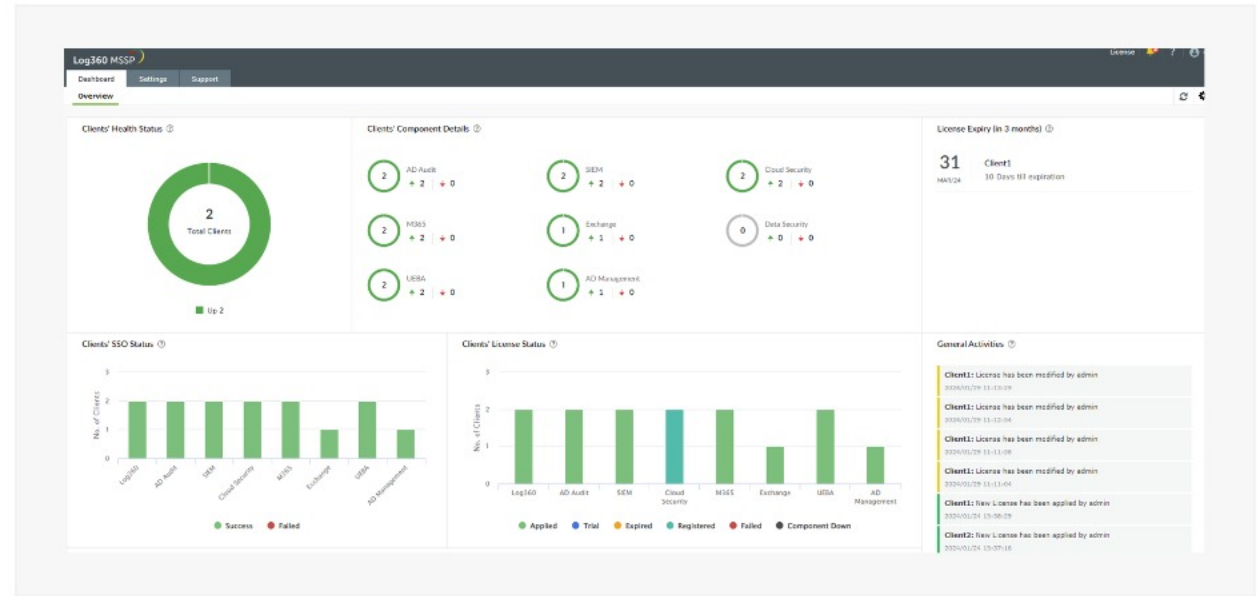
Below the table are several monitoring widgets:

- Log Trend Today:** A line chart showing log counts from 2019 to 2022. The count is approximately 100 in 2019, drops to 0 in 2020, and rises to about 800 in 2021 and 2022.
- Top 5 Devices Today:** A pie chart showing device distribution. The legend includes: ela-w2016-3 (blue), ela-2k19-alo (purple), 192.168.111.161 (yellow), and 192.161.23.41 (green).
- Recent Alerts Today:** A list of alerts with details such as time, IP address, and user information.
- Security Events Today:** A table showing counts for various security reports: Logon (0), Account Logon (0), Account Management (0), Object Access (0), System Events (0), and Policy Changes (0).
- Windows Severity Events Today:** A message indicating 'No Data Available'.
- Syslog Severity Events Today:** A bar chart showing counts for 'Notice' (approx. 80) and 'Warning' (approx. 20) events.
- Top 5 File Integrity Monitoring Events Today:** A message indicating 'No Data Available'.
- Application Events Today:** A pie chart showing the distribution of application events, with a legend for MySQL Logs (blue) and MSSQL Audit Logs (purple).

