

# Die RSA enVision™-Plattform auf einen Blick

## 3-in-1-Lösung für das Log-Management

### Was ist RSA enVision?

Führende Analysten, darunter auch Gartner, stimmen überein, dass die RSA enVision™-Plattform die marktführende Lösung für das Management von Sicherheitsinformationen und -ereignissen (Security Information and Event Management, SIEM) ist. Unternehmen bekommen eine integrierte 3-in-1-Lösung für die Protokollverwaltung an die Hand, die Compliance vereinfacht, die Sicherheit verbessert und Risiken minimiert. Gleichzeitig wird der Betrieb von IT und Netzwerk durch die Automatisierung von Erfassung, Analyse, Benachrichtigung, Auditing, Berichtswesen und die sichere Speicherung aller Log-Protokolle optimiert.

### Was bietet RSA enVision?

Die RSA enVision-Plattform erfasst alle Log-Protokolle, die von IP-Endgeräten innerhalb Ihres Netzwerks generiert werden, archiviert laufend Kopien von Daten, verarbeitet die Protokolle in Echtzeit und schlägt Alarm, wenn verdächtige Verhaltensmuster erkannt werden. Administratoren können den gesamten gespeicherten Datenbestand über eine intuitive Benutzeroberfläche abfragen. Eine ausgereifte Analysesoftware wandelt komplexe und unstrukturierte Rohdaten in strukturierte, übersichtliche Informationen um und ermöglicht Administratoren wertvolle Einblicke, um sie in drei wesentlichen Bereichen zu unterstützen:

**Vereinfachung der Compliance.** Administratoren können automatisch Protokoll Daten zu Netzwerk, Datei, Anwendung und Anwenderaktivität erfassen. Diese Daten vereinfachen den Compliance-Prozess erheblich. Mehr als 1.100 im Lieferumfang enthaltene Berichte sind speziell auf die aktuellen Compliance-Anforderungen zugeschnitten. Darüber hinaus vereinfacht die Lösung auch die Einhaltung künftiger Rechtsprechung, da alle Protokoll Daten ohne Informationsverlust gespeichert und vor Manipulation geschützt werden. So entsteht eine nachweisbar authentische Datenarchivquelle.

**Verbesserte Sicherheit und Risikominderung.** Durch Echtzeitalarme bei Sicherheitsverletzungen sowie die Überwachung und Drilldown-Funktionen für die Forensik gibt die Plattform Administratoren einen deutlichen Überblick über wichtige Informationen. Sie können Bedrohungen und Risiken schnell erkennen und so effektiv zur Minderung dieser Risiken beitragen.

**Optimierung von IT- und Netzwerkbetrieb.** Verwaltete Log-Protokolle sind die beste Informationsquelle über die Performance der Infrastruktur. IT-Verantwortliche können die RSA enVision-Plattform nutzen, um Aktivitätsprotokolle für Server, Netzwerkgeräte und Speicherplattformen nachzuverfolgen und zu verwalten. Des Weiteren lassen sich Netzwerkressourcen, Hardware und Geschäftsanwendungen überwachen. Die Lösung bietet ein intelligentes Forensik-Tool zur Behebung von Infrastrukturproblemen und zum Schutz von Infrastrukturressourcen und unterstützt IT-Manager bei Helpdesk-Aufgaben.

### Wie funktioniert RSA enVision?

Die RSA enVision-Plattform ist in der Lage, gleichzeitig die Protokoll Daten von Zehntausenden Geräten (wie z.B. Windows® Server, Check Point®-Firewalls und Cisco®-Router) zu sammeln, ohne dass clientseitige Softwareagents installiert werden müssen. So ist sichergestellt, dass alle Daten - All the Data™ - kontinuierlich erfasst werden. Die RSA enVision-Funktionen für das Erstellen von Baselines, Trendanalysen und Berichten erlaubt IT- und Netzwerkadministratoren einen grafischen Langzeitüberblick über Performance und Sicherheitsereignisse und verbessert so die Planungseffizienz, während die Arbeitslast reduziert wird. Die Plattform kann als Standalone-Modell, Plug-and-Play-Lösung oder als Teil einer skalierbaren, hochverfügbaren verteilten Architektur bereitgestellt werden, um auch den Anforderungen großer Unternehmensnetzwerke gerecht zu werden. Die benötigte Software wird bei allen Optionen ohne Zusatzkosten zur Verfügung gestellt.

Web-basierte Verwaltung und RSA enVision Event Explorer™-Technologie - ein äußerst intelligentes Analysetool - ermöglichen intuitive Bedienung und eine optimierte, detaillierte und genaue forensische Analyse. Bei der Standalone-Variante (ES-Serie) übernimmt ein eigenständiges, sicherheitsgehärtetes Gerät alle Aufgaben, inklusive Zusammenstellung, Verwaltung, Analyse und Speicherung von Daten. Die verteilte Architektur (LS-Serie) nutzt mehrere dedizierte Geräte, die bedarfsorientiert eingesetzt werden und jeweils Schlüsselrollen ausführen. Lokale und Remote-Geräte sorgen für die Datenerfassung. Die Datenverwaltung erfolgt über Datenserver. Anwendungsserver führen Analyse und Berichterstellung durch. Die Daten selbst können mithilfe von Direct Attached Storage, in einem Online-, Nearline- oder Offline-Speicher des EMC-Speicherportfolios abgelegt werden.





