RAZ-LEE

iSecurity Suite, die neue Generation April 2026

Die umfassende Sicherheitslösung für alle Anforderungen rund um IBM i

RAZ-LEE iSecurity

iSecurity Neue Generation

Version April 2026

- Umfassende Aktualisierung nahezu aller iSecurity-Produkte
- Verbesserte Zusammenarbeit der iSecurity-Produkte
- Jetzt auch mit Abonnement-Lizenz verfügbar
- Mehr Automatisierung, Sicherheit und Compliance

Neuerungen in dieser Version

- Einheitliches Lizensierungsmodell
- Verbesserte Integration in IBM i
- Erweiterte MFA-Funktionen
- Erweiterte Audit- und Reporting-Funktionen
- Intelligentere Automatisierung und Wartung
- Erweiterte Unterstützung für Cloud- und Drittanbieterlösungen

RAZ-LEE iSecurity

iSecurity Suite (*BASE)

Einheitliches Lizenzierungsmodell

Eine zentrale Lizenzdatei für mehrere Produkte, unterstützt mehrere Lizenzen über verschiedene LPARs hinweg, CHKISA warnt rechtzeitig vor dem Ablauf von Lizenzen

RAZ-LEE

iSecurity Suite (*BASE)

- Die **Lizenzdatei** unterstützt Unternehmen, die mehrere Lizenzen verwalten. Lizenzen für mehrere Produkte auf derselben oder auf unterschiedlichen LPARs werden gemeinsam in einer einzigen Lizenzdatei ausgeliefert. Die zugehörigen Hilfsprogramme (siehe Base Support (89), Option 22 „Import Authorization“) wurden erweitert und bieten folgende Funktionen:
  - Automatisches Laden aller Lizenzen, die für die LPAR gelten, auf der der Befehl ausgeführt wird.
  - Laden einer einzelnen Produktlizenz.
- Der Befehl **Check Authorization (CHKISA)** warnt vor Produkten, deren Lizenz demnächst abläuft. Installierte, aber nicht lizenzierte Produkte werden dabei nun übersprungen.
- **Live Partition Mobility (LPM)** ermöglicht die Verlagerung der kompletten Arbeitslast einer aktiven LPAR auf ein anderes System oder eine andere LPAR – ohne Unterbrechung des laufenden Betriebs. Die automatische Lizenz-Zuordnung wurde entsprechend erweitert, sodass das Betriebssystem beim Verschieben einer LPAR die erforderlichen Lizenzänderungen automatisch durchführt. Die Erweiterung umfasst außerdem den Befehl Work with LPM (WRKISLPM), mit dem das automatische Hinzufügen, Entfernen und Prüfen von Lizenzen bei einer LPM-Übertragung verwaltet werden kann.
- **Watchdog** stellt sicher, dass alle wichtigen Produktkomponenten aktiv und betriebsbereit sind. Dazu gehören sowohl die Subsysteme als auch produktspezifische Komponenten. Wird ein Produkt oder eine Funktion über einen definierten Zeitraum als inaktiv erkannt, wird eine Warnung ausgelöst. Dabei können in regelmäßigen Abständen Nachrichten oder E-Mails versendet oder ein benutzerdefiniertes Programm aufgerufen werden.
- Work with **Collected Data** im Menü Base Support (89) zeigt jetzt zusätzlich die Größe der Journal Receiver sowie der für die Datensicherung bereitstehenden Daten an.

iSecurity
SIEM & DAM Support

Verbesserte SOC-Integration für schnellere Reaktionszeiten

Für jedes SIEM-System kann festgelegt werden, ob das Syslog-Format RFC 5424 oder RFC 3164 verwendet wird.