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

Client Health monitoring



The Manage Clients interface allows for detailed monitoring and management of individual clients. Below is the health monitoring data for Client1:

Component Name	Build number	Status
Log360	5410	Up
ADAudit Plus	7260	Up
EventLog Analyzer	12400	Up
Cloud Security Plus	4170	Up
M365 Manager Plus	4600	Up
Log360UEBA	4055	Up

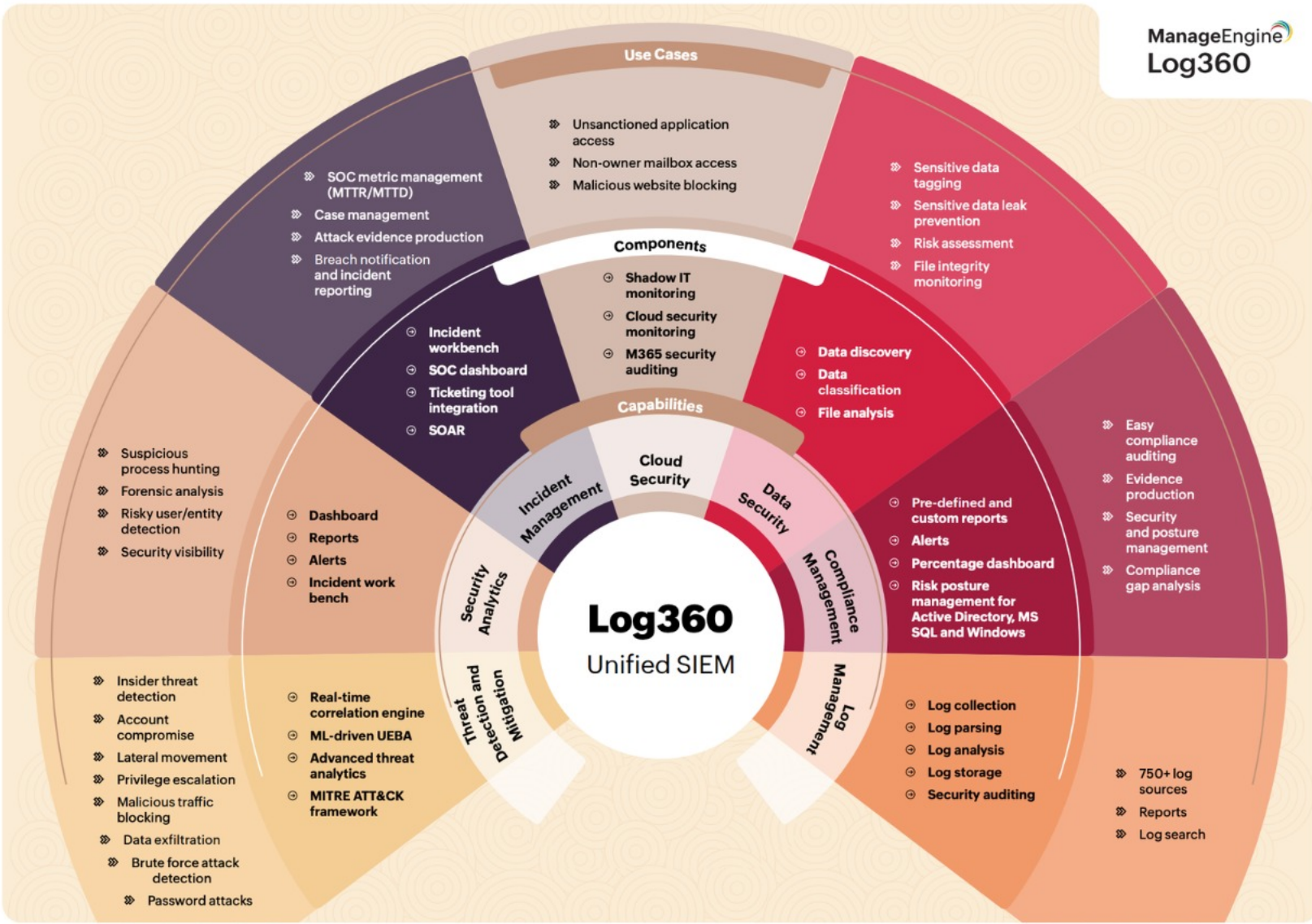
Real-time health monitoring of each client's network and its network components

