

enVision-Appliances

Jedes Unternehmen ist einzigartig. Aus diesem Grund bieten wir verschiedene Lösungen an, die sich für jede Unternehmensgröße skalieren lassen. Im Zuge Ihres Unternehmenswachstums wächst Ihre SIEM-Lösung für die Verwaltung von Sicherheitsinformationen und Ereignissen mühelos mit. Gerne helfen wir Ihnen dabei, eine Appliance-Lösung zu finden, die den Anforderungen Ihres Netzwerks entspricht.

| | EX Serie | HA Serie | LS Serie |
|--|--------------|-------------|-------------|
| Sustained Performance/Spitzenleistung (Ereignisse pro Sekunde) | 500-2000 | 2500-7500 | 5000-30000 |
| Maximale Geräteanzahl pro Appliance | 64-192 | 256-1024 | 1024-3072 |
| Maximale Anzahl zeitgleicher Benutzer | 2-6 | 8-16 | 16-32 |
| Verfügbare Festplattenspeicher | 320 GB | 630 GB | 630-1890 GB |
| Datenaufbewahrungsdauer | 365-180 Tage | 250-85 Tage | 250-60 Tage |

| | |
|-------------------------------------|--|
| Betriebsumgebung | Sicherheitsgehärtetes, integriertes Betriebssystem Microsoft Windows 2000 Server |
| Hardwareredundanz | ECC-geschütztes RAM, redundante Lüfter, redundante/Hot-Swap-Netzteile, RAID-5-geschützte Festplatten |
| Umgebungsüberwachung und Verwaltung | SMBus ermöglicht die vollständige Temperatur- und Spannungsüberwachung sowie einen integrierten Alarm; vollständig webbasierte Remote-Verwaltung der Anwendung |
| Stromversorgung | Redundante, 500W-Netzteile mit Lastverteilung, 120/240 V Auto-Umschaltung |
| Basisspeicher | Integrierte, vollständig erweiterbare Speichermöglichkeit über externen UltraSCSI-basierten Speicher |
| Zusätzlicher Speicher | Direct Attached Storage und Network Attached Storage |
| Datenschutz | Hardware-beschleunigter 66 MHz/64 Bit RAID-5-Controller mit 64 MB Cache und Backup-Batterie, Hardware-beschleunigte XOR-Berechnungen, 110 db Audioalarm, automatischer Neuaufbau im Hintergrund, Hot-Spare-Festplatten |
| Netzwerk | (2) integrierte 10/100/1000TX Ethernet-Ports. Insgesamt bis zu (6) 10/100/1000TX-Ports verfügbar über Add-On-Netzwerk-schnittstellen |
| Anwendungssoftware | enVision mit LogSmart Internet Protocol Database (IPDB), Echtzeit-Inline-Zuordnung mit automatischer Bedrohungs-bewertung, Universal Device Support zur Einbindung beliebiger Geräte, über 800 Standardberichte mit umfassendem Berichtsassistenten, Echtzeit-Event-Viewer und forensische Analysefunktionen |
| Genehmigungen von Behörden | Zertifiziert nach ISO9002, UL1950, CSA22.2 Nr. 950, EN 60950, FCC Part 15 Class A, ICES-003 EN55024:1998, EMI55022:1998, EN50082-1, VCCI V-3/2000.4, AS/NZS 3548 |
| Datensicherung | Integriertes Low-Profile 4-fach DVD+R-DL-Laufwerk mit bis zu 8,54 GB Speicher pro optischem Datenträger. Archivierungssoftware im Lieferumfang enthalten |
| Datenwiederherstellung | DVD-basierte Medien für rasche Image-Neuerstellung vor Ort |
| Abmessungen | 426x650x89 mm (BxTxH), 28"-Laufschiene für den Serverschrank im Lieferumfang enthalten (Rack mit Doppelrahmen erforderlich) |
| Gewicht | 24,0 kg |
| Hardwaregarantie | 3 Jahre erweiterte Austauschgarantie direkt ab Werk, Hardwaregarantie. Optionale Vor-Ort-Ersatzteilsets |
| Softwaregarantie | 90 Tage Zugang zum Technischen Support zur Unterstützung beim Anwendungssetup und der Fehlerbehebung. Optionaler Software-Abonnementplan mit gebührenfreiem Zugang zum Technischen Support und automatischen Softwareupdates |