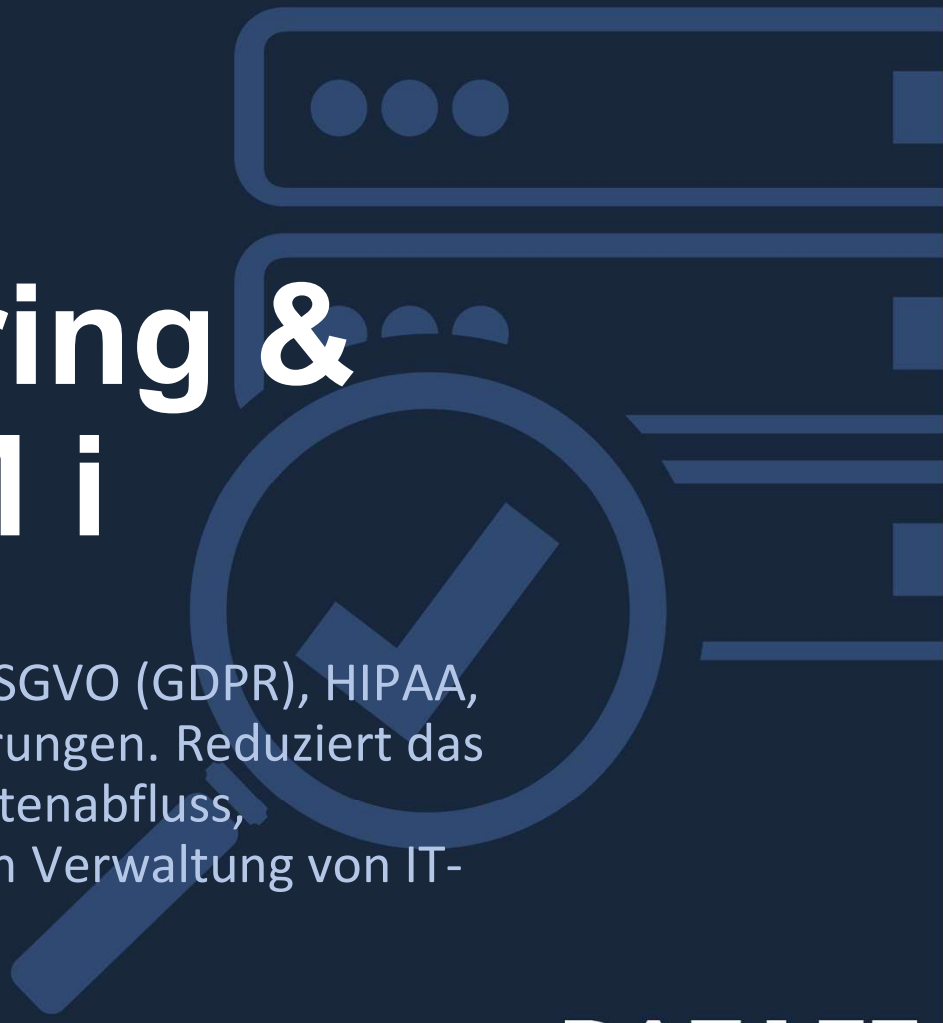
Die Standard-Schweregrade für jeden Ereignistyp und -untertyp wurden auf aussagekräftigere Standardwerte angepasst. Diese Änderung wirkt sich auf bestehende Installationen nur aus, wenn sie ausdrücklich übernommen wird.

RAZ-LEE

iSecurity
Audit

Auditing, Monitoring & Reporting für IBM i

iSecurity Audit unterstützt die Einhaltung von PCI, DSGVO (GDPR), HIPAA, NIS2, DORA, SOX und weiteren Compliance-Anforderungen. Reduziert das Risiko von Datenmanipulation, Datenverlust oder Datenabfluss, Serviceunterbrechungen sowie einer unzureichenden Verwaltung von IT-Systemen.



RAZ-LEE

iSecurity Audit

- Work with Queries (**STRAUD, 41**) bietet erweiterte Möglichkeiten zur Anzeige von Systeminformationen sowie verschiedener Systemwerte, Systemgrenzwerte und Statusinformationen.

- Die Unterstützung des Report Generators für die Trenderkennung von IBM-i-Systemgrenzwerten (Typ A#) wurde erweitert. Damit können Berichte zu mehr als 100 Trendtypen erstellt werden. Je Kategorie werden dabei die jeweils größten Werte pro Tag ausgewertet. Beispielsweise Datendateien mit der größten Größe oder Bibliotheken mit der höchsten Anzahl an Objekten.

