

Lösungsübersicht

Gewährleistung kontinuierlicher Compliance mit EZB-Mandaten für Netzwerksicherheit im Open-Banking

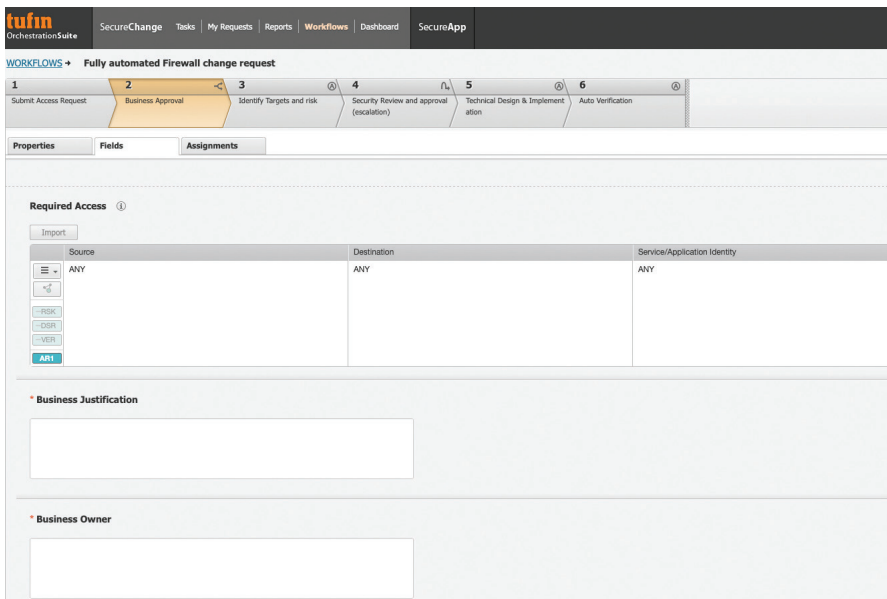
Die Anforderungen für Netzwerksicherheit der EZB für Open Banking oder die revidierte Zahlungsdienstleisterlinie (PSD2) fordern von Finanzinstituten der EU höhere Standards im Hinblick auf ihre Dokumentationsprozesse. Bei einem EZB-Audit müssen Finanzinstitutionen sämtliche Zugriffsregeln rechtfertigen; Zugriff mit geringsten Rechten garantieren; Aufgabentrennung gewährleisten und professionelle, dokumentierte und überprüfbare Prozesse für das Management des Netzwerkzugriffs einführen. Die Rezertifizierung von Compliance-Anforderungen muss innerhalb von 180 Tagen demonstriert werden.

Tufin ist die erste Wahl für Finanzinstitutionen (FI) in ganz Europa und darüber hinaus mit über 700 FI-Kunden weltweit. Kunden vertrauen in Tufin, wenn es um die Transparenz und Kontrolle ihrer Netzwerksicherheit geht. Wir unterstützen unsere Kunden, indem wir im Hinblick auf Compliance mit den EZB-Anforderungen für Netzwerksicherheit eine einzige, zentralisierte Lösung anbieten, die die gesamte Multi-Anbieter- und Multi-Plattform-Umgebung umfasst.

Geschäftliche Rechtfertigung und Inhaber aller Zugriffsregeln

Die EZB möchte sicherstellen, dass der Zugriff auf Anwendungen sowie der Netzwerkzugriff gerechtfertigt und ordnungsgemäß umgesetzt ist. Organisationen müssen ein Verzeichnis ihrer Zugriffsanfragen vorweisen, und dass jede Anfrage über einen Geschäftsinhaber sowie betrieblich gerechtfertigt werden kann. Darüber hinaus benötigen Unternehmen Transparenz darüber, wie Zugriffsanforderungen Firewallregeln sowie den Regeln auf Objektebene zugeordnet sind. Sie müssen wissen, dass die Regeln den Sicherheitsstandards des Unternehmens entsprechen und dass der Zugriff ordnungsgemäß umgesetzt wird.