- ◆ **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

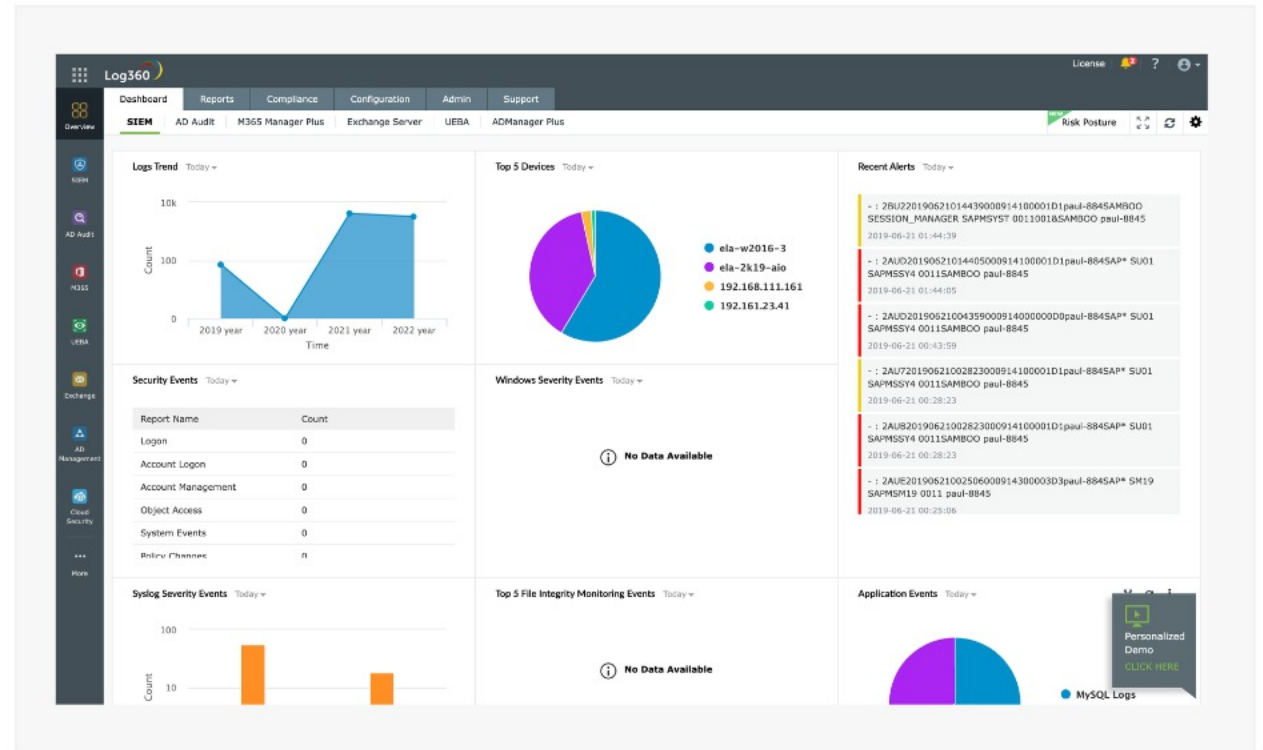


Core SIEM functionalities of Log360 MSSP





A comprehensive SIEM solution for your network



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



Threat detection and investigation



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



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



Log360 Dashboard Reports Compliance Search Correlation Alerts Settings LogMe Support

Log Receiver + Add Log Search

Add Alert Profile

* Alert Name: Possible ransomware activities

Severity: Critical

* Select Log Source: FINANCE-TAX

* Select Alert: File Modified

* Alert Format Message: %SOURCE% : %MESSAGE% + Add

Sample Alert message: User %ACCOUNT_NAME% was created by %CALLER_USER_NAME%

Advanced Configuration

Threshold
Aggregate events based on Smart Threshold within 1 minute(s)
On removing the Smart Threshold configuration, the information from the trained machine learning model will be deleted.

