



beta systems



Garancy® Suite

Stärken Sie die Cyberhygiene Ihrer Organisation mit Identity Access Management

Garancy bildet die erste Verteidigungslinie

Die Notwendigkeit einer ordnungsgemäßen Berechtigungsverwaltung und die Beschränkung der Zugriffsrechte auf ein erforderliches Minimum für die jeweilige Rolle werden immer wichtiger. Daher sollte Identity Access Management (IAM) auf der Agenda eines jeden IT Security Managers stehen.

Mit Garancy, der IAM-Lösung von Beta Systems, steuern und überwachen Unternehmen den Zugriff auf Daten und Anwendungen gemäß den individuellen organisatorischen Anforderungen und fachlichen Rolle eines jeden Benutzers.

” Insider-Attacken verursachen 200 % mehr Schaden im Vergleich zu externen Angriffen.

Quelle: Carnegie Mellon University

Fakten-Check

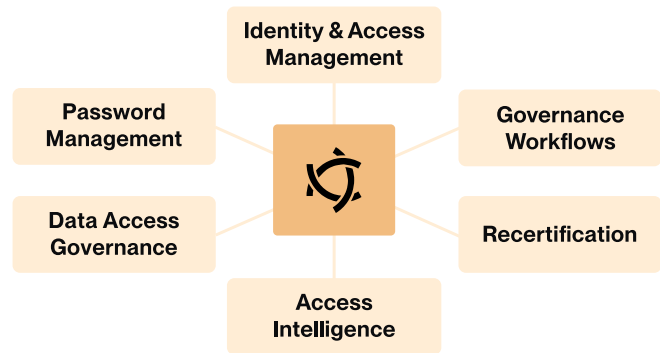
- Cyberangriffe auf Unternehmen nehmen weiter zu.
- Weltweit werden mehr als 42,8 Mio. Angriffe pro Jahr registriert – das sind 9 Attacken pro Sekunde.
- 60 % aller Sicherheitsvorfälle gehen auf Insider zurück.
- Insider-Attacken verursachen bis zu 200 % mehr Schaden als externe Angriffe.
- Viele Unternehmen unterschätzen noch immer das potenzielle Risiko innerhalb der Organisation.

Module der Garancy Suite

Die Garancy Module bedienen alle Aufgaben der Identity Access Governance und sind sowohl On-Premise als auch in der Cloud verfügbar.

IAM als Brücke zwischen Business und Security

Das Provisioning Modul ermöglicht die zentrale Administration und Steuerung aller Berechtigungsinformationen der Anwender (Identitäten, Gruppen, Rollen) in sämtlichen IT-Systemen:



Provisioning

- Anbindung und Steuerung von IT-Applikationen durch eine große Auswahl von Out-of-the-Box-Konnektoren
- Flexibler und hochskalierbarer Abgleich des Identity Managements mit den anzubindenden Zielsystemen
- Bereitstellung, Konsolidierung und Abgleich von Zugriffsrechten
- Umsetzung von Änderungen in Echtzeit

Access Governance

- Role Lifecycle Management mit Rollen-Hierarchien
- Automatische Zuordnung zu Rollen je nach identifiziertem Benutzerprofil
- Durchsetzung von SoD-Regeln (Segregation of Duties)
- Steuerung der Autorisierung basierend auf Rollen und internen IT-Sicherheitsrichtlinien

User Management

- Automatischer Import von HR-Daten
- Unterstützung des gesamten Mitarbeiter-Lifecycles (Joiner, Mover, Leaver)
- Differenzierung zwischen unterschiedlichen Benutzertypen, z. B. interne und externe Mitarbeitende

Audit und Security

- Festlegung von Audit-Prüfungen für zugewiesene Zugriffsrechte
- Single Point of Information und Durchsetzung von Zugriffsrichtlinien
- Unabhängige Verwaltung mehrerer Objekte über eine zentrale IAM-Plattform

Einbindung der Fachabteilungen durch Governance Workflows

Durch Governance Workflows innerhalb von Garancy können Kunden ihre Prozesse digital gestalten und alle Prozesse, die in Verbindung mit Zugriffsrechten stehen, beschleunigen.

Sie binden Fachabteilungen direkt ein und stellen gleichzeitig sicher, dass die IT-Sicherheitsrichtlinien eingehalten werden und zugewiesene Berechtigungen rückverfolgbar und auditierbar sind.

Die Verantwortung für die Verwaltung der Zugriffsrechte liegt in den Fachabteilungen.

- Verkürzte Bearbeitungszeiten für Zugriffs-freigaben
- Lückenlose Nachvollziehbarkeit für die Vergabe von Zugangsberechtigungen
- Erhöhte Nutzerzufriedenheit, da sie unmittelbar die benötigten Zugriffe erhalten
- Einhaltung der Compliance-Vorgaben hinsichtlich regulatorischer Vorschriften und Standards
- Entlastung von IT-Administratoren durch die Einbindung von Fachabteilungen
- Verkürzte Durchlaufzeiten aller Antragsprozesse

Rezertifizierung von Zugriffsrechten – Kontrolle ist besser als Vertrauen

Mit der webbasierten Portal-Lösung für die effiziente Rezertifizierung von Zugriffsrechten können die Berechtigungen für interne und externe Benutzer zentral vergeben, überprüft oder entzogen werden.

