



Kurzdarstellung des Produkts: ArcSight Express

Der Sicherheitsexperte "In der Box"

Schützen Sie Ihr Unternehmen mit integrierten Lösungen für die wichtigsten Sicherheits- und Compliance-Probleme

Höhepunkte:

- Umfassende Überwachung der Sicherheit von Geräten, Netzwerken und Servern
- Automatisierung von Sicherheitsoperationen
- Einfach bereitzustellende und zu verwaltende Appliance-Lösung

Das Netzwerk ist immer noch in Gefahr

Die Sicherheitsbedrohungen für Netzwerke nehmen weiterhin zu. Aktuelle Studien zeigen allein für das Jahr 2008 einen Anstieg bei der Malware um 300 %. Leider sind Organisationen mit kleineren Sicherheitsabteilungen und geringeren Budgets nicht von kleineren Risiken betroffen. Das hat zur Folge, dass viele Organisationen gegen Angriffe von Hackern, Viren, Malware, sowie gegen Datenverstöße und Identitätsbetrug anfällig sind. Noch problematischer ist, dass diese Firmen oft nicht einmal über ein spezialisiertes Sicherheitsteam oder über das notwendige Sicherheitswissen verfügen. Die Präsenz von Malware nimmt zu, Datenverstöße werden häufiger und die gesetzlichen Vorschriften immer umfangreicher; gleichzeitig schrumpfen aber bei vielen Firmen die personellen Ressourcen für diese Probleme.

Organisationen, die einer zunehmenden Bedrohung ihrer Netzwerke und ihrer kritischen Daten ausgesetzt sind, deren Möglichkeiten und Wissen auf diesem Gebiet aber begrenzt sind, steht mit ArcSight Express eine einfache, automatisierte und kostengünstige Lösung zur Verfügung.

ArcSight Express öffnet die Möglichkeiten, die sich aus einer leistungsfähigen Ereigniskorrelation mit Log-Management ergeben, für eine ganz neue Schicht von Kunden. ArcSight Express analysiert Logs von allen Geräten oder Systemen auf Ihrem Netzwerk, stellt fest, ob potenziell riskante Vorfälle auftreten, und benachrichtigt

Administratoren rechtzeitig, damit diese die entsprechenden Maßnahmen ergreifen können. ArcSight Express erledigt die Schwerstarbeit eines dedizierten Sicherheitsexperten: Netzwerksicherheitsereignisse erhalten eine Bedeutung, indem sie in den entsprechenden Kontext gesetzt werden. Dabei wird festgestellt, welches Ereignis wo, wann und warum aufgetreten ist und welche Auswirkungen dieses auf die Organisation hat. Echtzeitalarme zeigen Administratoren die kritischsten Sicherheits- und Compliance-Ereignisse im Unternehmen zusammen mit dem notwendigen Kontext, damit die damit verbundene Sicherheitsverletzung weiter analysiert und minimiert werden kann. ArcSight Express hilft auch bei der Einhaltung von Compliance-Anforderungen. Das Produkt bietet die Möglichkeit, Logs in Audit-Qualität zu speichern und aussagekräftige Compliance-Berichte für schnelle, einfache Audits zu erstellen.

Integrierte Sicherheitskompetenz

ArcSight Express enthält die Regeln, Alarme und Berichte, die für den Schutz mittelständischer Unternehmen relevant sind. Alle sind bereits integriert und können ohne vorherige Anpassung an die spezifische Situation verwendet werden. Eine Regel oder ein Bericht kann mithilfe der grafischen Konsole oder dem Regelerstellungstool in ArcSight in einfacher Weise erweitert werden. Die Produktkompetenz erstreckt sich auf die wichtigsten Probleme, mit denen Kunden konfrontiert werden. Dazu gehören unter anderem:



Bot-, Wurm- und Virenangriffe

- An der Spitze liegende infizierte Systeme
- Alle AV-Konfigurationsänderungen, Fehler

Bandbreitenverschwender und Richtlinienverletzungen

- Benutzer mit der höchsten Bandbreitenauslastung
- Konfigurationsänderungen
- Erfolgreiche und fehlgeschlagene Anmeldungen
- Kennwortänderungen
- Wichtigste Angreifer und interne Ziele

Datenbanküberwachung

- Datenbankfehler und Warnungen
- Datenbankszugriff, Konfiguration

Nicht autorisierter Zugriff auf Applikationen

- Benutzerauthentifizierung, Verwaltung und Konfigurationsänderungen

Netzwerkfehler und Änderungen

- Netzwerkgerätefehler und -status
- Zugriffs- und Konfigurationsänderungen
- An der Spitze liegende Verbindungen

