VIAVI Solutions

Broschüre

VIAVI Observer
GigaFlow

Aussagekräftige Enriched-Flow-Daten zu Netzwerken, Nutzern und Infrastrukturen für IT-Teams

In der IT den Durchblick behalten

Bei allen Änderungen in den IT-Umgebungen ist die IP-Technologie die einzige Konstante geblieben. Trotz ihrer Zuverlässigkeit und Skalierbarkeit hat diese Abhängigkeit aber auch Folgen:

1. Die IT-Teams wissen weniger über den Verbindungsaufbau und die Funktion der IT-Infrastruktur.
2. Es gibt keine offenen Standards, die das Wer, Was und Wo definieren sowie festlegen, wie Nutzer und Geräte miteinander kommunizieren.

Das Ergebnis: Den IT-Teams fällt es häufig schwer, den Überblick über das Nutzererlebnis und die Leistung zu behalten.

Doch es kommt noch schlimmer! Die heutigen hybriden IT-Umgebungen werden immer komplexer. Die wachsende Komplexität durch die hohe Anzahl unterschiedlicher Geräte für IT-Bereitstellungen und Cloud-Migrationen speziell am Netzwerkrand ist nicht mehr zu beherrschen. Die IT-Teams verlieren die Kontrolle.

Observer GigaFlow kombiniert zahlreiche Kennwerte intelligent und bewältigt die oben genannten Herausforderungen, indem es den Status jeder einzelnen Netzwerkschnittstelle unabhängig von deren Standort oder Zugehörigkeit exakt ermittelt. Auf diese Weise erhält das IT-Team mit angereicherten und genauen Netzwerkdaten zur forensischen Analyse erweiterte Einblicke in das Endnutzererlebnis.

Das Netzwerk und die Infrastruktur können dem IT-Team genau sagen, wer angeschlossen ist und wer kommuniziert. GigaFlow versetzt es in die Lage, zuzuhören und zu verstehen.

Enriched-Flow-Datensätze mit GigaFlow

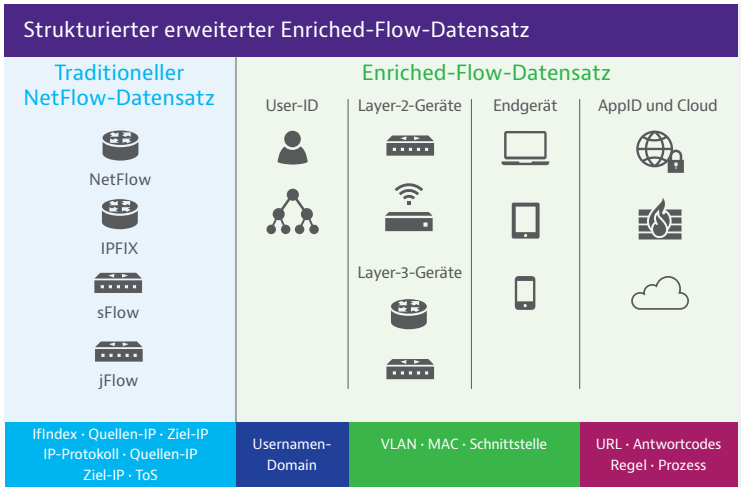
Wann ist ein Datenfluss nicht einfach ein Datenfluss? Wenn es sich um einen von GigaFlow angereicherten Datensatz („Enriched Flow“) handelt. Beim konventionellen Erfassen und Speichern von Verkehrsflüssen, wie mit NetFlow, werden die Daten zusammengefasst, bereinigt und dedupliziert. Dieser Prozess führt zu einem gewissen Genauigkeitsverlust, der die Aussagekraft forensischer Beweise einschränkt sowie eine effektive Behebung von Problemen erschwert.

GigaFlow ist die branchenweit erste Lösung, die den Datenfluss neu interpretiert, um dessen volles Leistungspotenzial auszuschöpfen. GigaFlow kombiniert und strukturiert mehrere Datenquellen, wie NetFlow, SNMP, Nutzeridentität und Session-Syslog, zu einem Enriched-Flow-Datensatz.