Additional Storage

| | PST-3105 | PST-3110 | PST-3115 | NST-2 | NST-4 |
|--|---------------|---------------|---------------|----------------|----------------|
| Verfügbare Ausgangskapazität | 1 TB | 2 TB | 3 TB | 1,1 TB | 2,4 TB |
| Anzahl der Plattenlaufwerke | 6 | 11 | 15 | 15 | 15 |
| Maximal verfügbare Kapazität | 3 TB | 3 TB | 3 TB | 10,8 TB | 13,2 TB |
| Festplattenlaufwerk | SATA | SATA | SATA | FC | FC |
| Anbindungsart | DAS | DAS | DAS | NAS | NAS |
| Redundantes Hot-Swap-Netzteil | ✓ | ✓ | ✓ | ✓ | ✓ |
| Redundanter Hot-Swap-Speicherprozessor | - | - | - | - | ✓ |
| Clustered Failover | Nein | Nein | Nein | Nein | Ja |
| RAID-Level | 5 + Hot Spare | 5 + Hot Spare | 5 + Hot Spare | DP + Hot Spare | DP + Hot Spare |
| Cache | 256 MB | 256 MB | 256 MB | 1 GB | 2 GB |

Zertifizierte Storage-Partner: EMC, NetApp



The Security Division of EMC

www.rsa.com
Tel.: +49/89/943 845-60
Fax: +49/89/ 943 845-66

RSA, The Security Division of EMC
Heisenbergbogen 2-4
D- 85609 Dornach

enVision™-Appliance

EX, HA, LS Serie

Die ehemalige Network Intelligence und jetzige Produktreihe RSA enVision ist anerkannter Marktführer im Bereich der Umwandlung unternehmensweiter Daten in Compliance- und Sicherheitsinformationen. Die ausgereifte LogSmart® Internet Protocol Database™ (IPDB) Architektur ist die einzige im Markt, die erwiesenermaßen alle unternehmensrelevanten Daten jedes IP-Geräts ohne Filter und Agenten effizient zusammenstellt und schützt.

Die Verwaltung von Sicherheitsinformationen und Ereignissen (Security Information & Event Management, SIEM) ist mittlerweile für jedes Unternehmen unabdingbar, das über eine betriebskritische IT-Infrastruktur und strenge Compliance-Vorgaben verfügt. Die innovative Technologie von RSA enVision erfasst und analysiert alle Daten (All the Data™) und bietet daher einen erhöhten Mehrwert. Einfach gesagt: Wir glauben, dass eine wirklich präzise Analyse nur auf Basis der Zusammenstellung aller vorhandenen Daten möglich ist. Im Gegensatz zu anderen Lösungen, die lediglich eine teilweise Momentaufnahme des Unternehmens erstellen, erfasst und speichert enVision™ Tausende Daten in der Sekunde. So bekommen die Kunden einen umfassenden Überblick aller Aktivitäten aus einer beliebigen Anzahl von Quellen, darunter externe Geräte, Netzwerkgeräte, Betriebssysteme und sogar proprietäre Anwendungen. Kein anderes Unternehmen bietet eine geringere Total Cost of Ownership oder einen höheren Return on Investment. Aus diesem Grund ist RSA enVision heute anerkannter Marktführer im Bereich SIEM.

Unternehmensweite Plattform für die Protokollverwaltung

enVision macht Schluss mit den Dateninseln, die in vielen Unternehmen noch trauriger Alltag sind. enVision stellt alle geschäftlich relevanten Daten zusammen und verwaltet sie zentral. Gleichzeitig dient enVision als Plattform, von der aus Sie praktisch jeden Mitarbeiter im Unternehmen mit Informationen versorgen können. Die Server-Techniker können Berichte erstellen lassen, um die Leistung der Infrastruktur zu prüfen. Andere Geschäftsbereiche sind in der Lage, die Wirksamkeit und den Durchsatz zu beleuchten. Compliance-Auditoren stehen umfangreiche Daten zur Verfügung, um Compliance-Vorgaben einzuhalten. Risikomanagement und Sicherheitsabteilungen können Sicherheitswarnungen in Echtzeit anzeigen. Darüber hinaus kann jeder Mitarbeiter, vom Sachbearbeiter über den Helpdesk bis hin zu Anwendungs- und Netzwerkadministratoren, jederzeit auf die benötigten Berichte zugreifen. enVision ermöglicht all dies über eine einzige Plattform.