Spezifikationen der ArcSight Express-Appliance

Modell	M7100-M	M7100-L	M7100-X	L3000
Betriebssystem	Linux	Linux	Linux	Linux
Komprimierung				Bis zu 10:1
Gesamtanzahl Geräte	140	350	725	Wie bei M7100
EPS max.	500	1.000	2.500	Wie bei M7100
Geräte max.	5.000	10.000	25.000	k.A.
Webbenutzer	Keine Einschränkung	Keine Einschränkung	Keine Einschränkung	Keine Einschränkung
CPU	2 x Intel Xeon E4505 Quad Core	2 x Intel Xeon E4505 Quad Core	2 x Intel Xeon E4505 Quad Core	1 x Dual Core Intel Xeon 3050
Schnittstellen	2 x 10/100/1000	2 x 10/100/1000	2 x 10/100/1000	2 x 10/100/1000
RAM	16 GB	16 GB	16 GB	4 GB
Speicher	6 x 400 GB - RAID10 Effektiv 1 TB	6 x 400 GB - RAID10 Effektiv 1 TB	6 x 400 GB - RAID10 Effektiv 1 TB	2 x 750 GB - RAID1 Effektiv 6 TB
Gehäuse	2U	2U	2U	1U
Stromversorgung	2x 750 W 100 – 240 VAC	2x 750 W 100 – 240 VAC	2x 750 W 100 – 240 VAC	Nicht redundant
Abmessungen (T x B x H)	74,4 cm x 43,7 cm x 8,6 cm	74,4 cm x 43,7 cm x 8,6 cm	74,4 cm x 43,7 cm x 8,6 cm	57,4 cm x 42,6 cm x 4,3 cm

Über ArcSight:

ArcSight (NASDAQ: ARST) ist ein weltweit führender Anbieter von Lösungen zum Sicherheits- und Compliance-Management zum Schutz von Unternehmen und Regierungsbehörden. ArcSight hilft Kunden bei der Einhaltung von Unternehmens- und gesetzlichen Richtlinien, bei der Sicherung ihrer Vermögenswerte und Prozesse und bei der Kontrolle der Risiken. Die ArcSight-Plattform sammelt Daten und korreliert Benutzeraktivitäten mit Ereignisdaten im gesamten Unternehmen, sodass Firmen Compliance-Verletzungen, Nichteinhaltung von Richtlinien, Angriffe auf die Computersicherheit und Insider-Gefahren schnell identifizieren, priorisieren und auf sie reagieren können. Weitere Informationen erhalten Sie auf unserer Website: www.arcsight.com.

VPN-Sneak-Angriffe

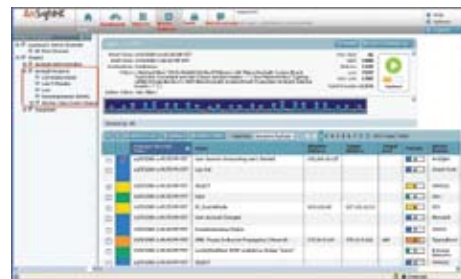
- VPN-Authentifizierungsfehler
- Verbindungsaktivitäten
- VPN-Konfigurationsänderungen

Server- und Desktopüberwachung

- Verwaltung von privilegierten Benutzern
- Zugriffs- und Konfigurationsänderungen
- Abgelehnte Verbindungen
- IPS/IDS-Alarme und Bandbreitenauslastung
- Erfolgreiche/fehlgeschlagene Anmeldeaktivität

Compliance-Berichte auf der Basis verschiedener Vorschriften

ArcSight Express bietet eine Reihe von Kontrollfunktionen zur allgemeinen Compliance-Überwachung, die für verschiedene Vorschriften angewendet werden können, darunter Sarbanes-Oxley, PCI DSS, Gramm-Leach-Bliley, FISMA, Basel II und HIPAA. Jede dieser Funktionen kann durch vordefinierte Pakete zur Compliance-Überwachung ergänzt werden. Dabei handelt es sich um spezielle Lösungsmodulare, die eine umfassende Berichterstattung im Hinblick auf spezifische Vorschriften ermöglichen.



Über die Webkonsole von ArcSight Express können Sie Ihr Netzwerk einfach und in Echtzeit überwachen.



ArcSight Express gibt Ihnen die kritischen Informationen, die Sie brauchen, um schnell reagieren zu können.



ArcSight, Inc.
5 Results Way, Cupertino, CA 95014, USA
www.arcsight.com info@arcsight.com

Konzernhauptszitz: +1 888 415 ARST
Hauptszitz für den EMEA-Raum: +44 870 351 6510
Hauptszitz für den asiatisch-pazifischen Raum:
+852 2166 8302

© 2009 ArcSight, Inc. Alle Rechte vorbehalten.
ArcSight und das ArcSight-Logo sind Warenzeichen von ArcSight, Inc. Alle anderen hier erwähnten Produkt- und Firmennamen sind möglicherweise Warenzeichen oder eingetragene Warenzeichen ihrer jeweiligen Eigentümer.
ARST-PB005-040109-02