Time Range
Custom From 9 Hours To 18 Hours

Alert Notification

Notification Settings Workflow

Enable Workflow

* Select Workflow: Log Off and Disable User

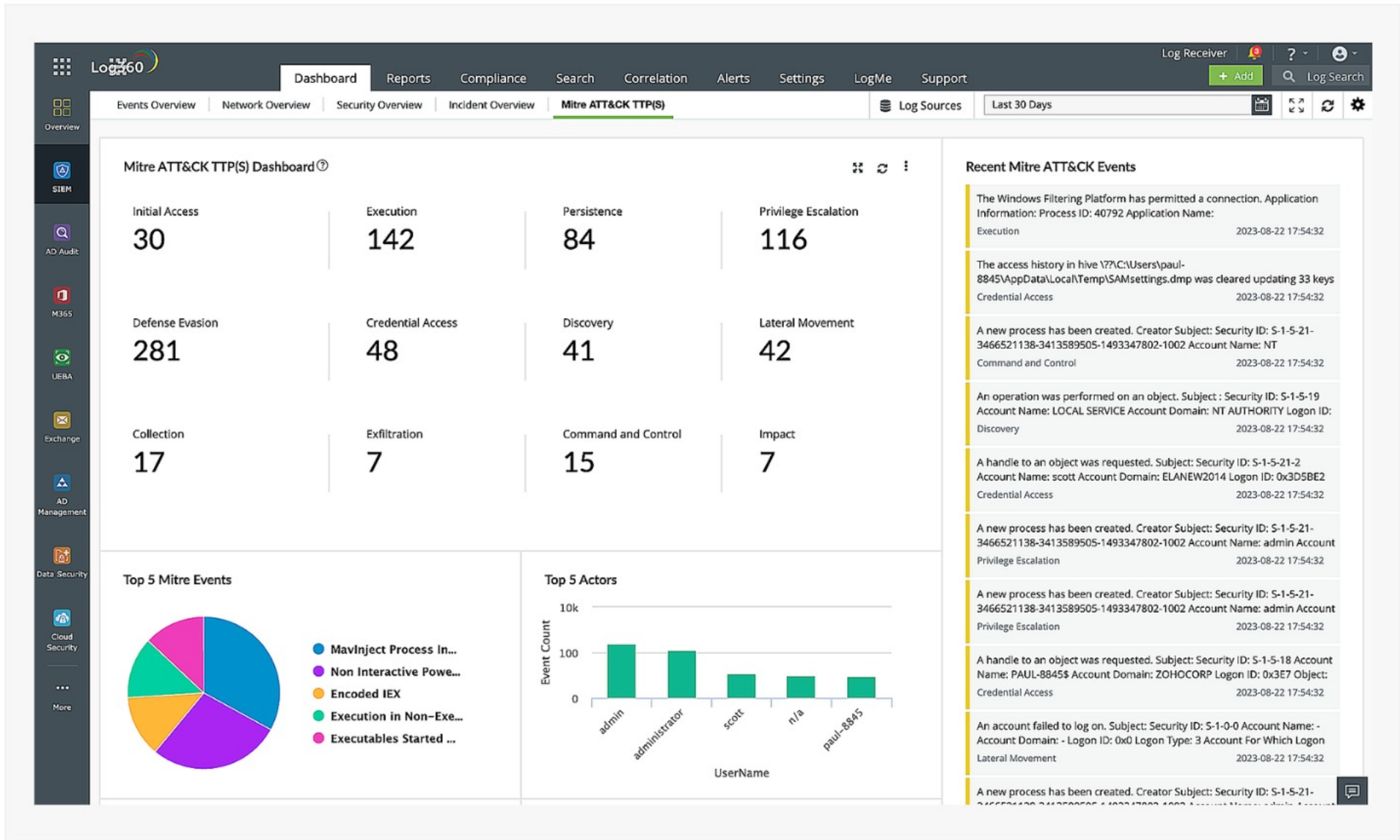
Modify Inputs

Save Profile Cancel

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



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



Log360 Dashboard | Anomaly Reports | Alerts | Settings | Support

Search... | Period: 2020-May-01 12:30:00 - 2020-Aug-01 12:30:00

359554 Number of Events Ingested | **72710** Anomalies Detected | **1688/1448** Tracking Users and Entities

Recent Alerts

[View All](#)

