NetIQ Privileged Account Manager

Sicherer Zugriff für berechtigte Benutzer aus der Cloud und auf die Cloud

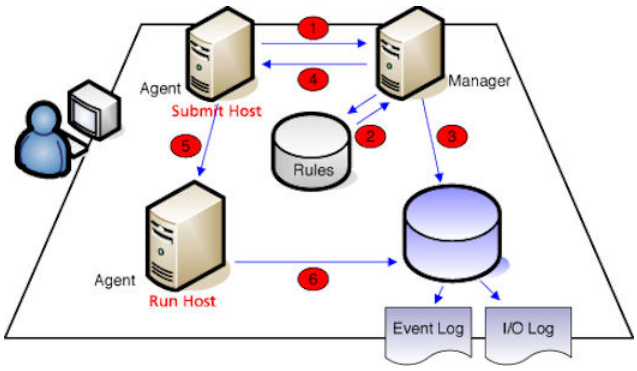
Experten-Schätzungen zufolge findet die Hälfte aller Sicherheitsverstöße innerhalb der Unternehmen selbst statt. Insider-Angriffe sind besonders ernst, wenn sie mit Mitarbeitern in Verbindung gebracht werden, die höhere Zugriffsrechte haben als sie eigentlich benötigen. Ob nun der Missbrauch eines privilegierten Zugriffs durch einen Mitarbeiter geschieht, oder das Werk eines Cyber-Kriminellen ist, der die Zugriffsberechtigung eines Insiders nutzt, um auf Ihr IT-Netzwerk zuzugreifen – am besten können Sie dieses Risiko eindämmen, indem Sie den Zugriff berechtigter Benutzer, wie Superuser und Datenbank-Administratoren genau kontrollieren und überwachen.

Produktübersicht

NetIQ® Privileged Account Manager beseitigt die Notwendigkeit, Anmeldedaten für Root-Accounts an all Ihre Administratoren weiterzugeben. Der Administrator-Zugriff wird durch zentrale Richtlinien zugewiesen. Diese Richtlinien können Sie konfigurieren, um Nutzeraktivitäten zuzulassen oder zu unterbinden, basierend auf einem „Wer-, Was-, Wo-, Wann-Modell", das den Namen, den eingegebenen Befehl, den Hostnamen sowie den Zeitpunkt des Benutzerzugriffs untersucht. Durch diese Art der Verwaltung von Zugriffsrechten kontrollieren Sie, welche Befehle Benutzer zu welchem Zeitpunkt und von welchem Standort aus ausführen dürfen.

NetIQ Privileged Account Manager umfasst ein Enterprise Credential Vault, d.h. ein verschlüsseltes Passwortdepot, für ein sicheres Speichern Ihres Systems, Ihrer Anwendung und Ihrer Datenbankpasswörter. Mit dem Enterprise Credential Vault können Sie die privilegierten Konten Ihres Unternehmens zentral verwalten. Außerdem bietet es eine intuitive Benutzeroberfläche für privilegierte Benutzer zur Überprüfung und Rückgabe von Passwörtern. Zusätzlich ermöglicht es umfassenderen Support privilegierter Konten für Anwendungen (wie SAPSystem), Datenbanken (wie Oracle DBMS) und Cloudservices (wie Salesforce.com.)

Dank der branchenweit einzigartigen GUI-basierten Drag-and-Drop-Oberfläche vereinfacht NetIQ Privileged Account Manager die Erstellung von Regeln. Zudem werden kaum noch komplexe manuelle Skripts benötigt. Sie verfügen über ein integriertes Test-Suite-Tool zum Erstellen und Testen neuer Regelkombinationen, bevor diese in der Produktionsumgebung eingesetzt werden.



1 Funktionsweise des Privileged Account Manager

Lösung

Zugriffsmanagement

Produkt

NetIQ Privileged Account Manager

„Mit NetIQ Privileged Account Manager können Sie und Ihr Unternehmen die privilegierten Zugriffsrechte für Datenbanken, Anwendungen und die Cloud kontrollieren und überwachen."

Der Privileged Account Manager verwendet eine einzigartige Risikoanalyse-Engine zur Analyse eines jeden eingegebenen Befehls und weist ihm eine Risikostufe zwischen 0 und 9 zu, wobei der ausgeführte Befehl, der für die Ausführung verantwortliche Benutzer und der Standort berücksichtigt werden. Befehle, die mit einem hohen Risiko behaftet sind, werden rot angezeigt; mit niedrigem Risiko behaftete Befehle erscheinen grün. Alle anderen Befehle sind mit einem dazwischenliegenden Farbton markiert. Auf diese Weise sind Ereignisse, die ein Sicherheitsrisiko darstellen, auf einen Blick erkennbar.

Zudem haben Sie die Möglichkeit, aufgezeichnete Tastatureingaben über eine benutzerfreundliche Oberfläche mit Wiedergabefunktionen abzurufen. Muss ein Ereignis genauer analysiert werden, so kann es im Rahmen eines Workflows an den zuständigen Manager weitergeleitet werden, der dann unverzüglich geeignete Maßnahmen ergreift.

Privileged Account Manager erweitert die risikobasierte Aktivitätskontrolle für eine automatische Durchsetzung von Richtlinien während der Sitzungen privilegierter Benutzer. Unternimmt ein Benutzer riskante Aktivitäten, versucht er z. B. auf vertrauliche Daten zuzugreifen oder einen Service anzuhalten, kann ein Administrator Privileged Account Manager so konfigurieren, dass die Sitzung automatisch getrennt wird oder einem Benutzer die Zugriffsrechte für privilegierte Konten entzogen werden.

Funktionen

Kontrollieren und überwachen Sie unbefugten und unüberwachten Zugriff privilegierter Benutzer in Ihrer gesamten heterogenen Umgebung.

- Zentrale Verwaltung von Sicherheitsrichtlinien.
- Kontinuierliche Einhaltung von internen Richtlinien und externen Auflagen.
- Vermeidung von komplexen manuellen Skripts.
- Einführung einer konsistenten Richtlinie in Ihrer Umgebung über eine zentrale Verwaltung.
- Durchsetzung von Zugangsrichtlinien, Analysen und Berichten zur Einhaltung von Datenschutzgesetzen und -Regulierungen.

Merkmale

Gestalten, konfigurieren, testen und verwenden Sie eine privilegierte Verwaltungslösung in Ihrer gesamten Umgebung von einem einzigen Standort aus.

- Enterprise Credential Vault für gesicherte Passwortarchivierung
- Privilegierte Kontenüberwachung von Datenbanken für Benutzer, Tools und Anwendungen
- Risikobasierte Sitzungskontrolle zur möglichen automatischen Sitzungsbeendigung oder Zugriffssperre
- Remote-Sitzungseinrichtung und -kontrolle für Betriebssysteme
- Risikoprofile, die umgehend risikoreiche Benutzer identifizieren.

Wichtige Unterscheidungsmerkmale

Bauen Sie ein umfassendes AuditProtokoll auf. Mit dem NetIQ Privileged Account Manager haben Sie die Möglichkeit zur Überprüfung jeglicher Benutzeraktivitäten durch Aufzeichnung aller Tastatureingaben sowie durch Bilderfassung für alle anmeldebasierten Umgebungen (wie SAP-System), Datenbanken (wie Oracle DBMS) und Cloudservices (wie Salesforce.com).

Die Auditoren können das gesamte Ereignis für bestimmte Zugriffsereignisse bis zu jeder einzelnen Tastatureingabe mit farbcodiertem Line-by-Line Detail zurückspulen und jedem Ereignis den Status „befugt" oder „unbefugt" hinzufügen.