



NEXTLABS

**Wie man Finanz- und Kundendaten mit
dynamischer Datenanonymisierung
und -trennung schützt**

fiserv.

Fallstudie der NextLabs Zero Trust Data Security Suite

Seit seiner Gründung im Jahr 1984 hat sich Fiserv zu einem führenden globalen Fintech-Unternehmen mit Hauptsitz in Wisconsin, USA, entwickelt. Fiserv wurde von der Aite Group als einer der „Best in Class“-Anbieter für Kernbanken anerkannt und bietet Kunden in verschiedenen Sektoren eine hervorragende API-fähige Integration, ein reaktionsschnelles Design und eine einheitliche Benutzererfahrung. Die innovativen Lösungen von Aite Group in den Bereichen Zahlungsverkehr, Verarbeitung, Risiko- und Compliance-Management sowie Kunden- und Vertriebskanalmanagement haben Tausenden von Finanzinstituten, darunter Banken, Kreditgenossenschaften und Leasinggesellschaften, sowie Millionen von Unternehmen in über 100 Ländern dabei geholfen, Geld effizient zu bewegen und ihre Finanzmanagementpraktiken zu verbessern, um dauerhaft erfolgreich zu sein.



Mit der Zunahme virtueller, globaler Arbeitsgruppen und immer strengeren Anforderungen an die Cybersicherheit steht Fiserv vor der Herausforderung, vertrauliche Informationen wie Kunden- und Finanzdaten sicher zusammenzuarbeiten und auszutauschen und gleichzeitig Flexibilität und Kostenkontrolle zu bewahren. Um die Vertraulichkeit und Integrität seiner Datenbestände zu schützen, implementierte Fiserv die Zero-trust Data Security Suite von NextLabs, die dynamische Sicherheitskontrollen auf Datenebene und eine feinkörnige Datenzugriffssteuerung in Echtzeit bietet. Dieser dynamische Ansatz ermöglicht es Fiserv, die Sicherheits- und Compliance-Verwaltung zu automatisieren, sensible Daten in einer einzigen globalen Instanz zu isolieren und dabei die geschäftliche Agilität inmitten sich entwickelnder Anforderungen aufrechtzuerhalten.



Innerhalb von vier Monaten hat das Global Fintech, Analytics & Digital Transformation Team von Fiserv eng mit dem Team von NextLabs zusammengearbeitet, um NextLabs' Data Access Enforcer (DAE) erfolgreich zu implementieren. Die Lösung ermöglicht dynamische Sicherheitskontrollen auf Datenebene, wie z.B. Verschlüsselung, Entschlüsselung, Maskierung und Trennung, um die Cybersicherheit von Fiserv für sein Ziel der digitalen Transformation zu verbessern. Mit diesem datenzentrierten Zero-Trust-Ansatz unter Verwendung von DAE werden die sensiblen Kunden- und Finanzdaten von Fiserv in einem nicht von Menschen lesbaren Format auf Datenbankebene verschlüsselt, wodurch verhindert wird, dass die Datenbestände und Backups kompromittiert werden oder autorisierte Benutzer darauf zugreifen können. Dies bietet einen zusätzlichen Schutzschild über heterogene Anwendungen und Systeme hinweg, um die Daten im Ruhezustand und während der Nutzung jederzeit sicher zu halten.



„Wir waren in der Lage, die NextLabs Data Security Suite für SAP S4/HANA innerhalb von vier Monaten in unserer Organisation zu implementieren“, sagte Roopa Prakash, Sr. Direktorin für digitale Transformation im Bereich FinTech bei Fiserv. „NextLabs hat hervorragende Arbeit in der Zusammenarbeit mit unserem SAP S4/HANA Fintech-Team geleistet. Ihre Teammitglieder waren reaktionsschnell, sachkundig und haben sich über ihre Pflichten hinaus engagiert, um die Dinge zu erledigen und gleichzeitig alle unsere Projektziele zu erreichen“, sagte Rajan Ray-Chaudhury, Sr. Director of Fin Tech Digital Transformation bei Fiserv.



fiserv.