- ueba_user2 - Insider Threats**
2020-Jul-22 00:05:51
- ueba_user1 - Insider Threats**
2020-Jul-22 00:05:51
- ueba_user2 - User : 192.168.6.1\ueba_user2, Obtained : 200 events, Threshold : 36 events**
2020-Jul-22 00:05:46
- 192.168.5.1 - Entity : 192.168.5.1, Obtained : 397 events, Threshold : 56 events**
2020-Jul-22 00:05:46
- 192.168.5.1 - Entity : 192.168.5.1, Obtained : 396 events, Threshold : 55 events**
2020-Jul-22 00:05:45
- ueba_user2 - User : 192.168.6.1\ueba_user2, Obtained : 200 events, Threshold : 36 events**
2020-Jul-22 00:05:45
- ueba_user2 - User : 192.168.6.1\ueba_user2,**

Recent Anomalies

- 4** Multiple Services Installed On ...
Entity: 192.168.22.1
Obtained: 250 events
Threshold: 6 events
100
- Windows - New Service Installed

Anomaly Trends

Month	Anomaly Count
Apr 2020	~0
May 2020	~1.5k
Jun 2020	~2k
Jul 2020	~9k

Top 10 Anomalous Activities

- Windows Registry Activities
- Windows File Activities
- AD Logon
- Windows Application Whitelisting
- Windows USB Activities
- Windows System Activities
- User Activities
- S3 Bucket Activity Reports
- IAM Activity
- Windows Logon

Anomalies Based on Categories

Category	Anomaly Count
Windows	9020
Active Di...	1740
AWS	1351
Google	2
Azure	31

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

EventLog Analyzer Personalized Demo Log Receiver

Home Reports Compliance Search Correlation Alerts Settings LogMe Support

Search | How to search? + Add

Search: Pick Log Source:

Basic | Advanced

Parent Process Name = "svchost.exe"

Count

23 00 01 02 03 04 05

How to extract fields?

Message: -

Time: 2020-04-26 12:21:03 Event ID: 192.168.1.23 Process Id: 0x2e0e4 User: [redacted]
Parent Process Id: 0x268 Parent Process Path: C:\Windows\System32\ Account Name: [redacted]

Incident Workbench + Add to Incident Export As [-] [X]

User Syed x Process ID: 0x2e0e4 x Device syed x User Jaga x User Hemaachandar x

User Risk Analysis | User Activity Overview | User Details

Period:

Risk Score

1M
100K
10k
0

09-01 09-02 09-03 09-04 09-05 09-06 09-07

Risk Score Trend

Domain	Microsoft.com
Department	Finace
Current Risk Score	30
Peak Risk Score	31

Cards Based Peak Risk Score

Insider Threat	Last Update: 03/12/2018 08:30 PM	91
Data Ex-Filtration	Last Update: 03/12/2018 08:30 PM	12
Data Ex-Filtration	Last Update: 03/12/2018 08:30 PM	65



Incident response and management



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





Log360 Dashboard | Reports | Compliance | Search | Correlation | Alerts | Settings | LogMe | Support

Download | Personalized Demo | Log Receiver | ? | Add | Log Search

Alerts Incident | Export as | Add Alert Profile

Select view: Active alerts | 2018-05-21 00:00:00 - 2022-05-21 23:59:59

Critical Alerts 35 | Trouble Alerts 0 | Attention Alerts 2 | All Alerts 37

Failed Logons - Test Profile2

Time Generated	Alert Fo
2019-06-21 14:14:39	-:2
2019-06-21 14:14:05	-:2
2019-06-21 13:13:59	-:2
2019-06-21 12:58:23	-:2
2019-06-21 12:58:23	-:2
2019-06-21 12:55:06	-:2
2019-06-21 12:55:06	-:2
2019-03-01 03:03:45	-:2
2019-03-01 03:03:45	-:2
2019-03-01 03:03:45	-:2

Alert Format Message

Aaa: %AAA-4-LOGIN_FAILED : user admin failed to login (from:) [service: login] [reason: Authentication failed - Bad secret]

