InTrust®

Cleveres und skalierbares Verwaltungstool für Ereignisprotokolle

Der wertvollste Posten Ihres Unternehmens sind seine Daten und die Benutzer, die darauf zugreifen können. Für IT- und Sicherheitsabteilungen ist die Verfolgung der Aktivitäten von Benutzer- und privilegierten Konten – vor allem auf Workstations und Endbenutzergeräten – Grundlage für die Sicherheit ihrer Umgebung und die Einhaltung verschiedenster Branchenvorschriften. Allerdings ist das eine schwierige Aufgabe wegen der immensen Menge an auf verschiedenen Systemen, Geräten und Anwendungen verteilten Daten. Die Erhebung, Speicherung und Analyse all dieser Daten erfordert im Allgemeinen große Mengen an Speicherkapazität, zeitaufwändige Erhebung von Ereignisdaten sowie Fachleute für die erhobenen Ereignisdaten vor Ort.

Mit Quest® InTrust® können Sie sämtliche Aktivitäten von Benutzer-Workstations und Administratoren von der An- bis hin zur Abmeldung überwachen. Reduzieren Sie die Massenspeicherkosten durch 20:1 Datenkomprimierung und speichern Sie Ereignisprotokolle aus mehreren Jahren von Windows- oder UNIX/Linux-Servern, -Datenbanken, -Anwendungen und -Netzwerkgeräten. Die Warnungen in Echtzeit von InTrust geben Ihnen die Möglichkeit, mit automatischen Reaktionen auf verdächtige Aktivitäten sofort auf Bedrohungen zu reagieren.

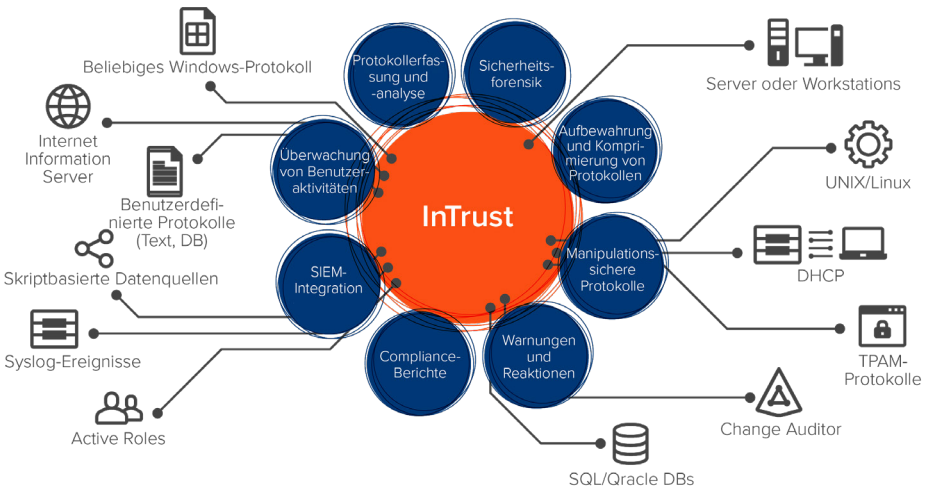
FUNKTIONEN UND MERKMALE

Zentrale Verwaltungsansicht

Sammeln und speichern Sie alle nativen Workstation-Protokolle und solche von Dritten von verschiedenen Systemen, Geräten und Anwendungen an einem einzigen suchbaren Ort mit umgehender Verfügbarkeit für Sicherheits- und Compliance-Berichterstellung. InTrust liefert eine vereinheitlichte Ansicht von Windows-Ereignisprotokollen, Protokollen von UNIX/Linux, IIS und Webanwendungen, PowerShell-Prüfpfade, Endgerätschutzsysteme, Proxys und Firewalls, Virtualisierungsplattformen, Netzwerkgeräten, benutzerdefinierten Textprotokollen sowie Ereignissen in Quest Change Auditor.

Überwachung von Benutzer-Workstation-Protokollen

Schützen Sie Ihre Workstations vor modernen Cyber-Angriffen wie Pass-the-Hash-Angriffen, Phishing oder



Überwachen Sie effizient alle Benutzer-Workstations und Administratoraktivitäten, um Ihren wertvollsten Posten zu sichern – Ihre Daten.