Brookfield, Wisconsin

Industrie

IT-Dienstleistungen und IT-Beratung

Produkte und Dienstleistungen

Lösungen für Kontoverarbeitung, Rechnungssteller, Karten, Geldautomaten, Kredit- und Debitkarten, Einlagen, Kreditvergabe, Ausgabe, Überweisungen und Credit Union-Plattformen

Mitarbeiter

41,000

Einnahmen

\$22.5 Billion (USD)

Lösung

NextLabs Data Access Enforcer (DAE)

Wie man Finanz- und Kundendaten mit dynamischen Sicherheitskontrollen auf Datenebene schützt

Vorher: Herausforderungen und Chancen

- Verhinderung des unbefugten Zugriffs auf vertrauliche Daten und deren Verletzung, die zu Compliance-Problemen und Rufschädigung führen kann.
- Effizienter Schutz wichtiger Kundendaten eines Kundenstamms von Finanzinstituten, Banken, Hypothekenanbietern usw.
- Persönlich identifizierbare Informationen (PII) und die Einhaltung der Payment Card Industry (PCI) erforderten einen verbesserten Schutz vor unbefugtem Zugriff und Verwendung.
- Das S/4 HANA-System von Fiserv erforderte zusätzliche Sicherheitskontrollen, um die Cybersicherheitsanforderungen in Bezug auf den Datenschutz zu erfüllen.
- Diese Anforderungen bieten die Gelegenheit, dynamische Datenmaskierung und Verschlüsselung als ganzheitlichen, leistungsstarken Ansatz für SAP-Ökosystemanwendungen zu betrachten.

Warum NextLabs

- Erstklassige Zero Trust Data Centric Security-Lösung.
- Bietet Out-of-the-Box-Unterstützung für zahlreiche führende Unternehmens- und Cloud-Anwendungen wie SAP ERP, SAP BW, SAP S4/HANA, Microsoft Power BI und Azure Data Lake.
- Expertise in ERP, Big-Data-Anwendungen und Erfahrung in der Implementierung von groß angelegten Data-Governance-, Risiko- und Compliance-Lösungen.
- Bietet Datenmaskierung, Datenverschlüsselung und dynamische Autorisierung von Geschäftstransaktionen, um die Einhaltung von Vorschriften zu gewährleisten.
- Kann nahtlos integriert und innerhalb weniger Wochen implementiert werden, so dass Fiserv alle Projektziele erfolgreich erfüllen und gleichzeitig eine optimale Sicherheitsabdeckung gewährleisten kann.

Nach: Wertorientierte Ergebnisse

- Implementierung der NextLabs DAE-Verschlüsselung im S/4 HANA-System, um die von der Cyber Security Group innerhalb von Fiserv festgelegten Compliance-Anforderungen zu gewährleisten und zu rationalisieren.
- Schutz sensibler Kundendaten im Ruhezustand durch Verschlüsselung, Sicherung des Datenzugriffs durch Segregation und Verschleierung und Durchsetzung der Zugriffskontrolle auf Applikationen mit geringsten Rechten.
- Automatisiertes und vereinfachtes Sicherheitsmanagement zum Schutz vertraulicher Informationen.
- Zentrale Protokollierung und Nachverfolgung aller Datenzugriffsaktivitäten für Audit- und Compliance-Berichte.
- Modernisierung der IT und Beschleunigung der Vereinheitlichung von Geschäftsprozessen, um eine ERP-Transformation zu erreichen, ohne die Sicherheitsabdeckung und die Betriebskosten zu beeinträchtigen.

NEXTLABS

Einhaltung von Vorschriften

Verbessern Sie die Sicherheit und optimieren Sie die Einhaltung von Cybersicherheitsanforderungen

Vorbeugende Sicherheit

Schutz vor Datenverletzungen und Reduzierung der Angriffsfläche

Schnelles Time-to-Value

100-prozentige Fertigstellung des Umfangs innerhalb des engen Zeitrahmens

Automatisierung

Schnelle Anpassung an neue Geschäftsanforderungen, vereinfachtes Änderungs- und Eskalationsmanagement

Wie Fiserv und NextLabs das Ergebnis gemeinsam erreichen

NEXTLABS

fiserv forum

fiserv.

Kernpunkt

Das Cyber Security Team von Fiserv und NextLabs arbeiteten produktiv zusammen, um die dynamische Datenschutzlösung von NextLabs nahtlos zu implementieren und so die Ziele der ERP-Transformation von Fiserv zu erreichen. Mit der Lösung von NextLabs kann Fiserv Datenschutzverletzungen und die unrechtmäßige Offenlegung von sensiblen Finanzdaten der Kunden verhindern und die globale ERP-Applikation von Fiserv unter einer einzigen globalen S/4 HANA-Instanz vereinheitlichen. Der Data Access Enforcer von NextLabs führt eine zusätzliche Ebene des Datenschutzes für Anwendungen mit Echtzeit-Durchsetzung ein, wodurch viele manuelle Aufgaben eliminiert werden und die vom Fiserv-Team und den sich entwickelnden Vorschriften vorgegebene Compliance erreicht wird.

NextLabs DAE for SAP