Tufin bietet einen anwendungsorientierten Ansatz zum Definieren, Identifizieren, Bereitstellen, Dokumentieren und Verwalten des Netzwerkzugriffs. Die Tufin Orchestration Suite ermöglicht die Modellierung von Konnektivität und



The screenshot displays the Tufin SecureChange interface. At the top, there's a navigation bar with tabs: SecureChange, Tasks, My Requests, Reports, Workflows, Dashboard, and SecureApp. Below this, a section titled 'WORKFLOWS' shows a 'Fully automated Firewall change request' workflow. The workflow consists of six steps: 1. Submit Access Request, 2. Business Approval, 3. Identify Targets and risk, 4. Security Review and approval (escalation), 5. Technical Design & Implementation, and 6. Auto Verification. Below the workflow, there are tabs for Properties, Fields, and Assignments. The 'Required Access' section shows a table with columns for Source, Destination, and Service/Application Identity, all set to 'ANY'. There are also sections for 'Business Justification' and 'Business Owner' with input fields.

Der Screenshot von Tufins SecureChange zeigt den Workflow für die Bereitstellung einer Zugriffsänderung. Das Workflow gewährleistet EZB-Compliance, da die Genehmigung der geschäftlichen Rechtfertigung und des Inhabers erforderlich ist. Dies ist ein „standardisierter und reproduzierbarer“ Prozess, der mit vollständiger Dokumentation bzw. Audit-Trail nicht kompromittiert oder umgangen werden kann.



Vorteile für Ihr Unternehmen:

- Gewährleistung kontinuierlicher Compliance mit EZB-Mandaten für Netzwerksicherheit
- Vereinfachtes Management mit dem Prinzip der geringsten Rechte und segmentiertem Zugriff durch Visualisierung, Regelübersetzung auf Anwendungs- und Geräteebe sowie vollständige Netzwerktopologie über das gesamte Multi-Anbieter-Netzwerk
- Anpassbarer und im Ticketsystem integrierter Workflow für das Ändern von Sicherheitsrichtlinien
- Dokumentation der Konnektivität über eine zentrale Konsole
- Automatisierter Workflow zur Rezertifizierung
- Zentralisierte Transparenz und Kontrolle des Netzwerkzugriffs über Anbieter und Plattformen

die Visualisierung der Zugriffsregeln, die jeder Anwendung zugeordnet sind. Automatisierte Workflows bieten vollständige Dokumentierung von Zugriffsanfragen, der geschäftlichen Rechtfertigung und der Inhaber. Dies kann durch automatisierte Bereitstellung automatisch umgesetzt und auf kontinuierliche Compliance überprüft werden. Da jeder einzelne Schritt im Workflow dokumentiert wird, ist ständige Audit-Bereitschaft gewährleistet.

Zugriffskontrolle mit geringsten Rechten und Aufgabenteilung

Die EZB möchte sicherzustellen, dass Unternehmen über geeignete Sicherheitslösungen verfügen, um Netzwerke vor Missbrauch oder Angriffen zu schützen. Der Netzwerkzugriff muss nach dem Prinzip der „geringsten Rechte“ auf ein striktes Minimum beschränkt werden. Zugriff ist auf Systeme, Anwendungen und Benutzer beschränkt, die diesen aus geschäftlicher Sicht benötigen. Darüber hinaus müssen Unternehmen Aufgaben trennen und auf die Segmentierung von IT-Umgebungen achten. Tufins granulare, rollenbasierte Ressourcen für Zugriffskontrolle ermöglichen es Unternehmen, Aufgabenteilung in Zusammenhang mit Anfragen, Genehmigung, Design, Verwaltung und Bereitstellung des Zugriffs durchzusetzen. Tufin vereinfacht die Visualisierung und Verwaltung der Aufgabenteilung bis ins Detail. Die Aufteilung in Zonen ermöglicht es Unternehmen, Netzwerkzonen zu bestimmen, die miteinander verbinden und den Netzwerkverkehr zulassen oder blockieren. Netzwerkzugriff mit geringsten Rechten wird erzielt, indem man Zugriff auf Ressourcen, Anwendungen und Benutzer beschränkt, die diesen aus geschäftlicher Sicht benötigen.

