ManageEngine
Log360

A comprehensive SIEM solution for your network.

ManageEngine

Log360

Why **Log360** is a complete **SIEM** solution

Security analytics

Spots network intrusions and threats by analyzing events from network devices, servers, databases, web servers, Office 365 platforms, Exchange servers, and AD.

Intuitive dashboards and pre-built reports help you detect and respond to anomalies instantly.

Threat intelligence

Detects attacks at their early stages with its built-in global IP threat database and STIX/TAXII threat feed processor that identifies malicious entities interacting with your network.

The real-time alerting system is tied together with the incident management system allowing you to quickly detect security incidents and resolve them.

User behavior analytics (UBA)

Spots anomalies without manual intervention using sophisticated machine learning techniques.

Detect unusual volume of logons, file activity, lockouts, and more with the intuitive dashboard and exhaustive reports.

Data security

Automatically discovers personal and sensitive data in Windows infrastructure with predefined confidential data detection policies. Protect these data with the extensive file integrity monitoring capability.

Monitors file and folder creation, deletion, modification, and permission changes in Windows, NetApp, EMC file servers, and more.

Incident management

Includes built-in incident tracking system which allows you to automatically assign owners to security alerts, track the incident resolution process, and more.

Integrates with JIRA, ServiceNow, ServiceDesk Plus, Zendesk and other help desk tools for streamlined incident tracking and resolution.

Cloud monitoring

Detects anomalous events by monitoring activities happening in PaaS and IaaS environments such as Azure, Amazon Web Services, and SaaS applications like Salesforce.

Spots activities such as unauthorized download of customer information from Salesforce with predefined reports and alerts.

Integrated compliance management

Stay compliant with PCI DSS, GDPR, FISMA, HIPAA, SOX, GLBA with audit-ready report templates. Exclusive dashboard to view the compliance state of your network.

Lets you tweak existing report templates to meet internal security policies and also allows you to build your own compliance reports easily with reusable components.

Security analytics

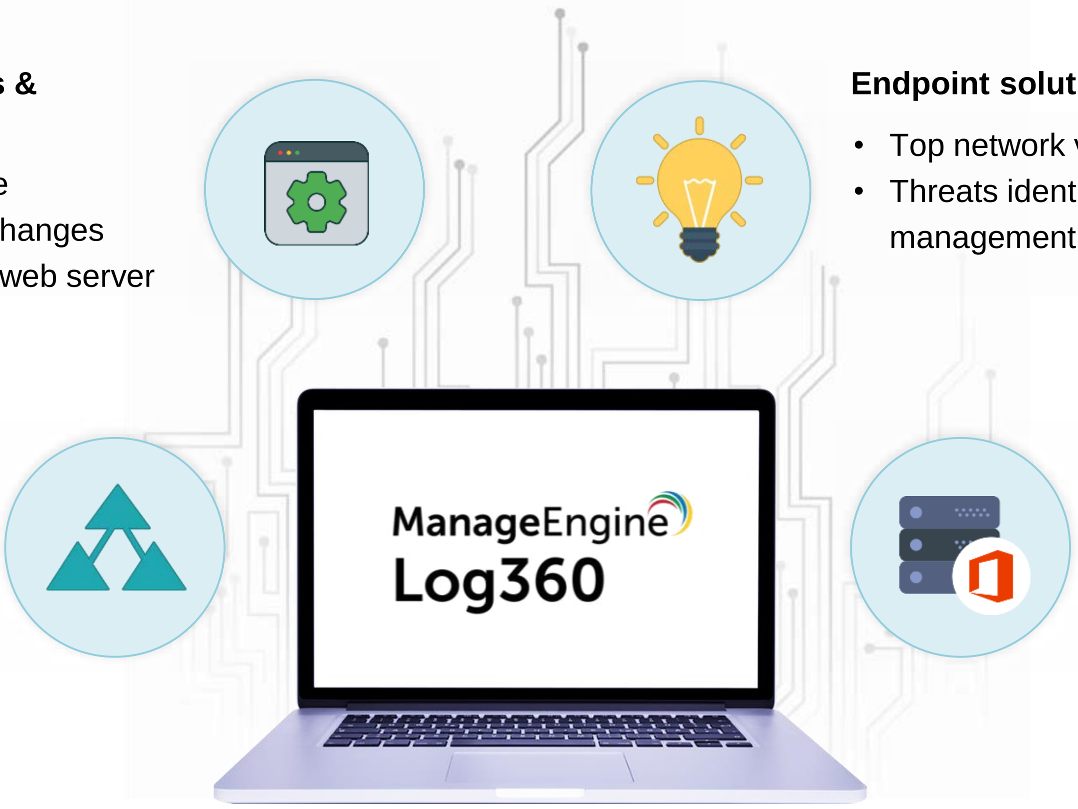
Central console for information

Network devices & application

- Security device configuration changes
- Database and web server activity

Endpoint solutions

- Top network vulnerabilities
- Threats identified by threat management solutions