- I Information Sources (STRAUD, Option 41, 2) unterstützt jetzt vollständig die speziellen internen Audit-Typen:
  - **A$** umfasst alle Audit-Typen, die sich auf Audit-Objekte beziehen. Angezeigt werden sämtliche Operationen an Objekten (z. B. Löschen, Erstellen usw.).
  - **A#** steht für sämtliche Audit-Typen.
  - **C@** kennzeichnet Änderungen an Benutzerprofilen.

- Große Sequenznummern von Journaleinträgen werden vollständig unterstützt.

- Im Rahmen der täglichen Wartung bleiben Journal Receiver erhalten, bis sie gesichert wurden.

- Bei Neuinstallationen werden nicht benötigte Jobplanungen nicht mehr eingerichtet.

- Bei vielen Befehlen, die benutzerdefinierte Elemente verwenden, zeigt F4=Eingabehilfe jetzt die tatsächlich verfügbaren Werte an und nicht mehr nur deren Namen..

- Die Berechtigungen für Produktobjekte wurden weiter verschärft.

iSecurity Audit

- Weitere Systeminformationen, beispielsweise Feldbeschreibungen des QAUDJRN oder Bezeichnungen von Grenzwerttypen, werden jetzt in der jeweiligen Landessprache angezeigt.
- Die Benutzerprofile SECURITY*P, die Eigentümer der Produktobjekte sind und die erforderlichen Berechtigungen bereitstellen, wurden überarbeitet. Dabei wurden die erforderlichen Sonderberechtigungen auf das notwendige Minimum reduziert. Die neue Einstellung gilt standardmäßig für Neuinstallationen und kann über eine Option im Menü Base Support (89) auch für bestehende Installationen übernommen werden.
  - **#A** Trendanalyse von Systemgrenzwerten. Beispiel: Warnung beim Erreichen der maximalen Anzahl von Membern
  - **#C** Informationen zu Group-PTFs – installiert bzw. verfügbar. Beispiel: Überblick über installierte und verfügbare Group-PTFs
  - **#D** Zertifikatsinformationen. Beispiel: Warnung vor dem Ablauf von Zertifikaten
  - **#E** Lizenzinformationen. Use case: Anzeige installierter und lizenzierter IBM-i-Produkte einschließlich Ablaufdatum der Lizenz
  - **#G** Informationen zu Group-PTFs. Beispiel: Anzeige nicht installierter PTF-Gruppen
  - **#H** PTF-Informationen. Beispiel: Anzeige angewendeter, geladener oder noch nicht geladener PTFs
  - **#K** NetStat-Informationen. Use case: NetStat-Verbindungen, Adressen, Portnamen und Verbindungstypen regelmäßig ausgeben oder in einer Datei speichern
  - **#L** NetStat-Schnittstellen. Use case: Netzwerkadressen, Verbindungs-typen, Subnetzmasken usw. anzeigen
  - **#M** Net Stat Routing Information. Use case: Routing-Ziele, Verbindungstypen und Subnetzmasken anzeigen
  - **#N** NetStat-Jobinformationen. Use case: Remote-Adressen, Portnamen usw. nach Job anzeigen
  - **#Q** TCP/IP-Informationen. Use case: Hostname, TCP/IP-Konfiguration und Adresstypen anzeigen
  - **#R** Aktuelle Serverinformationen. Use case: Servername, Betriebssystem und CPU-Anzahl anzeigen
  - **#S** Freigaben des Servers Use case: Freigaben, Pfade und erforderliche Berechtigungen anzeigen
  - **#U** Systemstatus. Use case: Anzahl aktiver Jobs, maximal zulässige Jobs usw. anzeigen
  - **#V** Informationen zu Speicherpools. Use case: Speicherpools, Größen und Thread-Anzahlen anzeigen
  - **#W** Aktive Jobs. Use case: Aktive Jobs mit Subsystem und Benutzerprofil anzeigen
  - **#X** Plattenstatus. Use case: Plattentypen sowie belegten und verfügbaren Speicherplatz anzeigen
  - **#Y** Ausgabewarteschlangen (Übersicht). Use case: Ausgabewarteschlangen, Status, Anzahl der Dateien und zugeordnete Drucker anzeigen

iSecurity
AP-Journal

AP-Journal-Container werden nicht ersetzt, wenn sie keine Daten enthalten.

