

# SafePoint Alarms

Boost Security while  
Streamlining Administration



*The Payment Card Industry (PCI) Data Security Standard and security best practices now mandate that organizations gather and process security events in a single location, so administrators get adequate visibility into the organization's real-time security status.*

*However, while HPE NonStop security event information can be gleaned from Safeguard audit files, this approach is complex, and lacks the intelligence needed to efficiently manage alarms and event data. Now, with SafePoint Alarms, security teams can intelligently harness Safeguard audit information to get a comprehensive view of security events, and more quickly spot and address any potential threats.*

## Purpose

SafePoint Alarms provides security administrators with a sophisticated way to monitor all NonStop security events. With SafePoint Alarms, organizations can intelligently aggregate all Safeguard events, configure a range of alarms, and automate notifications and other responses to security threats. Non-Stop security events can be automatically offloaded to a Security Information and Event Management (SIEM) platform as well.

## Features

### Comprehensive security event monitoring.

With SafePoint Alarms, organizations can do real-time monitoring of all HPE NonStop security events that are logged to Safeguard audit trails – including Safeguard, OSS, audit clients, and Event Management System (EMS) events.

### Flexible alarm configuration.

With SafePoint Alarms, administrators can monitor audit trails for any events matching custom-configured alarm criteria. Alarms can be triggered based on very granular events – like a specific user accessing a specific file – or on more general events, such as any users logging on to a group of systems. Alarms can be triggered based on such common alarm events as logons to administrative accounts, security violations for production files, and changes to the Safeguard configuration.

### Alerts sent right to your inbox or smartphone

With SafePoint Alarms security events can trigger SMTP (email) alerts which will appear in real time in your email inbox or on your smartphone. This provides instant notification of security threats.

### Sophisticated alarm presentation and event analysis.

The SafePoint Alarms product includes an NSK Security Events Console that displays alarm events in real time, and color codes them so users can easily distinguish the relative severity of alarms. In addition, the product offers real-time porting of Safeguard audit data to a Security Information and Event Management (SIEM) system, facilitating robust analysis of event data.

### Broad integration with enterprise management infrastructures.

The SafePoint Alarms product sends messages via SYSLOG or SNMP to tier-two event collectors like HPE's ArcSight product. SafePoint Alarms can also generate enterprise management system (EMS) messages that can be viewed using HPE's ViewPoint product or by any other EMS-aware NSK console product. Finally, SafePoint Alarms generates SYSLOG alerts that can be viewed by a range of SIEM management products, including HPE OpenView and ArcSight.

### Automated alarm response.

SafePoint Alarms offers capabilities for specifying a range of actions that will be taken for each alarm event – including displaying the alarm on an administrative console, generating messages for EMS and SNMP systems, sending SYSLOG messages to SIEM systems, writing SQL records, logging to a disk file, and sending email alerts (email alerts are scheduled for a future release).

## Key Features

- Real-time alarm generation
- Comprehensive event aggregation
- Color-coded alarm displays
- EMS, SYSLOG, and SNMP management systems integration
- Flexible alarm configuration
- Automated alarm response
- SQL database integration
- Email alerts

## Benefits

### ■ Boost security

By enabling security organizations to fully leverage all event information in their HPE Non-Stop environments, SafePoint Alarms enables administrators to more effectively monitor their entire infrastructure, and more quickly identify and respond to potential threats.

### ■ Streamline security administration

By enabling broad integration of event information and enterprise event management consoles, and automation of alarm response mechanisms, SafePoint Alarms dramatically streamlines the effort required to do enterprise security administration.

### ■ Leverage infrastructure investments

SafePoint enables organizations to work with their existing security infrastructure, including SNMP and EMS systems, while more fully leveraging all Safeguard-related security information, whether generated by OSS, EMS, audit clients, or other sources.

### ■ Integration with SIEM

SafePoint Alarms can stream, audit data directly to an enterprise SIEM system, providing security officers and auditors with access to NonStop audit data.