Active Directory

- Privileged user activity
- Critical AD changes

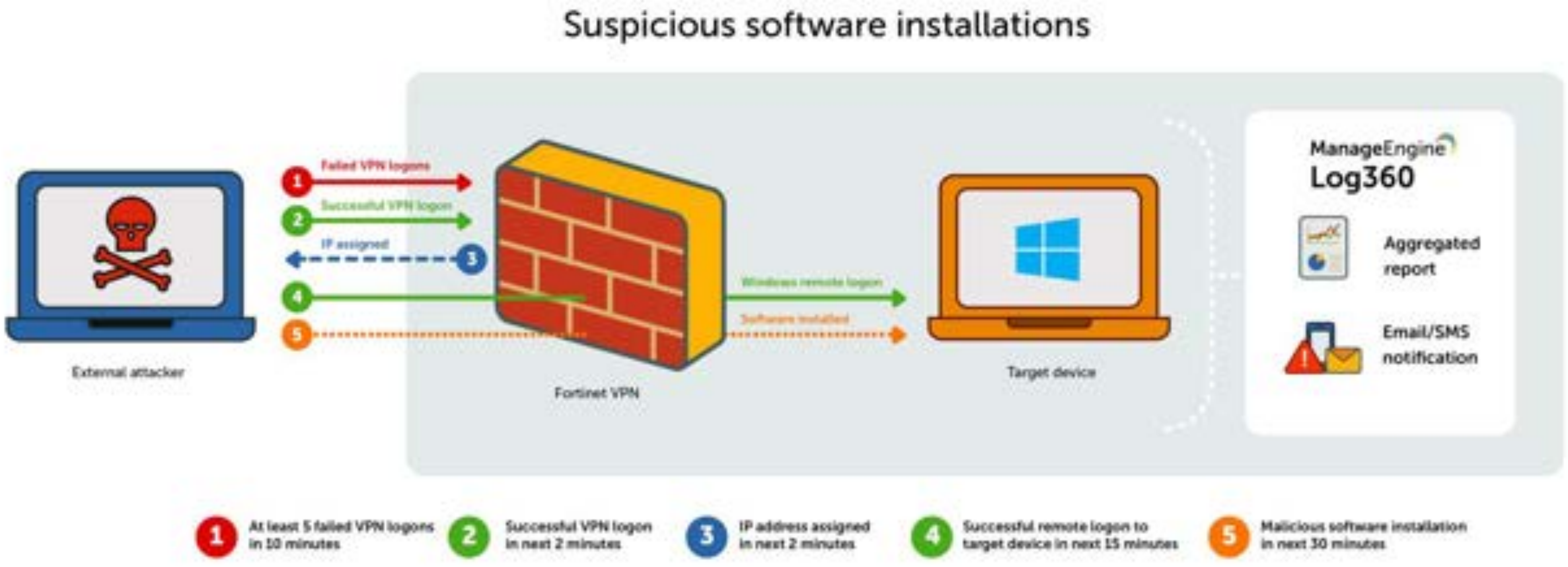
Office 365 & Exchange Server

- Mailbox traffic analysis
- Content, permission, traffic statistics for Exchange Server

Advanced event correlation

- Pattern-based incident detection
- **Over 30 predefined rules:** Detect suspicious software, cryptojacking, worm activity, and more
- Incident overview dashboard
- Detailed incident timelines
- Custom correlation rule builder with advanced field-based filters

Detecting suspicious software installations



Suspicious software installations

1 At least 5 failed VPN logons in 10 minutes

2 Successful VPN logon in next 2 minutes

3 IP address assigned in next 2 minutes

4 Successful remote logon to target device in next 15 minutes

5 Malicious software installation in next 30 minutes

Log forensics

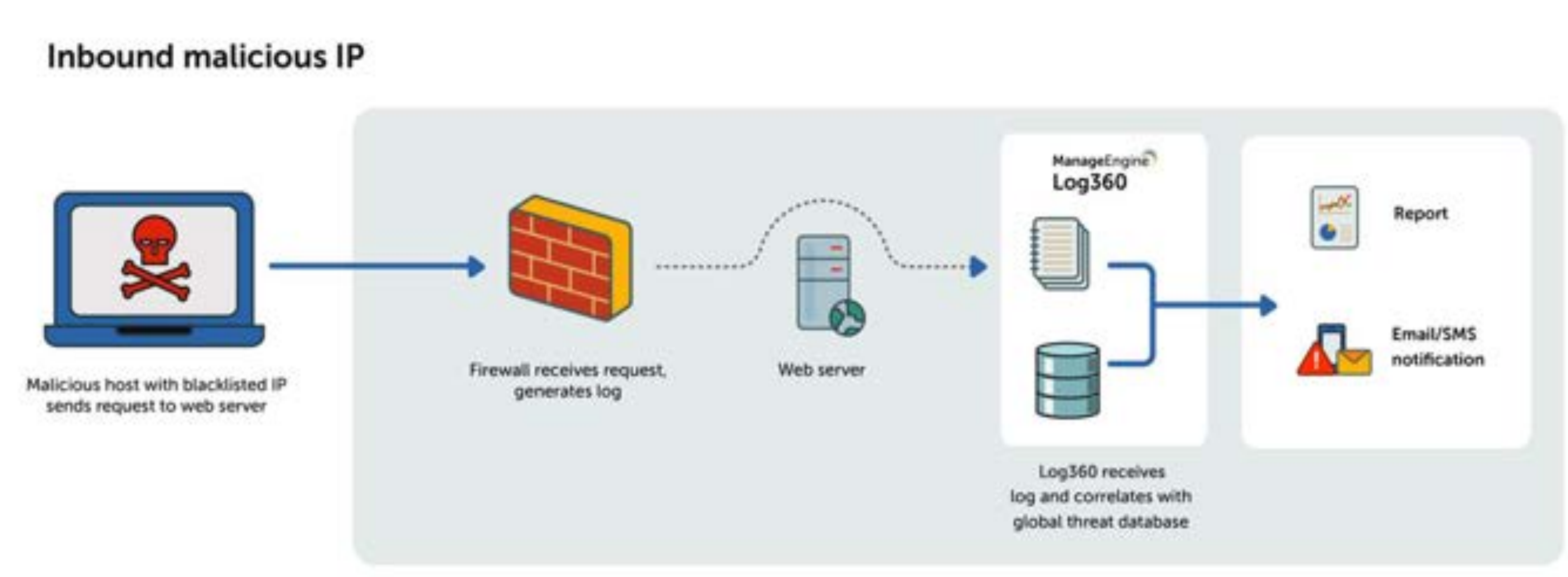
- Powerful Elasticsearch based search engine helps you analyze complex incidents and discover the root cause in minutes
- **Basic and advanced search:** Use flexible options to build search queries from scratch or use the advanced query builder interface
- Search through raw and formatted logs, including log archives
- Save searches as reports or alerts