Dies erhöht die Sicherheit und verbessert die Genauigkeit der Berechtigungsvergabe.

- Rezertifizierungskampagnen basierend auf Organisationen, Aufgabenprofilen und Risikobewertungen
- Substitution und Delegation über Workflows
- Verschiedene Ansichts-Modi, wie z. B. Single-User-Ansicht, Gruppenübersicht und SoD-Verletzungen
- Rezertifizierungsstatus jederzeit einsehbar – inklusive Details wie Fälligkeit, entzogene und bestätigte Berechtigungen
- Schnellrezertifizierung und automatische Out-of-the-Box-Deprovisionierung
- Auditierbare Kampagnen mit vollständiger Ereignisprotokollierung und Archivierung
- Optimierte für Desktopnutzung und mobiles Arbeiten mit Tablet oder Mobilgeräten

Name	Begrenzt bis	Gesperrt	Job-Funktion	SoD-Klasse	Userkategorie	Vertragslaufz...	Organisationseinheit	Meine Verantwortung			
Charlotte Barber			Key Account Manager	Markt	Mitarbeiter		Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	13	4	
Debbie Bates			Account Manager	Markt	Partner	3/28/25	Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	10	5	
Evangelina Black			Account Manager	Markt	Partner	3/28/25	Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	8	5	
Irene Bourne			Account Manager	Markt			Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	12	3	
Iva Bowden			Account Manager	Markt			Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	10	5	
Janet Bowman			Account Manager	Markt			Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	9	5	
Jerald Broderick			Account Manager	Markt			Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	10	5	
Jeremy King			Key Account Manager	Markt			Casualty Dir. Sal...	Disziplinarischer Vorgesetzter, Orga...	12	6	

Grafik 1 – Übersicht der Mitarbeitenden

Sicheres Password Management

Das Password Management dient dem sicheren und einfachen Zugriff von Computern auf verschiedene IT-Plattformen oder Anwendungen in verteilten Systemen. Es vereinfacht die Durchsetzung der IT-Sicherheitsrichtlinien, die mit Passwörtern verbunden sind.

Password Reset ermöglicht es den Anwendern, webbasiert Passwörter selbst zurückzusetzen und zu ändern. Dies führt zu einer spürbaren Entlastung des Helpdesk und steigert die Produktivität der Nutzer aufgrund kürzerer Unterbrechungszeiten.

Password Synchronisation ermöglicht Mitarbeitenden den Zugriff auf verschiedene Plattformen und Anwendungen mit nur einem einzigen Passwort. Passwortänderungen werden automatisch in allen angebundenen Systemen synchronisiert und stehen dem Nutzer systemübergreifend zur Verfügung.

Reporting und Analytics mit Access Intelligence

Das Access Intelligence Modul nutzt Business Intelligence, um Zugriffsrechte zu verwalten. Die Lösung bietet Berichte und multidimensionale Analysen für die Prüfung von Berechtigungsstrukturen im Unternehmen und die Identifizierung potenzieller Berechtigungsrisiken.

- 360-Grad-Monitoring: Übersicht über Zugriffsrechte und damit verbundene Risiken
- Intuitive Dashboards liefern einen vollständigen Überblick über Security-Indikatoren
- Geschäftsorientierte, einfach zu bedienende Reporting- und Audit-Tools für Out-of-the-Box-Analysen oder kundenspezifische Reportings
- Dynamische Historisierung: Alle Änderungen werden sofort erkannt und sind lückenlos nachvollziehbar
- Schnelle Korrektur von Autorisierungsfehlern oder Sicherheitslücken
- Sicherere Zugriffskontrolle und verbesserte Governance auf Faktenbasis

Management unstrukturierter Daten mit Data Access Governance

Die Menge unstrukturierter Daten – etwa Tabellen, Dokumente, Präsentationen oder E-Mails – wächst rasant. Neben klassischen IAM-Lösungen ist ein strukturiertes Berechtigungsmanagement daher unerlässlich.

Data Access Governance bietet ein spezialisiertes Modul zur Steuerung und Kontrolle von Zugriffsrechten auf unstrukturierte Daten. Vollständig in Garancy integriert, entlastet es den Helpdesk und sorgt für mehr Transparenz.

- Dateneigentümer verwalten Zugriffe eigenständig und ohne direkte IT-Beteiligung
- Integrierte Compliance-Checks unter Einbindung der Fachbereiche
- Automatische Umsetzung interner Richtlinien und gesetzlicher Vorgaben
- Regelkonforme Rechtevergabe über geschäftsorientierte Antrags- und Freigabeprozesse
- Soll-Ist-Rechteabgleich deckt kritische Abweichungen sofort auf
- Garancy als Single Point of Administration – auch als portalbasierte Stand-Alone-Lösung verfügbar

Bereit für den nächsten Schritt?

Kontaktieren Sie uns, um mehr über unsere IAM-Lösung zu erfahren – wir freuen uns auf Ihre Anfrage.

Schreiben Sie uns eine E-Mail an **info-iam@betasystems.com** oder melden Sie sich telefonisch unter **+49 (0) 30 726 118-0**.



www.betasystems.com/de/produkte/garancy