loom
Systems

Cloud Migration with AIOps

Predict and Prevent IT Issues in Hybrid Cloud Environments with AIOps

Cloud Monitoring with Sophie AIOps

Loom's AIOps technology delivers a smooth integration and protects your emerging infrastructures from issues that affect the business. Sophie frees IT teams to focus on higher-level tasks by bridging the monitoring skill gap, mitigating the risk of a fragile infrastructure, and enabling your team to become proactive by predicting issues and producing insights

Increased Productivity

Sophie correlates all relevant events into one consolidated incident, reducing alert fatigue. Before an incident is created, it is measured against historical events, verifying that it is truly anomalous and not arising from seasonality.

Prevent P1 Incidents

By auto-detecting anomalies without the need to set any alerting rules or thresholds, Sophie empowers your IT team to become proactive about incidents that require their attention.

Built-in Insights & Recommendations

Sophie enriches incidents with corrective insights and resolutions written in plain English, reducing MTTR by 45%.

Stream any Data

On-premise, cloud or in a hybrid environment, Sophie's technology catches everything.

Azure Monitoring

Loom's advanced AIOps solution Sophie, monitors your disparate environment directly from Azure's Log Analytics tool or directly from your Azure cloud or applications. Sophie acts as an intelligence layer on top of your Azure Log Analytics, and provides resolutions and insights in plain English. Learn how Loom Systems augments Azure log analytics here.

Smooth Integration

Natively integrated with Microsoft Log Analytics API to allow seamless data ingestion. Streamline new data feeds in minutes. You can find Loom Systems on Azure Marketplace here.
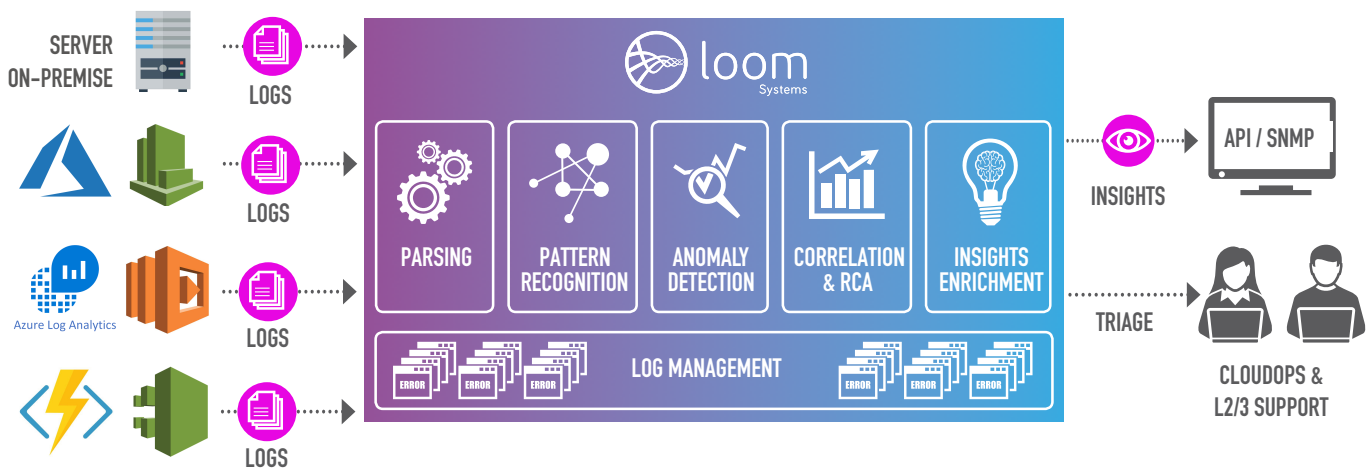
AWS Monitoring

Sophie enables AWS customers to gain immediate insight into the uptime, performance, and availability of their applications and systems through a quick diagnosis and resolving of applications and infrastructure issues before they impact customers.

AI-powered Problem Resolution

Sophie is able to pinpoint the underlying root cause of application problems –improving MTTR by up to 45% and notifies your IT team of problems across AWS infrastructure components including EC2, ELB, RDS, S3, and Availability Zones.
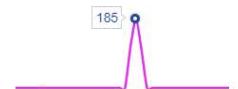
Improve AWS Security & Compliance

Monitor all user access, platform configurations, and changes across all AWS and on-premises workloads and generate audit trails to demonstrate compliance.

---

1   Application: Azure-OpsManage...   Service: **LsaSrv**   Time: Mar 11, 2018, 21:16   © 1 Insight ∧

Pattern Behavior ⓘ

The Security System could not establish a secured connection with the server LDAP/BDC-APDC700.ap.acme.com/ap.acme.com@AP.ACME.COM. No authentication protocol was available.

185

© Insights (1)

#1

This means that the login time will take longer!

It appears that VPN / SSL connection may hinder the Kerberos protocol from successfully authenticating to the domain controller / global catalog server.

© Actions |

Netlogon debug mode will help to find out the issue. To enable the Netlogon Debug Mode, create the following key on your client computer:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]

DBFlag=dword:2080ffff (hexadecimal value)

Then open a cmd and type net stop netlogon & net start netlogon to enable the debugging mode. The Debug logging writes to C:\Windows\Debug\netlogon.log In the netlogon.log, find that client on the remote location could not authenticate with Kerberos and try to fallback to NTLM. Since Windows 2008 R2 does not have NTLM enabled by default, the authentication consequently failed. Referring back to the VPN / SSL connection: Kerberos uses UDP and this is known to be unreliable through VPN tunnels. Therefore, we have to force the authentication to use TCP, using the following registry key on the client:
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters]
\"MaxPacketSize\"=dword:00000001

Among our Customers & Partners