Threat intelligence

Threat intelligence

- Detect network intruders with threat feed data
- Real-time alerts for malicious URLs, IPs, and domain names
- Add custom STIX/TAXII threat feeds
- No configuration needed
- Dynamic and daily updates

Detecting suspicious software installations



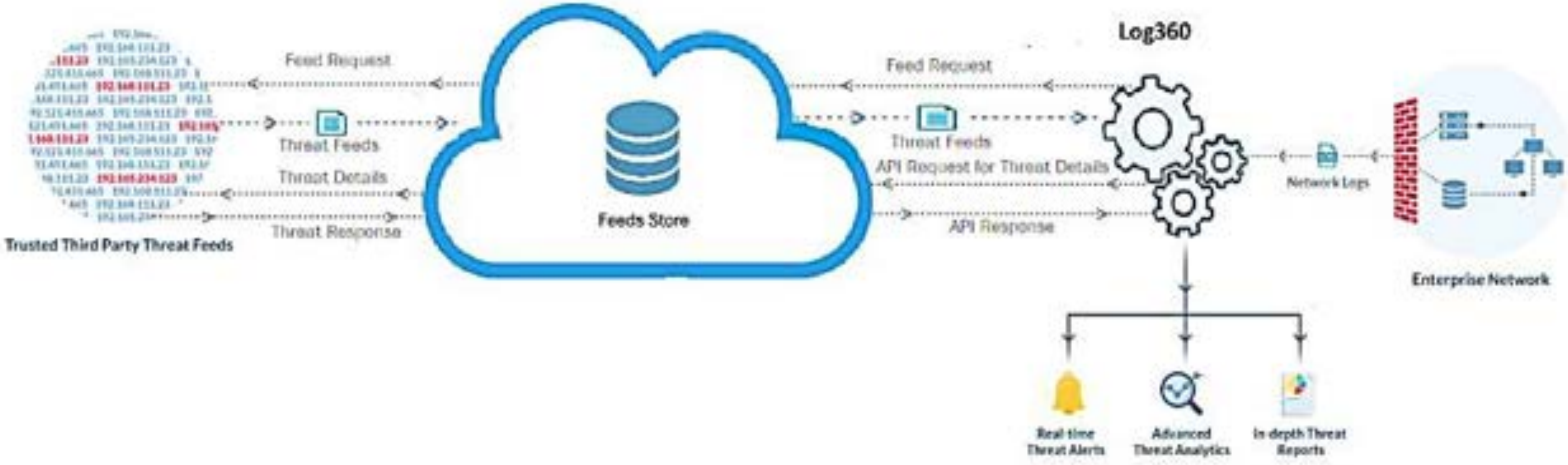
Inbound malicious IP
Malicious host with blacklisted IP sends request to web server
Firewall receives request, generates log
Web server
ManageEngine
Log360
Log360 receives log and correlates with global threat database
Report
Email/SMS notification