Compliance, Sicherheit und Geschäftsvorgänge

Neben Compliance- und Sicherheitsaspekten fungiert enVision im Unternehmen als eine Art Nachrichtendienst, der bei Bedarf alle betroffenen Stellen im Unternehmen über Ihre Aktionen informieren kann. Über eine Plattform für die Protokollverwaltung, die sowohl Compliance- als auch Sicherheitsbelange unterstützt, können Sie diesen geschäftlichen „Nachrichtendienst“ für Ihr Unternehmen nutzen. Der wahre Mehrwert, der durch die Analyse aller vorhandenen Daten entsteht, wird besonders bei der Betrachtung der folgenden Probleme deutlich, mit denen die meisten IT-Administratoren immer wieder konfrontiert werden. Da jeder einzelne Vorgang im Netzwerk erfasst wird, steht die Wirksamkeit Ihres SIEM-Systems außer Frage. Dank der leistungsstarken enVision-Tools für die Zusammenstellung, Verwaltung und Analyse lassen sich die Ziele im Hinblick auf Compliance und Sicherheit spielend erreichen.

| Ich bin: | Szenario: | enVision-Lösung: |
|---------------------------|--|--|
| Netzwerk-Administrator | Welche Systeme sind vorhanden, um die Zugriffssteuerung, privilegierte Benutzer und die Konfigurationssteuerung zu überwachen? | Durch die Erfassung aller Daten (<i>All the Data</i>) analysiert enVision Hunderte verteilte Sicherheitsvorkommnisse, warnt bei Änderungen und nicht autorisierter Verwendung von Systemen in Echtzeit und verschlankt so die Sicherheitsverwaltung. |
| Sicherheits-Administrator | Wie erstellt Ihr Unternehmen ein Compliance-Programm, das kostengünstig ist? | Nachweis der Compliance durch formatierte Berichtsschablonenpakete speziell für Sarbanes Oxley, GLBA, PCI, HIPAA, FISMA, NERC, Basel II und NISPOM. |
| Server-Administrator | Wie halten Sie mit Überwachung in Echtzeit, der Erkennung von Bedrohungen und böartigem Code Schritt, ohne zahlreiche Fehlalarme zu verursachen? | enVision senkt die Anzahl der Fehlalarme durch den Abgleich von Daten mit anderen Netzwerk- und Sicherheitsgeräten. Außerdem lassen sich Bedrohungen nach den wichtigsten Ressourcen ordnen, damit diese sofort Aufmerksamkeit erlangen. |
| Datenbank-Administrator | Wie lassen sich aus einer erkannten Sicherheitsbedrohung Querverweise auf das übrige Netzwerk erstellen? | Der enVision Event Explorer™ ermöglicht den Blick über Anwendungen, Firewalls, IDS- und anderen Datentypen sowie die Vergrößerung der Daten aus unterschiedlichen Perspektiven. |
| Anwendungs-Administrator | Wie kann ich diesem verschiedenartigen System meine proprietäre Anwendung hinzufügen? | Zusätzlich zu Hunderten unterstützter Geräte gibt Ihnen die offene Architektur von enVision alle Tools an die Hand, mit denen Sie nach Belieben neue Quellgeräte hinzufügen können. |

Zusammenstellung

Erfassung aller Daten von mehreren Hundert Quellgeräten

| | |
|--------------|-----------------|
| Apache | NFR |
| Apple | Nokia |
| Arbor | Nortel |
| Barbed Wires | Novell |
| Bivio | Omni Cluster |
| Blue Coat | Open Source |
| Celestix | Oracle |
| Check Point | Qualys |
| Cisco | RapidStream |
| CrossBeam | Redhat |
| CyberGuard | Resilience |
| Enterasys | RLX |
| Extreme | RSA |
| Fortinet | Secure |
| Foundry | SecureGuard |
| Foundstone | Siemens |
| Free BSD | Smart-Plattform |
| HP/Compaq | Solsoft |
| IBM | SonicWall |
| Intel | SourceFire |
| Intrusion | Sun |
| ISS | Symantec |
| [Juniper] | Tipping Point |
| McAfee | Top Layer |
| Microsoft | Trend Micro |
| nCircle | Websense |
| NetApp | Und viele mehr |

Eine vollständige Liste finden Sie im Internet unter:
www.network-intelligence.com