Work with Collected Data im Menü Base Support (89) zeigt jetzt auch die Größe der einzelnen **AP-Journal-Anwendungen** an.

Der Mechanismus, mit dem **AP-Journal** eine Bibliothek für die zu sichernden Daten anlegt, wurde geändert. Eine Bibliothek wird jetzt nur noch erstellt, wenn tatsächlich Daten vorhanden sind.

RAZ-LEE

iSecurity
Firewall

Firewall wurde angepasst und unterstützt jetzt die tatsächliche IP-Adresse von Mapepire.

Der Befehl Delete Firewall Statistics (DLTFWSTT) wurde in die tägliche Wartung aufgenommen. Dadurch lässt sich die für Business-Intelligence-Auswertungen gespeicherte Datenmenge gezielt begrenzen.

SQL-Anweisungen vom Typ DECLARE und VALUES werden nicht mehr protokolliert, da sie keine sicherheitsrelevanten Informationen enthalten.

RAZ-LEE

iSecurity
Command

Steuerung und Überwachung der Befehlszeile

Es kann jetzt festgelegt werden, dass sich Benutzer vor der Ausführung eines Befehls zusätzlich per **MFA** authentifizieren müssen. Diese Funktion ergänzt die bereits vorhandene Freigabe per PIN oder Warnhinweis.

Wird ein Befehl von **COMMAND** abgewiesen, erscheint dies als *ESCAPE-Nachricht für den ursprünglichen Befehl im Joblog.

RAZ-LEE

iSecurity
Capture

Visual Track für Green-Screen-Benutzeraktivitäten auf IBM i

Der Zugriff auf eine aufgezeichnete Sitzung ist jetzt auch über die Jobnummer möglich – wahlweise **mit oder ohne** Jobname bzw. Benutzerprofil.

RAZ-LEE

iSecurity
Antivirus

Nativer Schutz für IBM i Server

Die erweiterte Bedrohungsschutz-Lösung zum Schutz von IFS-Dateien auf IBM i wurde um neue Funktionen ergänzt.

RAZ-LEE

iSecurity Antivirus

- Jedes SCANAV-Protokoll enthält den IBM-i-Befehl einschließlich der verwendeten Parameter. Ideal für Audits und die Nachvollziehbarkeit von Scanvorgängen.
- Wird ein Scan nicht ordnungsgemäß beendet, enthält das Protokoll zusätzlich die zuletzt geprüfte Datei. So sehen Sie sofort, an welcher Stelle der Scan unterbrochen wurde.
- Eine neue Funktion ermöglicht es, den Scan genau an dieser Stelle fortzusetzen. Dabei werden dieselben Parameter verwendet – das spart Zeit.
- Das ist besonders hilfreich, da SCANAV auch bei On-Demand-Scans (Batch) die Funktion *ONLYNEW(YES) unterstützt. Damit steht die von IBM für On-Access-Scans bekannte Funktionalität jetzt auch für On-Demand-Scans zur Verfügung.

RAZ-LEE iSecurity

iSecurity
Anti-Ransomware

Schutz der IBM i von innen heraus

Asynchrone Verarbeitung sorgt für sofortige Reaktionszeiten und ermöglicht gleichzeitig umfassendere Sicherheitsprüfungen.

RAZ-LEE

iSecurity
Multi Factor Authentication

Unsere MFA-Lösung basiert auf dem Konzept von Personen!

„Eine einzige Maßnahme kann 99,9 % aller Angriffe auf Ihre Benutzerkonten verhindern.“