# SafePoint Alarms

comforte 21 GmbH, Germany  
phone +49 (0) 611 93199-00  
sales@comforte.com

comforte, Inc., USA  
phone +1-303 256 6257  
ussales@comforte.com

comforte Asia Pte. Ltd., Singapore  
phone +65 6818 9725  
asiasales@comforte.com

comforte Pty Ltd, Australia  
phone +61 2 8197 0272  
aussales@comforte.com

[www.comforte.com](http://www.comforte.com)



For distribution partners in your region visit comForte's homepage [www.comforte.com](http://www.comforte.com)

System	#	Date/Time	Action	Target Object or User Name	By User	For User	IP Address	Objtype	Outcome	Event Terminal
NRBQ	001	21NOV2013 15:25:42.333	LOGON	SUPER.SUPER	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	003	21NOV2013 15:30:18.848	LOGON	SUPER.JAY	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	007	21NOV2013 15:30:44.582	OPEN FOR READ/WRITE	\$DATA02 BAKT00 MYFILE7	SUPER.JAY	SUPER.JAY	192.168.1.100	DISKFILE	DENIED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	007	21NOV2013 15:30:58.877	CREATE	\$AUDIT TEST BGRFILE	SUPER.JAY	SUPER.JAY	192.168.1.100	DISKFILE	DENIED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	002	21NOV2013 15:32:05.024	OPEN FOR EXECUTE	\$SYSTEM JUNKJUNKBJ	SUPER.JAY	SUPER.JAY	192.168.1.100	DISKFILE	DENIED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	007	21NOV2013 15:32:05.024	OPEN FOR EXECUTE	\$SYSTEM JUNKJUNKBJ	SUPER.JAY	SUPER.JAY	192.168.1.100	DISKFILE	DENIED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	008	21NOV2013 15:32:06.024	OPEN FOR EXECUTE	\$SYSTEM JUNKJUNKBJ	SUPER.JAY	SUPER.JAY	192.168.1.100	DISKFILE	DENIED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	006	21NOV2013 15:32:33.808	CREATE	BAKER.SAM	joel_sandberg	SUPER.SUPER	192.168.1.100	USER	GRANTED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	009	21NOV2013 15:32:57.808	ALTER DIR-DEVI	SAFEGUARD CONFIGURATION	joel_sandberg	SUPER.SUPER	192.168.1.100	SIG CONFIGURATI	GRANTED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	005	21NOV2013 15:34:22.144	PURGE	\$AUDIT TEST BGRFILE	joel_sandberg	SUPER.SUPER	192.168.1.100	DISKFILE	GRANTED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	001	21NOV2013 15:41:13.702	LOGON	SUPER.SUPER	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	004	21NOV2013 15:41:13.702	LOGON	SUPER.SUPER	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	004	21NOV2013 15:42:08.451	LOGON	hacker	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	002	21NOV2013 15:43:02.705	OPEN FOR EXECUTE	\$SYSTEM JUNKJUNKBJ	joel_sandberg	SUPER.SUPER	67.188.109.115	DISKFILE	GRANTED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	006	21NOV2013 15:43:02.705	OPEN FOR EXECUTE	\$SYSTEM JUNKJUNKBJ	joel_sandberg	SUPER.SUPER	67.188.109.115	DISKFILE	GRANTED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	003	21NOV2013 15:43:19.445	LOGON	BAKER.BAKER	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	009	21NOV2013 15:44:52.801	ALTER DIR-DEVI	SAFEGUARD CONFIGURATION	BAKER.BAKER	BAKER.BAKER	67.188.109.115	SIG CONFIGURATI	GRANTED	NRBQ.SZNDIC.#PTGHQVQ
NRBQ	001	21NOV2013 15:45:34.301	LOGON	SUPER.SUPER	SUPER.SUPER	SUPER.SUPER	192.168.1.100	USER	PASSED	NRBQ.SZNDIC.#PTGHQVQ

SafePoint Alarms NonStop Security Event Console