Advanced threat analytics

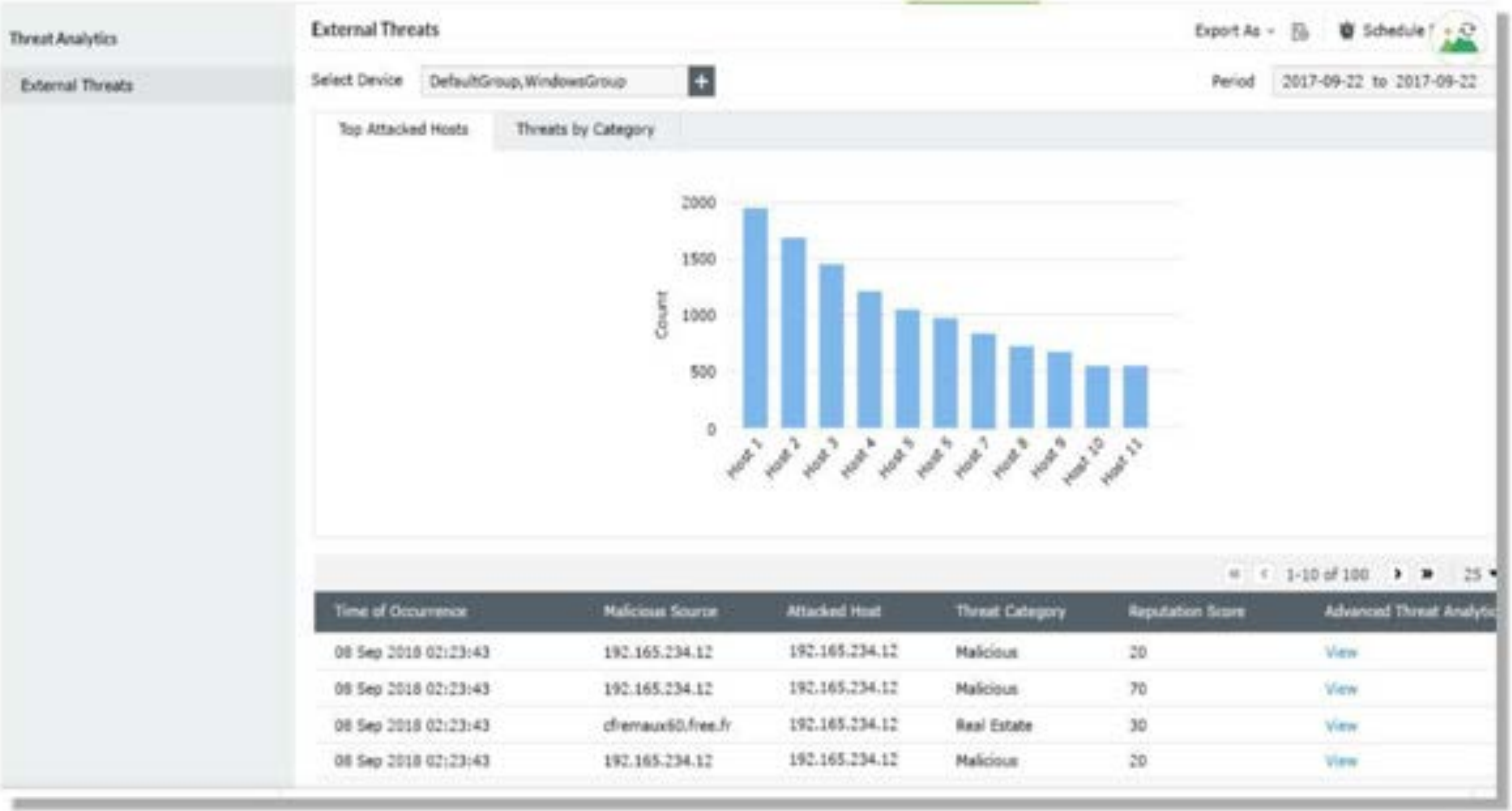
Advanced threat analytics

- Integration with trusted threat intelligence provider
- Deeper insights into the threat flagged
- IP/URL classification
- Reputation score

Integrated threat feeds

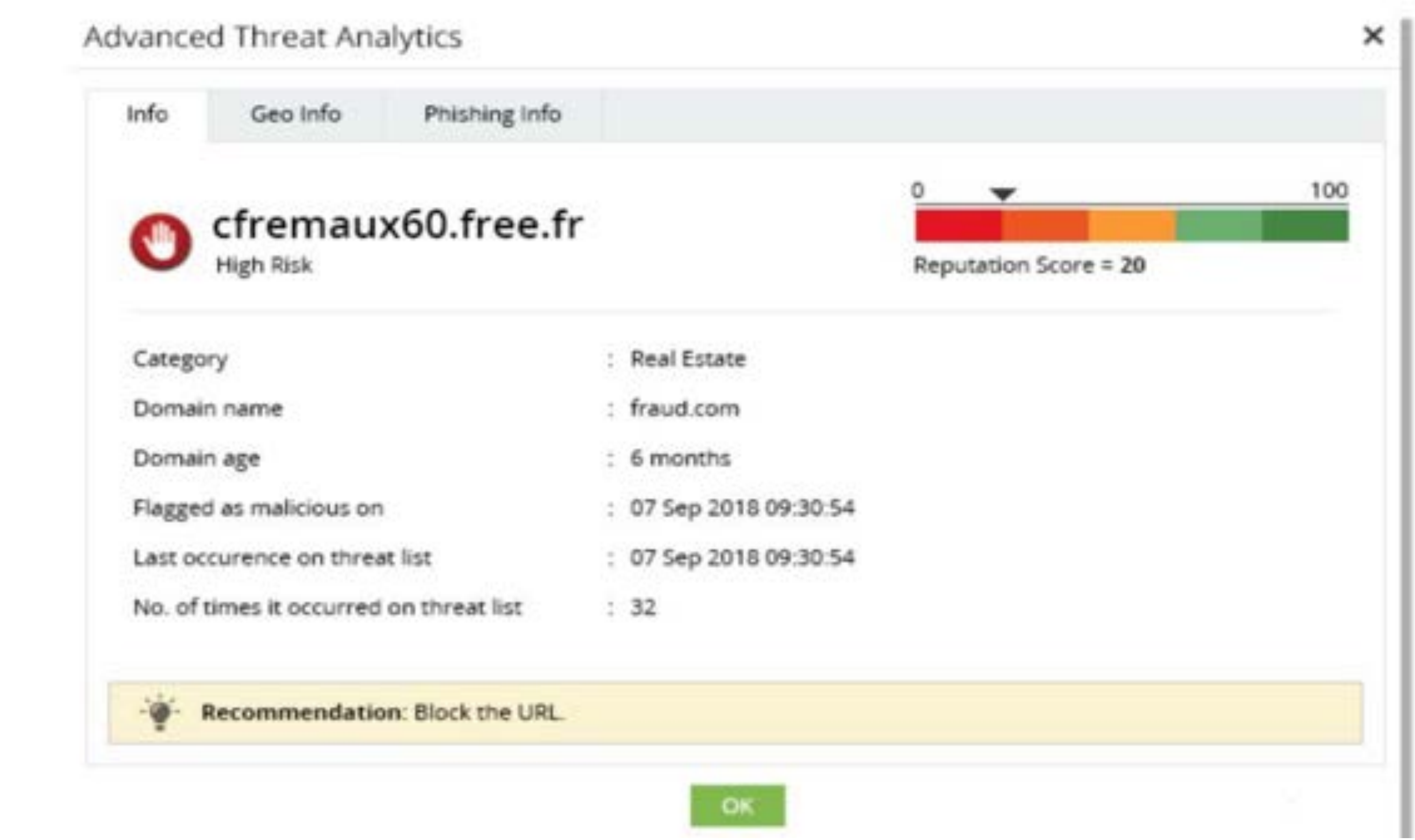


ManageEngine
Log360



External Threats

Time of Occurrence	Malicious Source	Attacked Host	Threat Category	Reputation Score	Advanced Threat Analytic
08 Sep 2018 02:23:43	192.165.234.12	192.165.234.12	Malicious	20	View
08 Sep 2018 02:23:43	192.165.234.12	192.165.234.12	Malicious	70	View
08 Sep 2018 02:23:43	cfremaux60.free.fr	192.165.234.12	Real Estate	30	View
08 Sep 2018 02:23:43	192.165.234.12	192.165.234.12	Malicious	20	View



cfremaux60.free.fr

High Risk

Reputation Score = 20

Category	: Real Estate
Domain name	: fraud.com
Domain age	: 6 months
Flagged as malicious on	: 07 Sep 2018 09:30:54
Last occurence on threat list	: 07 Sep 2018 09:30:54
No. of times it occurred on threat list	: 32

Recommendation: Block the URL.