„Wir verwenden InTrust zur Protokollerfassung von Domänencontrollern und Überwachungsereignissen zur Überprüfung der SOX-Compliance. Mir gefällt die Verzeichnisansicht. Darüber kann man zu Sicherheitszwecken gut nach Kontosperrungen und anderen Anmeldeereignissen suchen."

Techniker, S&P 500 Professional Services Company

TVID: 726-084-5E5

VORTEILE:

- Verringerung von Speicherkosten und Gewährleistung kontinuierlicher Compliance dank stark komprimiertem und indexiertem Protokollverzeichnis
- Durchsuchen aller Aktivitäten von Endbenutzern und privilegierten Konten von einem Ort
- Schnelles Melden, Beheben und Untersuchen von Sicherheitsereignissen
- Mit normalisierten nativen Ereignisprotokollen Daten ordnen
- Einfache Integration in Ihre bestehende SIEM-Lösung
- Umgehende Reaktion auf Bedrohungen mit Warnungen in Echtzeit und automatischen Reaktionen
- Schutz von Ereignisprotokolldaten vor Manipulation oder Zerstörung durch Duplizieren der Ereignisse beim Erstellen

„Ich finde, das Produkt bietet Funktionen zur Sicherheitsberichterstellung und Warnung von unschätzbarem Wert. Obwohl andere Produkte Ähnliches können, glaube ich, dass InTrust eine schnelle Implementierung ermöglichen kann, die auf dem Gebiet der Überprüfung und Compliance sofortigen Nutzen liefert."

Senior IT Manager, Fortune 500 Automotive & Transport Company

TVID: D2B-CDB-505

SYSTEMANFORDERUNGEN

UNTERSTÜTZTE PLATTFORMEN
Ereignisse in Microsoft Windows
Ereignisse in Microsoft IIS
Ereignisse in Microsoft Forefront Threat Management Gateway und ISA Server
Ereignisse in Microsoft DHCP Server
Ereignisse in Solaris
Ereignisse in Red Hat Enterprise Linux
Ereignisse in Oracle Linux
Ereignisse in SUSE Linux
Ereignisse in Debian GNU/Linux
Ereignisse in Ubuntu Linux
Ereignisse in IBM AIX
Ereignisse in HP-UX
Ereignisse in VMware vCenter
Ereignisse in VMware ESX und ESXi
Weitere Informationen finden Sie in der Dokumentation zu den Systemanforderungen.

Ransomware, indem Sie die Aktivitäten von Benutzern und Administratoren von der An- bis hin zur Abmeldung überwachen. Sammeln und speichern Sie alle wichtigen Einzelheiten des Benutzerzugriffs wie z. B. die durchführende Person, worum es bei der Aktion ging, auf welchem Server diese Aktion stattfand und von welcher Workstation sie ausging.

Vereinfachte Ereignisprotokollanalyse

Konsolidieren Sie kryptische Ereignisprotokolle aus unterschiedlichen Quellen in ein einfaches, gewöhnliches Format mit den Angaben Wer, Was, Wann, Wo, Von wo und An Wen, um die Daten einfacher auswerten zu können. Vor allem Syslog-Daten unterscheiden sich erheblich von Anwendung zu Anwendung. Mit InTrust® können Sie strukturierte Daten in Syslog-Ereignissen feststellen und diese Daten richtig analysieren. Die einzigartige Volltext-Indexierung macht Ereignisdaten über einen längeren Zeitraum für schnelle Berichterstellung, Fehlerbehebung und Sicherheitsuntersuchungen einfach auffindbar.