## Erhältliche Optionen

Die umfangreiche Produktpalette der ES- und LS-Lösungen basiert auf derselben Hardware-Plattform mit Lizenzierungsmodell und wird so den individuellen Anforderungen Ihres Unternehmens gerecht. Um das für Sie optimale System auszuwählen, sollten Sie die Anzahl der zu überwachenden Netzwerkgeräte sowie die Anzahl der zu verarbeitenden Ereignisse pro Sekunde kennen.

ES Serie		ES 560	ES 1060	ES 2560	ES 5060	ES 7560
Beschreibung		Eigenständige SIEM -Appliance	Eigenständige SIEM -Appliance	Eigenständige SIEM -Appliance	Eigenständige SIEM -Appliance	Eigenständige SIEM -Appliance
Maximale Anzahl von EPS pro Appliance		500 EPS	1,000 EPS	2,500 EPS	5,000 EPS	7,500 EPS
Maximale Anzahl von Devices pro Appliance		100	200	400	750	1,250
Gleichzeitige Nutzung von RSA enVision		6	8	10	12	14
Gleichzeitige Event Explorer-User (enthalten/maximal)		1/5	2/5	3/5	4/5	5/5
Speicher		300 GB intern	300 GB intern	300 GB intern	Externer Speicher erforderlich	Externer Speicher erforderlich
LS Serie	LS A60	LS D60	LC L605	LS L610	LS R601	LS R602
Beschreibung	Anwendungs -Server -Appliance	Datenbank -Server -Appliance	Lokale Collector -Appliance	Lokale Collector -Appliance	Remote -Collector -Appliance	Remote -Collector -Appliance
Maximale Anzahl von EPS pro Appliance	-	30,000 EPS	5,000 EPS	10,000 EPS	1,000 EPS	2,000 EPS
Maximale Anzahl von Devices pro Appliance	-	3,072	1,500	2,048	512	1024
Anzahl gleichzeitiger RSA enVision™ Plattform-User	16	-	-	-	-	-
Gleichzeitige Event Explorer-User (enthalten/maximal)	5/15	-	-	-	-	-
Speicher	Die RSA enVision™ plattform NAS 3500					

## Produktspezifikationen

### BETRIEBSUMGEBUNG

Sicherer, integrierter Microsoft Windows 2003 Server (Standard).

Hardwareundanz

ES: ECC-geschütztes RAM.

LS: 8 GB RAM (buffered).

ES/LS: Redundante/Hot-Swap-Lüfter, Netzteile und

RAID-1-geschützte Festplatten.

### UMGEBUNGSÜBERWACHUNG UND MANAGEMENT

IPMI 2.0 Out-of-Band-Management. 100 % „Headless“-Remote-Appliance-Management.

### NETZWERK

ES: Zwei 10/100/1000TX Ethernet-Anschlüsse enthalten, bis zu sechs über Add-On-Netzwerkschnittstellen.

LS: Sechs 10/100/1000TX Ethernet-Anschlüsse.

### SPEICHEROPTIONEN

Direct Attached 2,75 TB nutzbar (siehe Datenblatt RSA enVision DAS2000)

Network Attached 3,5 TB bis 7 TB nutzbar (siehe Datenblatt RSA enVision NAS3500)

### RECHTLICHE UND BEHÖRDLICHE FREIGABE

ISO9002-zertifiziert, UL1950, CSA22.2 -Nr. 950, EN 60950, FCCPart15 - Klasse A, ICES-003 EN55024:1998, EN55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS3548.

### ANWENDUNGS SOFTWARE

RSA enVision-Plattform mit RSA enVision LogSmart™ IPDB, Echtzeit-Inline-Zuordnung mit automatischer Risikobewertung, Universal Device Support, mehr als 1.100 Standardberichte mit umfassendem Berichtsassistenten, erweiterte Visualisierung mit Event Explorer und forensische Analyse-Tools, ILM-Schutz, Verwaltung von Archivierungsrichtlinien, Unterstützung für Tiered Storage.

### NETZTEILOPTIONEN

Redundante 400-W-Netzteile mit Lastausgleich. Automatische Umschaltung zwischen 120/240 Volt.

### ABMESSUNGEN

74,4 x 44,5 x 8,6 cm (T x B x H). Schienen für die Rack-Montage enthalten (Rack mit vier Trägern erforderlich).

Gewicht: 24,5 kg.

### GEWÄHRLEISTUNG

90-tägige Hardwaregewährleistung, mit gültigem Wartungsvertrag auf fünf Jahre erweiterbar



RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)

The Security Division of EMC

©2008 RSA Security Inc. Alle Rechte vorbehalten.  
RSA, enVision, All the Data, Event Explorer und das RSA-Logo sind Warenzeichen oder eingetragene Warenzeichen von RSA Security Inc. in den Vereinigten Staaten und anderen Ländern. EMC ist ein eingetragenes Warenzeichen der EMC Corporation. Alle weiteren hier angeführten Produkte und Services sind Warenzeichen ihrer jeweiligen Inhaber.  
3IN1 DS 0208