Manipulationssichere Rezertifizierung

Die bisher akzeptable manuelle Verwaltung des Netzwerkzugriffs, oft mit Tabellenkalkulationen und E-Mail, ist ungenau, nicht skalierbar und entspricht nicht mehr den EZB-Richtlinien. Der Netzwerkzugriff muss von Unternehmen mit professionellen, wiederholbaren und prüfbar Prozessen verwaltet werden. Zudem ist ein effektiver Prozess zur Rezertifizierung des Zugriffs erforderlich, und ggf. einer der den Zugriff alle 180 Tage entziehen kann. Zu einem solchen Prozess gehören Regelrechtfertigung, Rezertifizierungsdatum, Freigabegenehmigung und ein manipulationssicherem Audit-Trail. Finanzinstitute, die den Richtlinien der EZB nicht nachkommen, müssen einen Korrekturplan vorlegen, in dem sie zeigen, wie sie die Richtlinien in naher Zukunft erfüllen. Anderenfalls riskieren sie schwere Strafen, bis hin zum Herunterfahren einer Anwendung bis diese konform ist. Tufin bietet einen automatisierten, richtlinienbasierten Regelprüfungsprozess mit einsatzbarem Workflow für E-Zertifizierung, damit Kunden die Rezertifizierung des Zugriffs alle 180 Tage (oder beliebig häufig) durchsetzen können. Dieser Prozess bietet Compliance-Warnungen und einen Workflow zur Überprüfung, Genehmigung und ggf. zum Entzug des Zugriffs. Ein Zugriffsentzug führt möglicherweise direkt zu einem automatisierten, dokumentierten Prozess zum Außerkraftsetzen der Regel. Tufin automatisiert die Identifizierung riskanter, undokumentierter Regeln und dokumentiert den erforderlichen Zugriff sowie die Rechtfertigung, den Status und die Einhaltung der Standards. Compliance kann mit vollständigem Audit-Trail schnell und einfach nachgewiesen werden.

Tufins Multi-Anbieter-Plattform beinhaltet:

Netzwerk- und Cloud-Plattformen



Lösungsintegrationen



Die einzige Komplettlösung, die Audit-Bereitschaft für EZB-Netzwerksicherheit bietet

Die Tufin Orchestration Suite lässt sich zusammen mit dem Netzwerk skalieren und gewährleistet Compliance. Heutzutage kann Compliance im Netzwerk jederzeit einfach nachgewiesen werden sowie im zunehmend komplexeren Netzwerk der Zukunft. Tufin hilft Unternehmen nicht nur bei der Einhaltung der EZB-Richtlinien, wir unterstützen Sie auch, das Risiko der Netzwerkrichtlinien zu mindern und zu verwalten, die Umsetzung von Zugriffsanfragen von Tagen auf Minuten zu reduzieren und die Produktivität Ihres Teams zu erhöhen. Darüber hinaus verbessern wir den allgemeinen Sicherheitsstatus – und das bei maximaler Unternehmensagilität. Über 2300 der weltweit größten Unternehmen vertrauen auf Tufin, wenn es um die Automatisierung ihrer Sicherheitsrichtlinien über komplexe hybride Umgebungen geht. Gewinnen Sie Vertrauen, Transparenz und Compliance für Ihren Sicherheitsstatus.

Tufin (NYSE: TUFN) vereinfacht das Management einiger der größten und komplexesten Netzwerke der Welt, die aus tausenden von Firewall- und Netzwerkvorrichtungen bestehen sowie das entstehender hybrider Cloud-Infrastrukturen. Unternehmen wählen die Tufin Orchestration Suite™, um im Angesicht sich ständig ändernder Unternehmensanforderungen flexibel zu bleiben und einen robusten Sicherheitsstatus zu bewahren. Die Tufin Orchestration Suite reduziert die Angriffsfläche und sorgt für mehr Transparenz, um sichere und zuverlässige Anwendungskonnektivität zu gewährleisten. Tufin zählt seit der Unternehmensgründung über 2000 Kunden. Durch die Automatisierung der Netzwerksicherheit von Tufin können Unternehmen Änderungen in Minuten statt Tagen umsetzen. Gleichzeitig verbessern sie ihren Sicherheitsstatus und die Unternehmensagilität. Erfahren Sie mehr unter www.tufin.com.

¹ <https://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf>

² Die Häufigkeit wird in den Richtlinien nicht ausdrücklich festgelegt. Wirtschaftsprüfungsunternehmen empfehlen in der Regel 180 Tage.