



ENTRUST



nShield Monitor

Konsolidierte Überwachung verteilter HSM

HIGHLIGHTS

- Rund-um-die-Uhr-Überwachung aller nShield-Hardware-Sicherheitsmodule (HSM)
- Erkennt Leistungsengpässe für eine verbesserte Kapazitätsplanung
- Ermöglicht dank umfangreicher Alarmmeldungen eine unmittelbare Reaktion auf potenzielle Probleme
- Kein physischer Zugriff auf HSM erforderlich, um wichtige Daten abrufen zu können
- Kann nahtlos in bestehende HSM-Hardware- und Softwarekonfigurationen integriert werden

nShield Monitor ist eine umfassende HSM-Überwachungsplattform, mit der Betriebsteams rund um die Uhr Einblick in den Status aller ihrer nShield HSM erhalten, einschließlich derer, die sich in verteilten Rechenzentren befinden. Mit dieser Lösung können Sicherheitsteams HSM effizient inspizieren und sofort herausfinden, ob potenzielle Sicherheits-, Konfigurations- oder Nutzungsprobleme ihre unternehmenskritische Infrastruktur beeinträchtigen können.

Zentrale Überwachungsfunktionen

- Aktualisiert die Nutzungsstatistiken aller HSM auf Minutenbasis
- Gibt basierend auf benutzerdefinierten Schwellenwerten eine Reihe von Warnungen aus
- Sendet auf der Grundlage von unabhängigen benutzerdefinierten Schwellenwerten in kritischen Situationen Alarmmeldungen
- Ermöglicht dem Benutzer, die Zeiträume für eine detaillierte Analyse (letzte Stunde, 24 Stunden, 7 Tage, 30 Tage oder benutzerdefiniert) festzulegen
- Sendet Warnungen und Alarmmeldungen per E-Mail, SNMP und Remote Syslog Server

HSM-Kompatibilität

- nShield Edge, Solo+, Solo XC, Connect+ und Connect XC mit Security World Software v12.40 und höher





nShield Monitor

Rollenbasierte Zugriffssteuerung

- Unterstützt drei verschiedene Rollen: Administrator, Group Manager und Auditor
- Teilt jeder einzelnen Rolle eine Reihe von separaten Aufgaben zu, wobei die Verantwortlichkeiten deutlich getrennt sind
- Verbessert die Sicherheit in Bezug auf die Konfiguration und Verwaltung allgemeiner nShield-Monitor-Systeme
- Verwaltung der Bereitstellung durch den Administrator
- Steuerung der Überwachung der HSM durch den Group Manager
- Prüfung der Daten und Berichte durch den Auditor

Lösungskomponenten

- nShield Monitor wird im Open-Virtual-Appliance-Format (OVA-Format) und im Microsoft Hyper-V-Format bereitgestellt.
- Webbasierte Verwaltungsoberfläche und Command Line Interface (CLI).
- Die Browser Firefox, Internet Explorer und Chrome werden unterstützt.
- Ein flexibler Mechanismus zur Endpunkt-Lizenzierung unterstützt bis zu 500 HSM.

Mindestanforderungen für Virtual Appliances

- 2 CPUs mit jeweils 2 Kernen
- 8 GB RAM
- Thin-Provisioned-Festplatten
- Hypervisor-Kompatibilität

- Die OVA kann auf den folgenden virtuellen Plattformen installiert werden:
 - vSphere ESXi 6.0, ESXi 6.5
 - VMware Workstation 12, 14
 - VMware Fusion 10
 - Oracle VirtualBox 6.0
- Hyper-V Image kann auf den folgenden virtuellen Plattformen installiert werden:
 - Microsoft Hyper-V, Azure

Sicherheit

- Verwaltung von Webserver-Zertifikaten, die beim Sitzungsaufbau Client-Browser für nShield-Monitor-Authentifizierung bereitstellt
- Sichere Aufteilung von Rollen und Aufgaben von Administratoren und Group Managern
- Starke Passwortrichtlinien: Kontrolle des Ablaufdatums und der Dauer der automatischen Anmeldung
- Auswahl der Algorithmen für Authentifizierung und Datenschutz
- Nutzt SNMP v3 für die Verbindung zwischen nShield Monitor und dem HSM

Weitere Informationen

Mehr Informationen zu den nShield HSMs von Entrust finden Sie auf [entrust.com/HSM](https://www.entrust.com/HSM). Auf [entrust.com](https://www.entrust.com) erfahren Sie zudem mehr über die digitalen Sicherheitslösungen für Identitäten, Zugriff, Kommunikation und Daten von Entrust.



Weitere Informationen auf
[entrust.com/HSM](https://www.entrust.com/HSM)