Melanie Maynes, Director of Product Marketing,
Microsoft Security

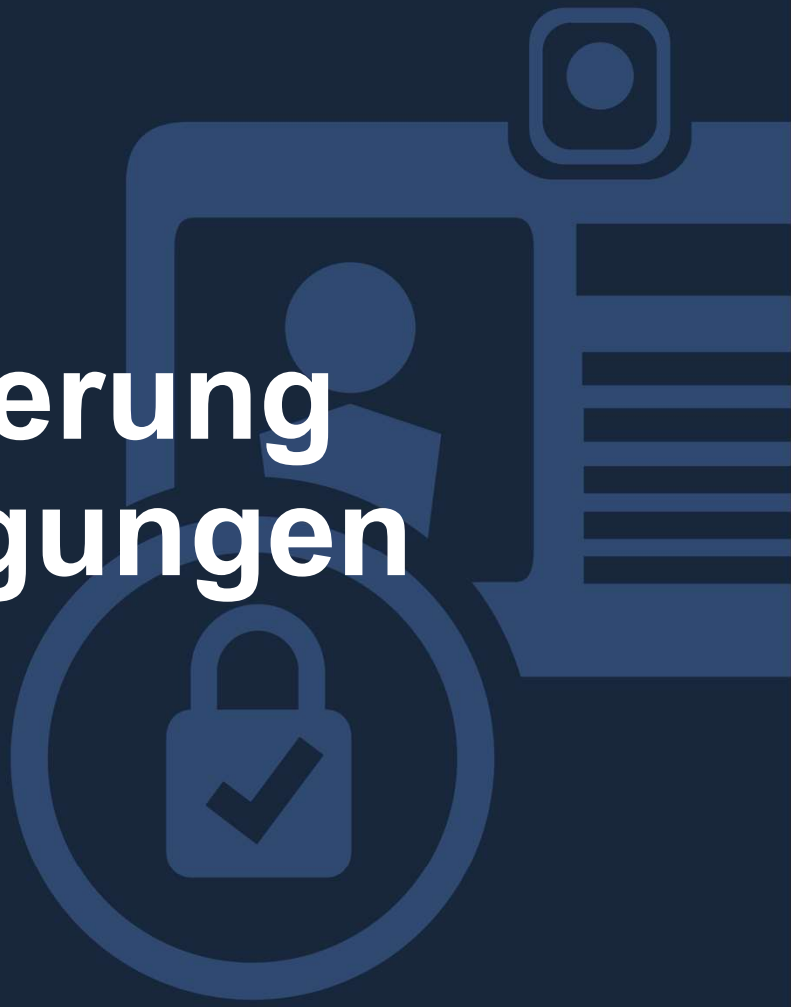
RAZ-LEE

iSecurity MFA

- MFA-Unterstützung für beliebige Web- und **Desktop-Anwendungen von Drittanbietern** hinzugefügt, einschließlich der **iSecurity GUI.**
- MFA unterstützt jetzt neben **Microsoft Entra ID** auch **OKTA, DUO, PingID, Google** und weitere Identitätsanbieter.
- Unterstützung des neuen **MFA-Exit-Points** in IBM i 7.6. Kunden mit IBM i 7.6 können den IBM-Exit-Point verwenden oder ihre bisherige Konfiguration beibehalten.
- Die **TOTP**-Konfiguration lässt sich jetzt an die Sicherheitsrichtlinien des Unternehmens anpassen, einschließlich des geheimen **TOTP-Schlüssels** und der Notfall-Tokens. Die Einstellungen befinden sich in Option 81.
- Der Befehl **GETMFA** wurde um den Parameter ***MFA(CHECK)** erweitert. Schlägt die **MFA-**Prüfung fehl, wird eine *ESCAPE-Nachricht ausgegeben. Dadurch lässt sich vor sicherheitskritischen Operationen eine MFA-Prüfung durchführen. Die konfigurierte Safe Time nach einer erfolgreichen Authentifizierung wird dabei berücksichtigt.
- Eine neue API ermöglicht die programmgesteuerte Prüfung, ob sich eine Sitzung innerhalb der Safe Time befindet. Hierzu dient die **API MFCHECKR**, die den **MFA**-Status anhand von Benutzer und IP-Adresse ermittelt. Dadurch können Web- und GUI-Anwendungen **MFA** nur dann anfordern, wenn dies tatsächlich erforderlich ist. Rückgabewerte:
  - *NOMFA – keine MFA erforderlich
  - *MFAREQ – MFA erforderlich
  - *MFAACTmm – verbleibende Safe Time in Minuten
  - *REJECT – Aktion abgelehnt
- Der Schutz von Freigaben wurde erweitert. Hierfür kann jetzt eine separate Safe Time verwendet werden.
- Personen und die zugehörigen **Benutzerprofile** können jetzt auch über Befehle angelegt, geändert und gelöscht werden. Dadurch lässt sich eine große Anzahl von Benutzern komfortabel per Batch oder Skript bereitstellen – eine Vorgehensweise, die viele Kunden bevorzugen. Verfügbar sind Befehle zum Anlegen einer Person, zum Hinzufügen bzw. Entfernen von Benutzerprofilen, für die MFA-Konfiguration einer Person, zum Versand der geheimen Informationen sowie zum Löschen einer Person.