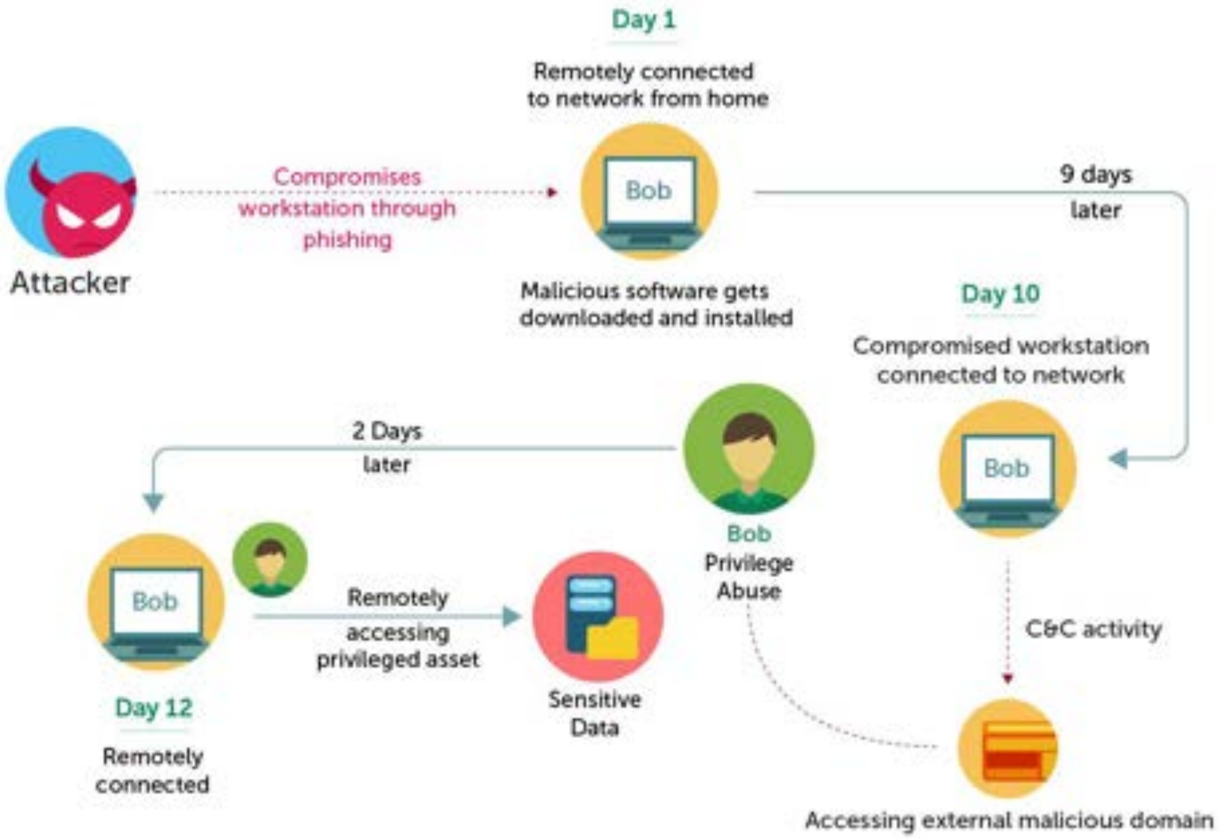
User and entity behavior analytics

User and entity behavior analytics

- Machine learning based anomaly detection
- **Anomalous behavior detection:** Based on time, pattern, or count
- **Risk score based threat prioritization:** Determine degree of risk posed by an identified threat
- Add high risk users and entities to a watchlist
- **Threat corroboration:** Identify indicators of common threats (account compromise, data exfiltration, and more)

Use case:

Compromised workstation & data exfiltration attempt


Attacker
Compromises workstation through phishing
Day 1
Remotely connected to network from home
Bob
Malicious software gets downloaded and installed
9 days later
Day 10
Compromised workstation connected to network
Bob
C&C activity
Accessing external malicious domain
Bob
Privilege Abuse
2 Days later
Bob
Day 12
Remotely connected
Remotely accessing privileged asset
Sensitive Data