Auf diese Weise stehen den IT-Teams für sämtliche Kommunikationen, die die IT-Umgebung aus gleich welcher Richtung passieren, bis auf Ebene des einzelnen Nutzers tiefgehende Einblicke in die Netzwerk-Gerätetypen, Verbindungen, Verkehrssteuerungen und Nutzungsmuster zur Verfügung.

Die in Echtzeit erstellten angereicherten Datensätze werden ohne Bearbeitung im Zeitverlauf in einer relationalen Datenbank gespeichert. Damit sind die IT-Teams in der Lage, jede operative Variable mühelos zu lokalisieren und das Netzwerk sicherzustellen und dauerhaft zu schützen.

VIAVI sorgt für einen aussagekräftigen Überblick über das Netzwerk. Die Infrastruktur und der Verkehr werden allen beteiligten Parteien übersichtlich dargestellt und dienen den IT-Teams als Ausgangspunkt für weitere Maßnahmen.



Welche Vorteile bietet der Enriched Flow?

Der Enriched Flow gewährt Einblicke in:

- Drittgeräte, wie Packet-Broker, Proxy-Server, Load-Balancer, SD-WAN-Forwarder und Firewalls
- ARP- und CAM-Tabellen
- Authentifizierungsdaten von Active Directory und anderen Quellen von Drittanbietern
- DNS-Antworten und -Zeit
- Cloud-Quellen wie VPC Flow Logs

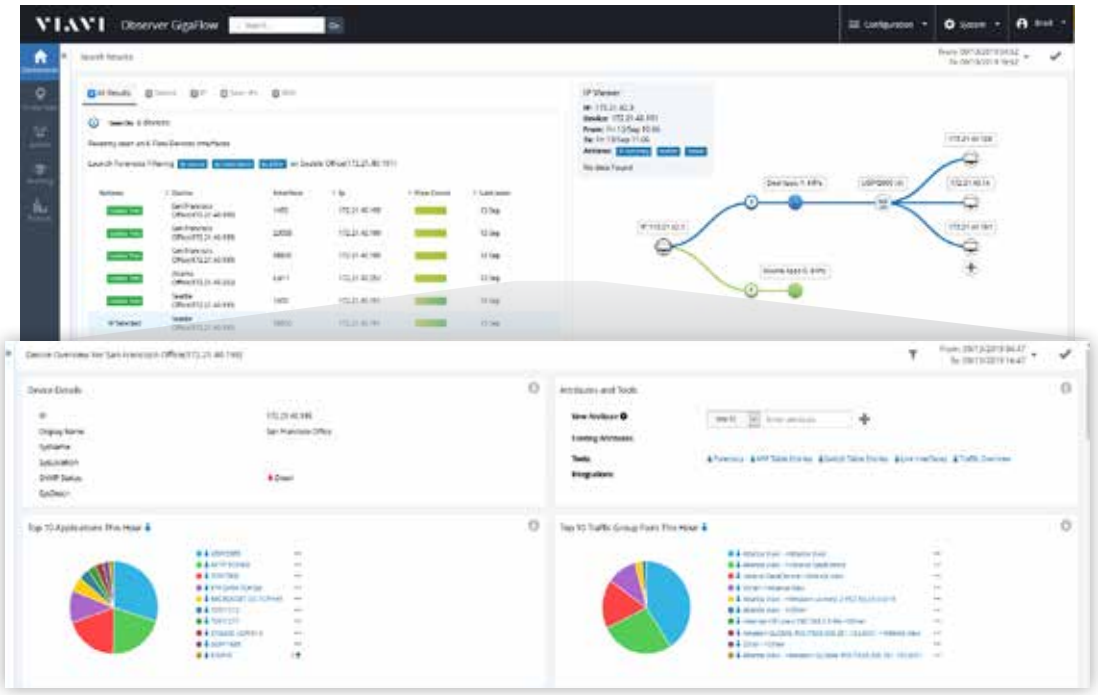
Beispielhafte Felder. Der tatsächliche GigaFlow-Datensatz kann sehr viele unterschiedliche Felder enthalten.