Time : 2019-03-01 03:03:45

Device: 192.161.23.41 | Severity: Critical | Status: Open

Notification Status: Failed | testmail@zoho.com

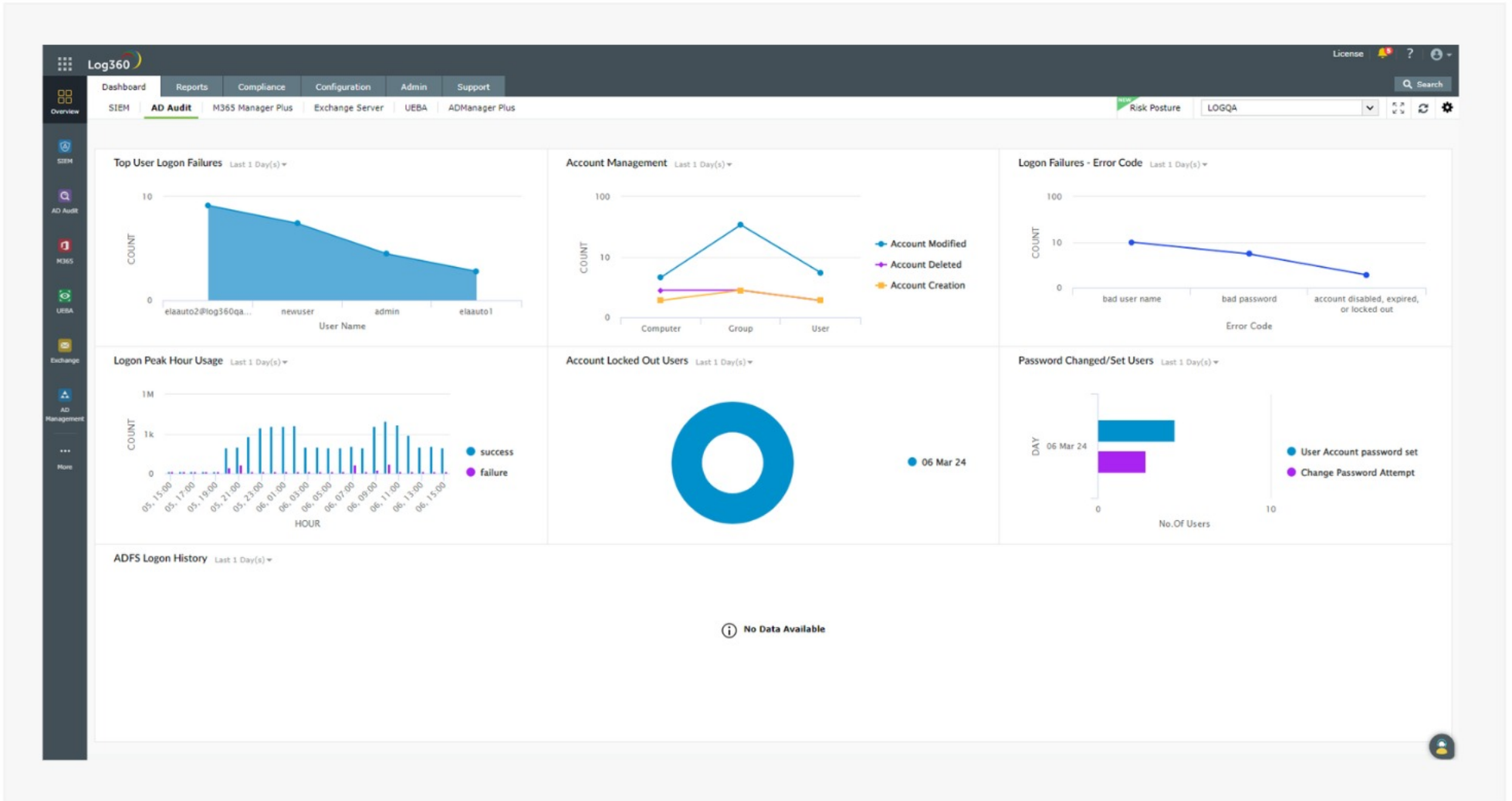
Workflow Status: Run Workflow

Active Directory (AD) auditing and reporting