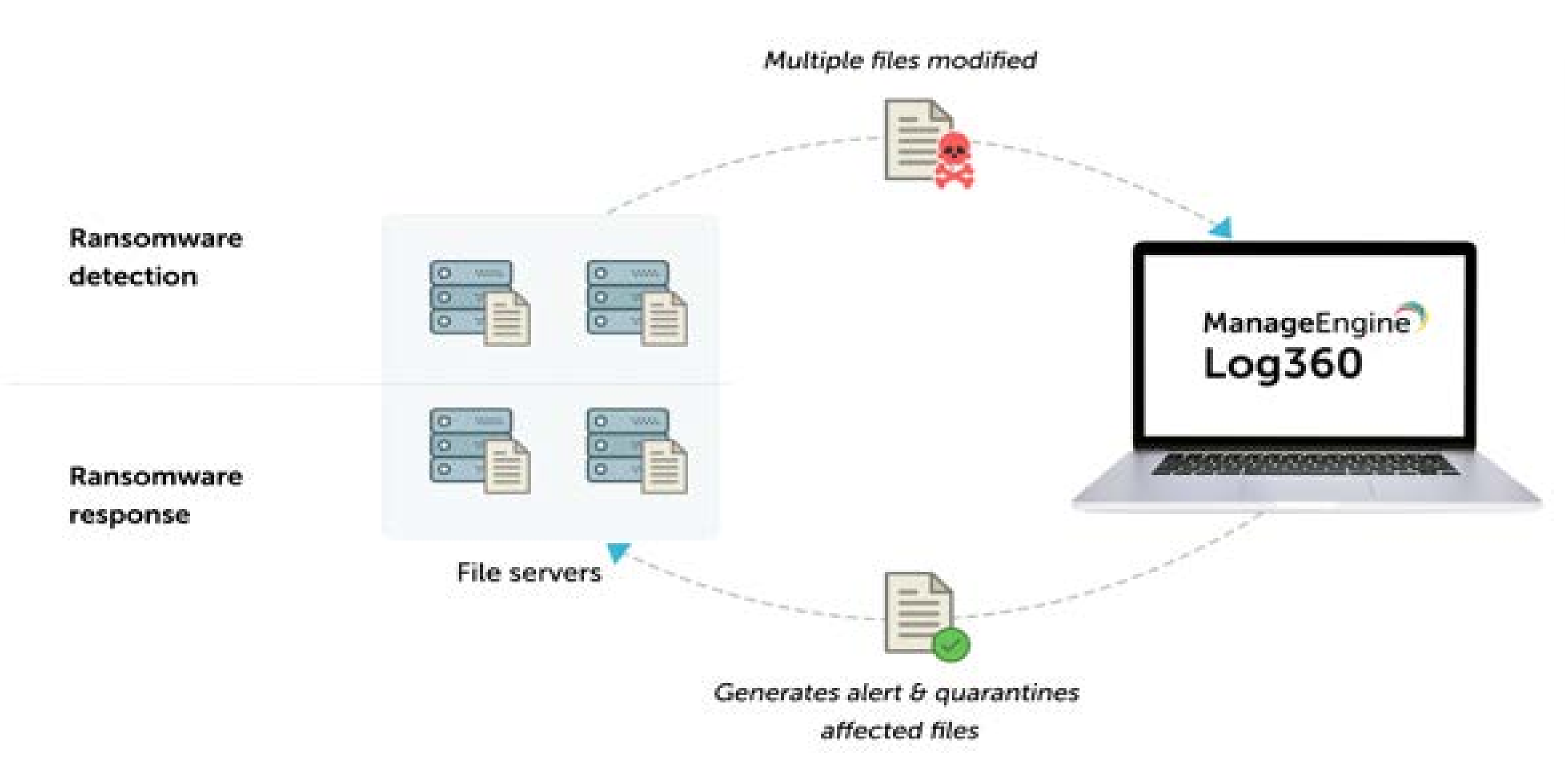
ManageEngine Log360

Data security

Data security

- 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.

Detecting suspicious software installations



ManageEngine Log360

Incident management

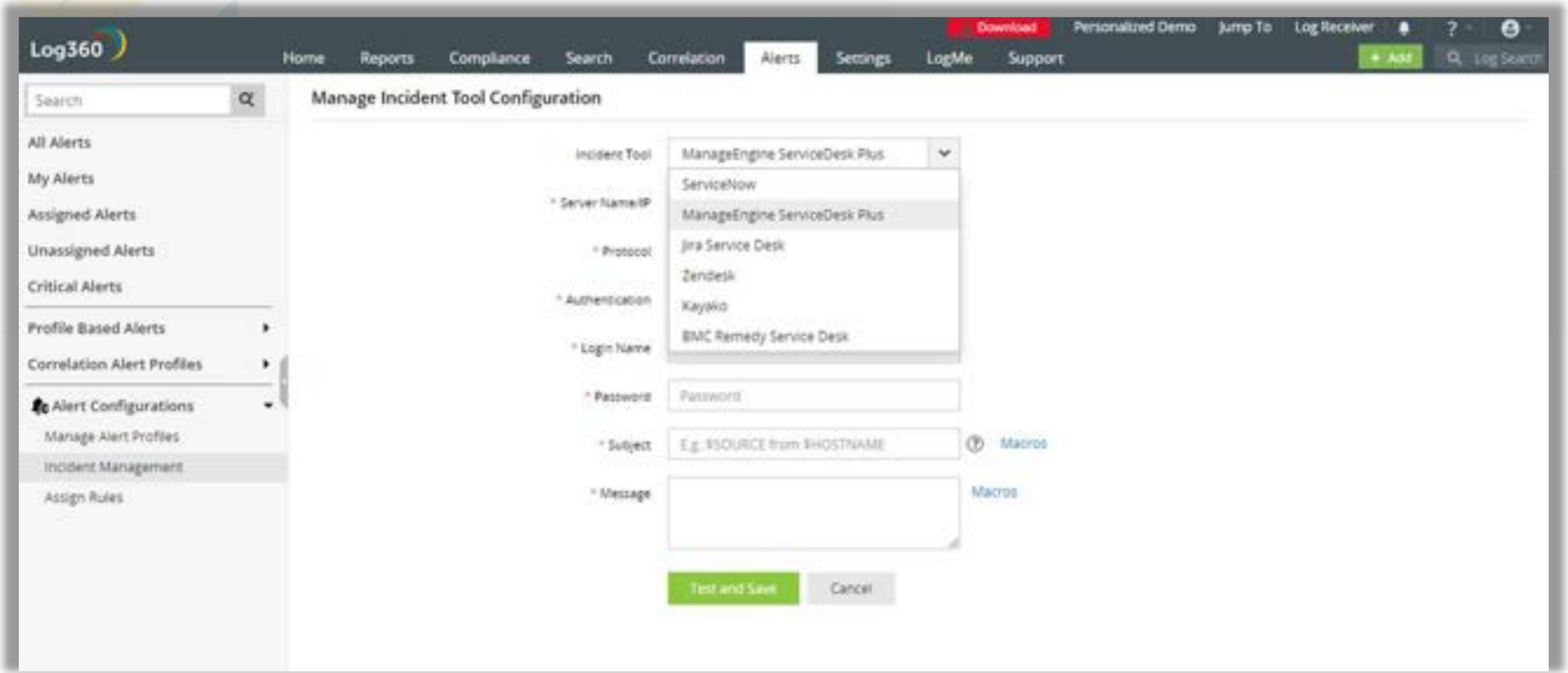
Incident management

Built-in ticketing system:

