Top 10 reasons HSM monitoring helps you avoid outages

Instant alerting

1. Eliminates need for repetitive manual checking

Alerts and status information are delivered automatically through a variety of interfaces avoiding the need to be in the physical presence of any HSM. Multiple options to receive information include the payShield Monitor web-based dashboard, SNMP, email accounts for authorized users and an external System Information and Event Management (SIEM) system using the payShield Monitor syslog data output.

2. Enables corrective actions to be taken proactively

There are three distinct user roles within payShield Monitor – Administrators who manage the system configuration including creating other users (specifically Group Managers and other Administrators), Group Managers who are responsible for managing specific HSMs individually and in groups and Auditors who view data and reports. The receipt of an instant alert by an Administrator or a Group Manager enables rapid action to be taken if for example faulty HSMs are discovered or there is a distinct possibility of a capacity overload or unauthorized changes have been made to any HSM.

3. Avoids information overload by filtering status data for specific operational roles

Any Administrator can see quickly at a high level if there is an alarm anywhere in the security domain associated with any HSM. A high level group report showing average utilization, transactions per second and the number of alarms active per type is available to Group Managers. Any Group Manager will only receive information and alerts for HSMs under his or her control. Email notification events are configurable at group level providing the ability to filter on information, notification, warning, error, critical, alert and emergency status.

Continuous tracking

4. Monitors HSM performance individually and in groups

Group performance over a user-selectable time period can be monitored – any device can be associated with multiple groups if necessary. There is the ability to quickly review statistics for all HSMs in any given group such as status, utilization, host tps and unacknowledged alarms. It is easy to retrieve the top 5 devices by utilization through the dashboard which is refreshed every 60 seconds.

5. Provides advance warning of capacity overload

Separate user-configurable thresholds for 'utilization overload' and 'utilization peak event' are available and controlled by warning level, critical level, peak level and peak duration parameters that are individually configurable for each group. Alarms can be switched on or off for each group independently. Exceeding a warning threshold generates a warning severity event whereas exceeding a critical threshold generates a critical severity event. Sampling occurs every 10 minutes and covers the activity over the previous 10 minutes.

6. Performs ongoing background monitoring of HSM health and significant events

Monitoring of each HSM is updated every 60 seconds on average – all HSMs defined on the system across all groups are covered. Health information includes the HSM operation state, alarm/tamper status, fraud detection analysis, overload status, network status and communication/management port information.

Comprehensive data

7. Provides bundled view of HSM configuration for analysis and comparison

The Group Manager can quickly view all the devices in any relevant group and click on any individual HSM to retrieve information including the device name, group association, serial number, IP address, detailed health check statistics and LMK information. It is easy to navigate from this display to the associated utilization graphs and host command graphs for both the HSMs and groups.

8. Supports generation of detailed reports on HSM utilization and performance

The performance graph on the dashboard provides a 'snapshot view' of the current utilization enabling Group Managers to pan backwards and forwards in time across all relevant groups. Clicking on the graph enables more detailed information to be viewed – printing or exporting in CSV format is supported for external processing and analysis. There is a very flexible time range supported for data filtering – last hour, last 24 hours, last 7 days, last 30 days or a user-definable date range.

9. Enables drill down for detailed analysis of performance, error or other significant data

The cryptographic performance of all HSMs both individually and as part of a group can be analysed for various different time periods – right down to individual commands. Device and group logs record information including tamper events and new HSM devices added to the payShield Monitor system – various options to filter data by date/time, severity and message content are supported. At all times issues such as active alarms, offline HSMs and overloaded HSMs are highlighted clearly enabling Group Managers to take corrective action where necessary.

10. Delivers insight of HSM utilization down to specific functions

There is a user-selectable time period to ensure both instant, short term and long term trends can be evaluated. All host commands active in the time period are presented together with their call frequency. This enables potential fraudulent events such as unexpected host command processing to be easily identified.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

> thalescpl.com <

Americas – Arboretum Plaza II, 9442 Capital of Texas Highway North, Suite 100 Austin, TX 78759 USA • Tel:+1 888 343 5773 or +1 512 257 3900 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com