iSecurity
Authority on Demand

RegeIn für die Anforderung zusätzlicher Berechtigungen



Die Verwendung des Befehls **GETAOD** (Get Authority On Demand) kann jetzt zusätzlich durch **MFA** mittels **OTP** oder **TOTP** abgesichert werden.

RAZ-LEE

iSecurity
Password Reset

Self Service & Mobile

Benutzeraktionen und Identitäten können zusätzlich durch **MFA** verifiziert werden.

RAZ-LEE

Ihr Mehrwert auf einen Blick

Wir kümmern uns um unsere Kunden – unabhängig von ihrer Unternehmensgröße.

Raz-Lee-Kunden weltweit

Zu unseren internationalen Kunden zählen unter anderem:

- AIG Insurance
- AXA Insurance
- Banco de Ciudad
- Comarch
- Costco
- CHCS
- Euronet
- First American Bank
- Fiserv
- Hollywood Casino
- Svenska Handelsbanken
- Leumi Bank
- Leaseplan
- Michael Kors
- Migdal
- Mitsubishi Motors
- MUFG
- OCBC Bank
- Office Depot
- Penn National Gaming
- Santander Bank
- Steve Maden
- Tieto
- Vermont

und viele weitere Unternehmen….

iSecurity Suite in der Übersicht

Cyber Protection

- **Anti-Ransomware**
- **Antivirus** / Schutz gegen Malware
  - **ICAP** Optional Client/Server for Antivirus
  - **Antivirus für AIX**
  - **Orchestrator für AIX**

Authentifizierung & Autorisierung

- **MFA** Multi Factor Authentifizierung
- Self **Password Reset**
- **Authority On Demand**

Netzwerk-Schutz

- **Firewall** FTP, ODBC…access
- Monitor CL **Commands**
- **Safe-Update - S**chutz von Produktionsdateien

Auswertung, Reporting und Warnmeldungen

SIEM & DAM Support

Syslog, SNMP, CEF, LEEF

Visualizer

Business Intelligence für IT-Sicherheit

Score Cards

for GDPR, NIS2, SOX, PCI, HIPAA…

Security Investigator

Data Discovery, Authority Inspector, Sicherheitsbewertung

Verschlüsselung

- DB2 **Feld-Verschlüsselung** (FIELDPROC)
- **Open PGP Datei-Verschlüsselung**

Datenbanklösungen

- **AP-Journal** DB Audit, Filter, Alerts, SIEM
- **DB-Gate** Native SQL to Oracle, MSSQL…
- **FileScope** Sicherer Datei-Editor

Auditierung & Reaktion

- **Audit** QAUDJRN, Systemwerte, Systemstatus
- Proactive re-**Action** in real time
- **Capture:** Aufzeichnung von Bildschirmaktivitäten
- **Compliance** für Benutzer, Objekte und das IFS
- **Change Tracker** wüberwachung von Produktionsbibliotheken

RAZ-LEE iSecurity

Was Raz-Lee auszeichnet

Was macht Raz-Lee so besonders – und welchen Mehrwert bietet das für unsere Kunden?

- Die **iSecurity Suite** ist als integrierte Gesamtlösung konzipiert – mit einheitlicher Terminologie und durchgängigen Arbeitsabläufen.
- Alle **Raz-Lee-Lösungen** wurden vollständig nativ für IBM i entwickelt.
- Als **Softwarehersteller** entwickeln wir unsere Lösungen kontinuierlich weiter und stellen regelmäßig Updates bereit.
- Unsere Kunden profitieren weltweit von **direktem technischem Support** durch Raz-Lee.

RAZ-LEE

Kontaktieren Sie uns, wenn Sie mehr über unsere Produkte wissen möchten!

E-Mail:

info@razlee.de

Website:

www.razlee.de