- Automatic incident ticket assignment
- Track incident status
- Maintain in-house knowledge base of resolved incidents

Forward incident information to external help desk software:

- Supported help desk software: ServiceDesk Plus, ServiceNow, Jira Service Desk, ZenDesk, BMC Remedy, Kayako



Manage Incident Tool Configuration

Incident Tool: ManageEngine ServiceDesk Plus

* Server Name/IP

* Protocol

* Authentication

* Login Name

* Password: Password

* Subject: E.g. $SOURCE from $HOSTNAME

* Message

Cloud monitoring

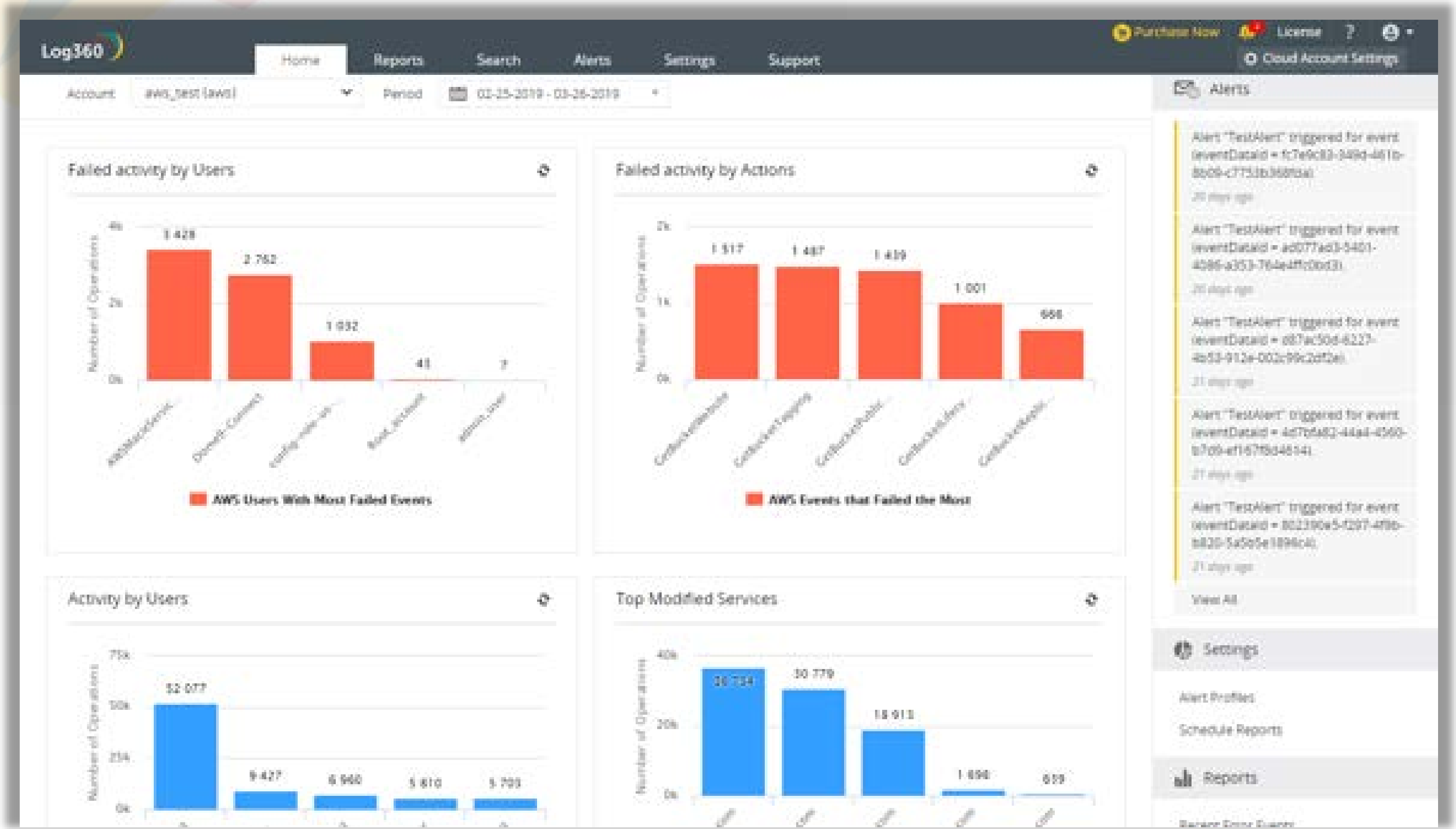
Cloud environments

Get information on:

AWS: Amazon S3, Amazon EC2, Web Application Firewalls (WAF), Relational Database Service (RDS), and more

Microsoft Azure: User activity, changes made to network security groups, virtual networks, DNS zones, databases, and more

Salesforce: Login, report, content, and search activities



Alert "TestAlert" triggered for event (eventDataId = fc7e9c83-349d-461b-8b09-c7753b368fba)
20 days ago

Alert "TestAlert" triggered for event (eventDataId = ad077ad3-5401-4086-a353-764e4ffc0bd3)
20 days ago

Alert "TestAlert" triggered for event (eventDataId = d87ac50d-6227-4b53-912e-002c99c2df2e)
21 days ago