Clevere und skalierbare Komprimierung von Ereignisprotokollen

Sammeln und speichern Sie riesige Datenvolumen in einem stark komprimierten Verzeichnis (20:1 mit Indexierung, 40:1 ohne Indexierung), damit Sie Ihre Massenspeicherkosten um bis zu 60 Prozent verringern und die fortgesetzte Einhaltung von HIPAA-, SOX-, PCI-, FISMA- und anderen Vorschriften sicherstellen können. Zudem kann ein InTrust-Server mit 10.000 Agenten, die gleichzeitig Ereignisprotokolle schreiben, bis zu 60.000 Ereignisse pro Sekunde verarbeiten, was Ihnen mehr Effizienz, Skalierbarkeit und erhebliche Einsparungen bei Hardware-Kosten verschafft. Und wenn Sie mehr Volumen benötigen, können Sie einfach einen weiteren InTrust-Server hinzufügen und die Rechenlast aufteilen. Die Skalierbarkeit ist quasi unbegrenzt.

Warnungen und Reaktionen in Echtzeit

Halten Sie Ausschau nach unautorisierten und verdächtigen Benutzeraktivitäten wie das Erstellen von Dateien über Begrenzungen hinaus, indem Sie die Dateierweiterungen bekannter Ransomware-Angriffe oder verdächtige PowerShell-Befehle nutzen. Reagieren Sie dank Echtzeitwarnungen umgehend auf Bedrohungen. InTrust gibt Ihnen die Möglichkeit, problemlos automatische Reaktionen auf verdächtige Ereignisse auszulösen. So können Sie die betreffende Aktivität zum Beispiel blockieren, den angreifenden Benutzer deaktivieren, die Änderung rückgängig machen und/oder Notfallprüfungen aktivieren.

Manipulationssichere Protokolle

Schützen Sie Daten aus Ereignisprotokollen vor Manipulationen oder Vernichtung, indem Sie auf jedem Remote-Server, wo Protokolle, wenn sie erstellt werden, dedupliziert werden können, einen gecachten Speicherort erstellen.

SIEM-Integration

Verringern Sie Ihre jährlichen Kosten für SIEM-Lizenzen mit InTrust-Konnektoren für Splunk und IBM QRadar. Speichern Sie Langzeit-Ereignisprotokolldaten mit InTrust. Filtern und leiten Sie basierend auf Branchen-Best-Practices nur relevante Daten an Ihre SIEM-Lösung weiter, um Sicherheitsanalysen in Echtzeit durchzuführen.

Bessere Einblicke mit IT Security Search

Nutzen Sie die wertvollen Erkenntnisse all Ihrer Sicherheits- und Compliance-Lösungen von Quest® an einem Ort. Mit IT Security Search können Sie Daten von InTrust, Change Auditor, Enterprise Reporter, Recovery Manager for AD und Active Roles in einer Google-ähnlichen IT-Suchmaschine zur schnelleren Reaktion auf Sicherheitsvorfälle und forensischen Analyse korrelieren. Analysieren Sie einfach Benutzerberechtigungen und Aktivitäten, Ereignistrends, verdächtige Muster und vieles mehr mithilfe aussagekräftiger Darstellungen und Ereigniszeitleisten.

Automatisierte Berichterstellung zu Best Practices

Wandeln Sie Untersuchungen einfach in verschiedene Berichtformate wie HTML, XML, PDF, CSV oder TXT sowie Microsoft Word, Visio und Excel um. Sie können Berichte planen und die Verteilung an die Teams automatisieren oder aus einer großen Bibliothek vordefinierte Best Practice-Berichte mit Informationen zur Ereignisprotokollierung auswählen. Mit Datenimport und Konsolidierungs-Workflows können Sie sogar eine Datengruppe zur umfassenderen Analyse an SQL Server weiterleiten.

ÜBER QUEST

Quest liefert Softwarelösungen für die ständig im Wandel befindliche Welt der Unternehmens-IT. Wir helfen, die durch Datenexplosion, Hybrid-Rechenzentren, Sicherheitsbedrohungen, und gesetzliche Bestimmungen hervorgerufenen Schwierigkeiten zu verringern. Unser Portfolio beinhaltet Lösungen für Datenbankverwaltung, Datenschutz, vereinheitlichte Endpunktverwaltung, Identitäts- und Zugriffsverwaltung sowie Verwaltung von Microsoft Plattformen.

Quest
quest.com/de
Sie finden Informationen zu lokalen Niederlassungen auf (quest.com/de-de/locations)

DataSheet-InTrust-US-KS-DE-WL-39601