Im Gegensatz zu anderen, eingeschränkten Lösungen, die Daten von Quellgeräten reduzieren oder vorfiltern, erfasst enVision sämtliche Daten vollständig. Durch LogSmart® Internet Protocol Database (IPDB), die revolutionäre Architektur zur Zusammenstellung von Protokolldaten von RSA enVision, die auf Agenten verzichten kann, profitiert Ihr Unternehmen von der Analyse in Echtzeit und der gleichzeitigen Authentifizierung, Komprimierung und Verschlüsselung von Quelldaten. Somit sind Warnungen äußerst präzise und werden zeitnah ausgegeben, was wiederum zu einer sehr geringen Anzahl von Fehlalarmen führt. Diese Lösung ist ein absolutes Muss im Bereich der Sicherheit.

Die Vorteile der Datenzusammenstellung ohne Agenten liegen auf der Hand: keine Filterung der Daten an der Quelle, keine laufende Verwaltung von Agenten, die im gesamten Netzwerk verteilt sind, kein Risiko für die und keine Beeinträchtigung der Netzwerkinfrastruktur sowie eine geringere TCO, die durch die einfache Konfiguration und Bereitstellung möglich wird.

Die Zusammenstellung aller Vorgangsdaten ist der Schlüssel zu einer vollständigen Abdeckung im Einklang mit den Regelungen und Richtlinien für Sicherheit und Compliance. Diese Daten verraten Ihnen alles, was Sie über die Aktivitäten Ihrer Mitarbeiter wissen müssen, über den Zugriff auf Kunden- und Finanzdaten, über verdächtige und verweigerte Zugriffe von außerhalb des Netzwerks usw. Mit enVision können Sie Daten von Hunderten verteilter Geräte und Anwendungen im gesamten Unternehmen erfassen. Darüber hinaus können Sie mit dem Universal Device Support proprietäre Geräte und Anwendungen im Handumdrehen einbinden.

Universal Device Support

Die offene Architektur von enVision gibt Ihnen alle Tools an die Hand, mit denen Sie neue Quellgeräte rasch und nach Belieben einbinden können. Dies ist besonders ideal für intern entwickelte Auditing-Anwendungen sowie Second-Tier-Geräte. Der Universal Device Support stellt dem Benutzer eine einfach zu verwendende Plattform für das Zusammenstellen, Analysieren und Verwalten von Protokolldaten für neue Geräte zur Verfügung.

- Benutzeroberfläche zum Hinzufügen neuer Nachrichten
- Steuerung der Geräte- und Nachrichtenklassifizierung
- Einfache Definition von Nachrichten-IDs und Nutzdaten
- Unterstützung mehrerer Anwendungen auf demselben Host



Paketlösungen für Compliance-Berichte

enVision beinhaltet zahlreiche Berichtsfunktionen zur Unterstützung der Compliance- und Sicherheitsanforderungen für jeden Unternehmenstyp. Sie ermöglichen u.a. die spontane oder zeitgesteuerte Erstellung umfangreicher Berichte, wobei die Ausgabe direkt im spezifischen Format im Einklang mit den jeweiligen Compliance-Vorgaben erfolgt: GLBA, HIPAA, SOX, PCI, Basel II, NISPOM, FISMA, NERC.

Analyse

Baselines

enVision setzt auf einer Wissensdatenbank auf, die Zehntausende bekannter Protokollnachrichten sowie ein offenes Klassifizierungswörterbuch enthält (Taxonomie). Das System lernt Ihre Netzwerkmuster, um Baselines zu erstellen.

- Baselines werden automatisch erstellt und müssen nicht konfiguriert werden.
- Baselines sind für beliebige Zeiträume verfügbar.
- Sie können Zuordnungsregeln erstellen, um prozentuale Abweichungen von Baseline-Werten zu erkennen.
- Sie können dynamische Baselines erstellen, um bestimmte Gerätegruppen und Vorgänge nachzuverfolgen.