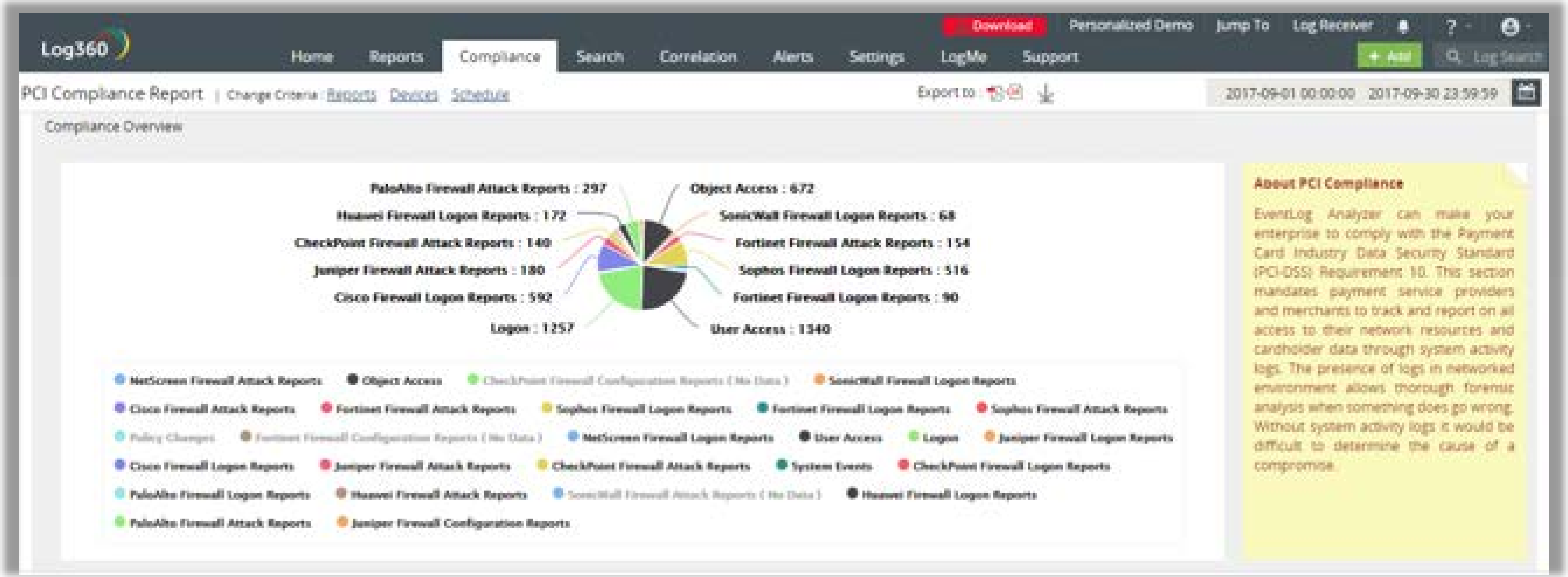
Alert "TestAlert" triggered for event (eventDataId = 4d7b6a82-44a4-4560-b7d9-ef167f8d4614)
21 days ago

Alert "TestAlert" triggered for event (eventDataId = 802390e5-f297-4f9b-b820-5a5e5e1896c4)
21 days ago

Regulatory compliance

Compliance

- **Out-of-the-box compliance reports for:** PCI DSS | SOX | GLBA | HIPAA | GPG | GDPR | ISO 27001 | ISLP
- Custom compliance report builder for new or in-house compliance policies
- Predefined compliance alerts available
- **Automatic log archival:** Retain logs for as long as required by regulatory requirements.
- Archives are secure and tamper-proof


Log360
Download
Personalized Demo
Jump To
Log Receiver
Home
Reports
Compliance
Search
Correlation
Alerts
Settings
LogMe
Support
+ Add
Log Search
PCI Compliance Report
Change Criteria : Reports
Devices
Schedule
Export to :
2017-09-01 00:00:00 2017-09-30 23:59:59
Compliance Overview
PaloAlto Firewall Attack Reports : 297
Huawei Firewall Logon Reports : 172
CheckPoint Firewall Attack Reports : 140
Juniper Firewall Attack Reports : 180
Cisco Firewall Logon Reports : 592
Logon : 1257
Object Access : 672
SonicWall Firewall Logon Reports : 68
Fortinet Firewall Attack Reports : 154
Sophos Firewall Logon Reports : 516
Fortinet Firewall Logon Reports : 90
User Access : 1340
● NetScreen Firewall Attack Reports
● Object Access
● CheckPoint Firewall Configuration Reports (No Data)
● SonicWall Firewall Logon Reports
● Cisco Firewall Attack Reports
● Fortinet Firewall Attack Reports
● Sophos Firewall Logon Reports
● Fortinet Firewall Logon Reports
● Sophos Firewall Attack Reports
● Policy Changes
● Fortinet Firewall Configuration Reports (No Data)
● NetScreen Firewall Logon Reports
● User Access
● Logon
● Juniper Firewall Logon Reports
● Cisco Firewall Logon Reports
● Juniper Firewall Attack Reports
● CheckPoint Firewall Attack Reports
● System Events
● CheckPoint Firewall Logon Reports
● PaloAlto Firewall Logon Reports
● Huawei Firewall Attack Reports
● SonicWall Firewall Attack Reports (No Data)
● Huawei Firewall Logon Reports
● PaloAlto Firewall Attack Reports
● Juniper Firewall Configuration Reports

About PCI Compliance

EventLog Analyzer can make your enterprise to comply with the Payment Card Industry Data Security Standard (PCI-DSS) Requirement 10. This section mandates payment service providers and merchants to track and report on all access to their network resources and cardholder data through system activity logs. The presence of logs in networked environment allows thorough forensic analysis when something does go wrong. Without system activity logs it would be difficult to determine the cause of a compromise.

Additional highlights

Additional features: Product security

- ✓ **Secure data transmission:** Encrypt all communication between Log360 and your browser through the secure HTTPS protocol.
- ✓ **Role-based access control:** Limit users' access to added devices and product features with user roles.
- ✓ **User auditing:** Audit all EventLog Analyzer user actions.
- ✓ **High availability:** Designate a secondary server to take over in event of the primary server failure.

Awards and recognitions

- ✓ Recognized in the Gartner Magic Quadrant for SIEM, for the fourth consecutive time.
- ✓ Gartner Peer Insights Customer Choice for SIEM, 2019.
- ✓ Placed as a leader in the Software Reviews Customer Experience Diamond for SIEM, 2019.

ManageEngine
Log360

Thank you!

Contact

log360-support@manageengine.com