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

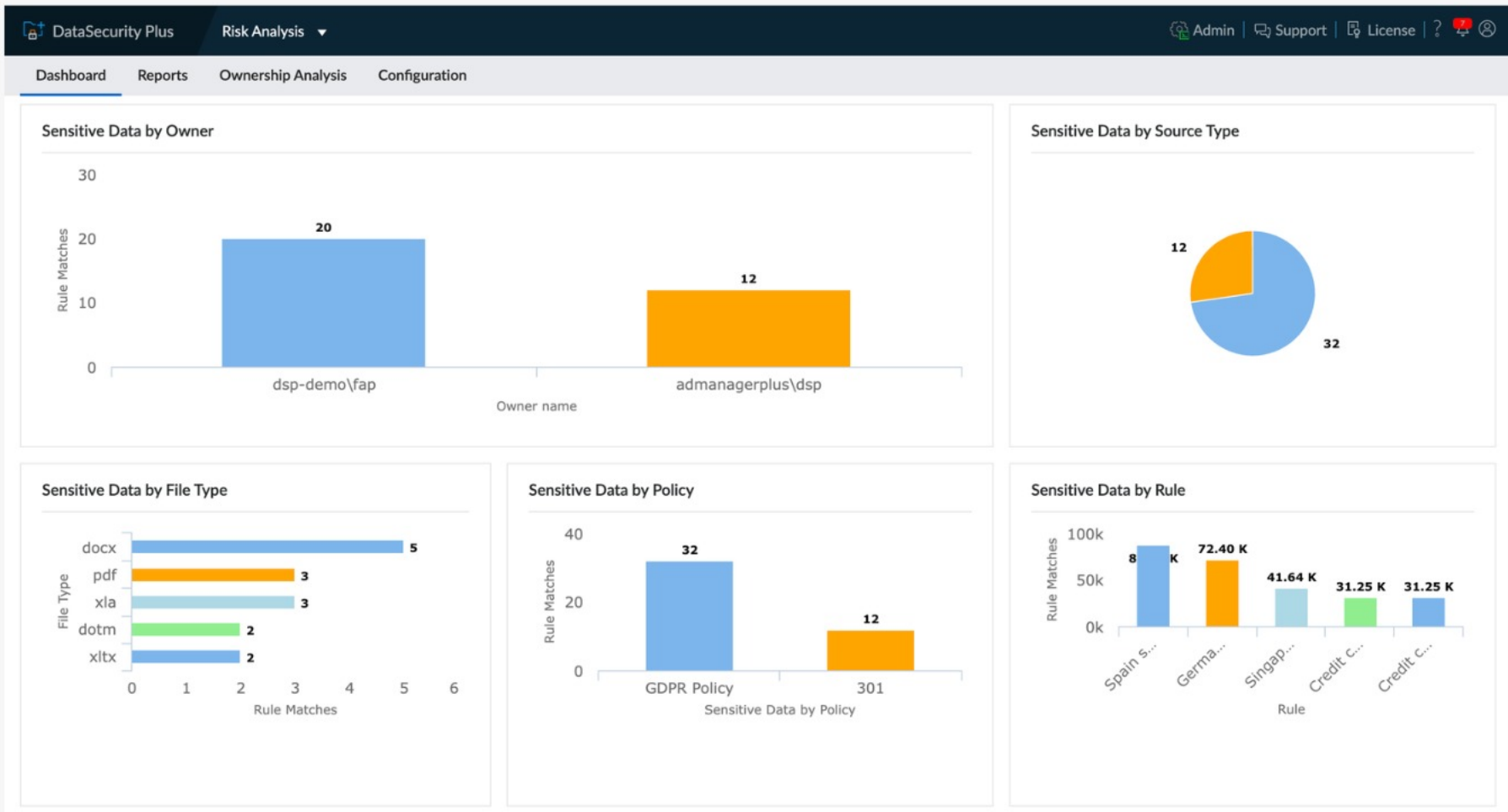


Data security monitoring



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

Thank you!

Contact

log360-support@manageengine.com