Zugeordnete Warnungen und Sicherheitsberichte

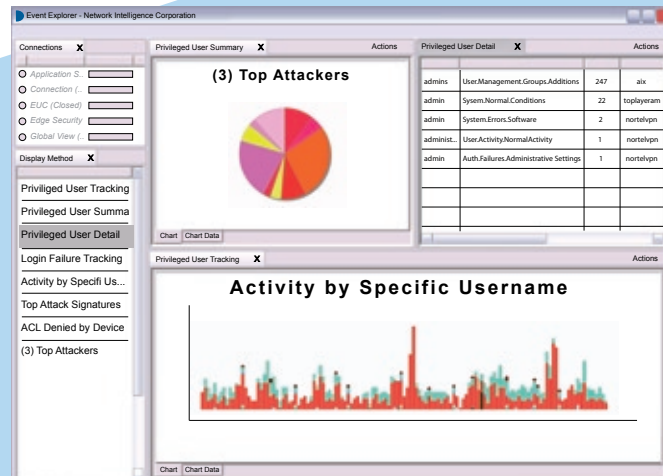
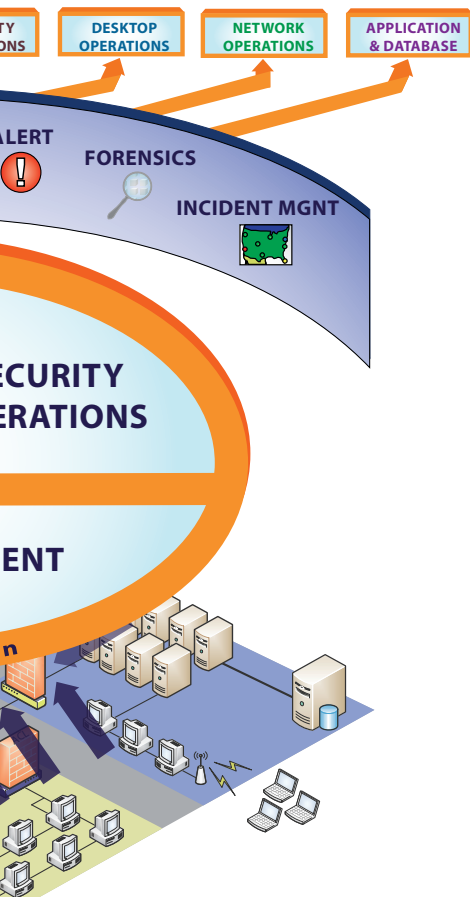
Durch die skalierbare Datenzusammenstellung und der umfangreichen Ansichten aller Protokolle bietet die Berichts-Engine von enVision schnellen und einfachen Zugriff auf Compliance-relevante Daten. Für bestimmte Compliance-Vorgaben sind integrierte Berichte verfügbar, und Berichtsadministratoren können auf Basis der unternehmensspezifischen Compliance-Vorgaben selbst Berichte erstellen.

Mit über 700 integrierten Berichten bietet enVision Informationen für zahlreiche Themen, z.B. Netzwerk, Sicherheit, Host und Storage.

- Alle Berichte können an die individuellen Anforderungen angepasst werden.
- Berichte können einen beliebigen Datenzeitraum betreffen, der Minuten, aber auch Monate umfassen kann.
- Berichte können sofort ausgeführt oder für die automatische Ausführung programmiert werden.
- Verschiedene tabellarische und grafische Darstellungsformen werden unterstützt.
- Es werden mehrere Exportformate unterstützt, z.B. .csv, .xls usw.

Forensik

enVision ermöglicht durch umfangreiche Drilldown-Funktionen die detaillierte Ansicht der Vorgänge, die Sicherheitsbedrohungen auslösen. Sicherheitsadministratoren können genau sehen, welche Muster sich in ihren Netzwerken entwickeln. Dazu zählen auch die bestimmten IP-Adressen, Ports, Hosts, Benutzer und Protokolle, die mit diesen Mustern in Zusammenhang stehen. Umfangreiche Abfrage- und Filterfunktionen sowie leistungsstarke Tools in der Benutzeroberfläche ermöglichen eine leichte Datensuche nach beliebigen Attributen.



Event Explorer

Der Event Explorer ist eine „völlig neue Art, alle Daten zu visualisieren.“ Dieses fortschrittliche Analysemodul für enVision bietet eine vollkommen neue Detailebene. Sie können damit nicht nur sämtliche Daten erfassen, sondern sie auch dynamisch anzeigen. So können Sie z.B. ausgewählte Ansichten vergrößern, wobei der Event Explorer die gleichzeitig zu prüfenden Bereiche ausweitet. Durch die Erstellung einer Plattform für die Protokollverwaltung sind Sie jederzeit für neue Compliance-Vorgaben sowie Sicherheits- und Geschäftsbelange gewappnet.