1057.900.0122

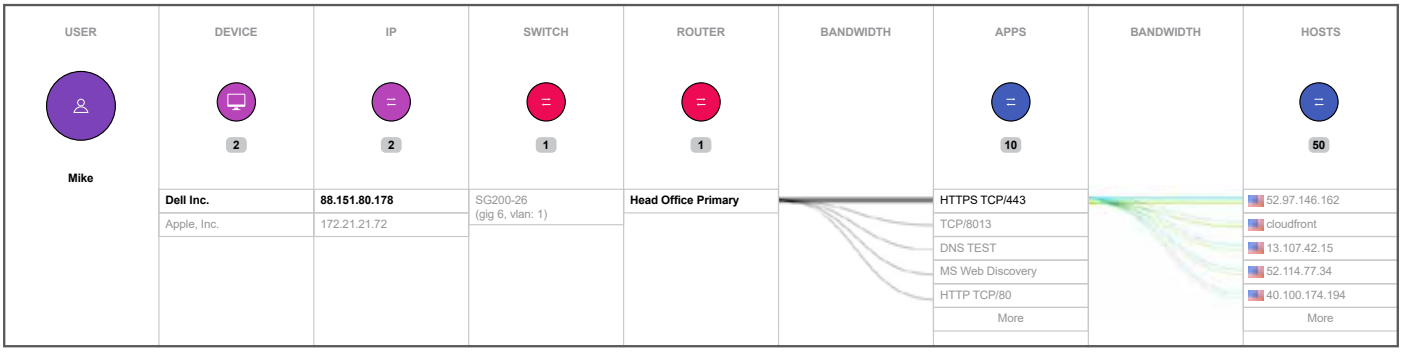
Enriched-Flow-Datensätze für Sicherheits- und Netzwerkteams

In Abhängigkeit vom Status des zugrunde liegenden Dienstes vermittelt GigaFlow zu jeder Schnittstelle des Netzwerkverkehrs historische Langzeit- und Echtzeit-Einblicke in den Endnutzer und das Gerät. Die Enriched-Flow-Datensätze von GigaFlow erfassen alle relevanten Daten, sogar Zeitstempel und Standorte, über längere Zeiträume dynamisch und kontinuierlich. Dadurch sind die IT-Teams in der Lage, zu einem spezifischen Ereignis oder einer Anomalie in der Vergangenheit zurückzugehen, um zu untersuchen, wer wann und wo davon betroffen war und wie diese Störung aufgetreten ist, sodass eine Problemlösung möglich ist.

Das ist insbesondere für Sicherheitsteams von Vorteil, die diese datenflussbasierte Analyse nutzen können, um die Verweildauer des Angreifers zu verringern und schneller auf Sicherheitsverletzungen zu reagieren. Da die meisten Angriffe längere Zeit unentdeckt bleiben, sind die Teams auf aussagekräftige Daten zur Infrastruktur, zu den Datenflüssen, Geräten, Hosts und Nutzern angewiesen, um eine retrospektive forensische Analyse durchführen und Sicherheitsverletzungen rechtzeitig beheben zu können.



Lückenlose Datenflussdaten zur forensischen Analyse mit IP-Angaben



Da Observer die auf den Layern 2 und 3 gesammelten Informationen zu einem einzigen Enriched-Flow-Datensatz zusammenfasst, können beispiellose interaktive Visualisierungen erstellt werden, die die Beziehung zwischen Nutzer, IP, MAC und Anwendungsnutzung im Netzwerk verdeutlichen. Die Mitglieder der Netzwerk- und Sicherheitsteams (NetOps/SecOps) geben einfach einen Namen/Nutzernamen ein und erhalten sofort alle Geräte, Schnittstellen und Anwendungen, die mit diesem Namen in Verbindung stehen, angezeigt. Nie war es einfacher herauszufinden, welche Geräte angeschlossen sind und wer im Netzwerk kommuniziert.

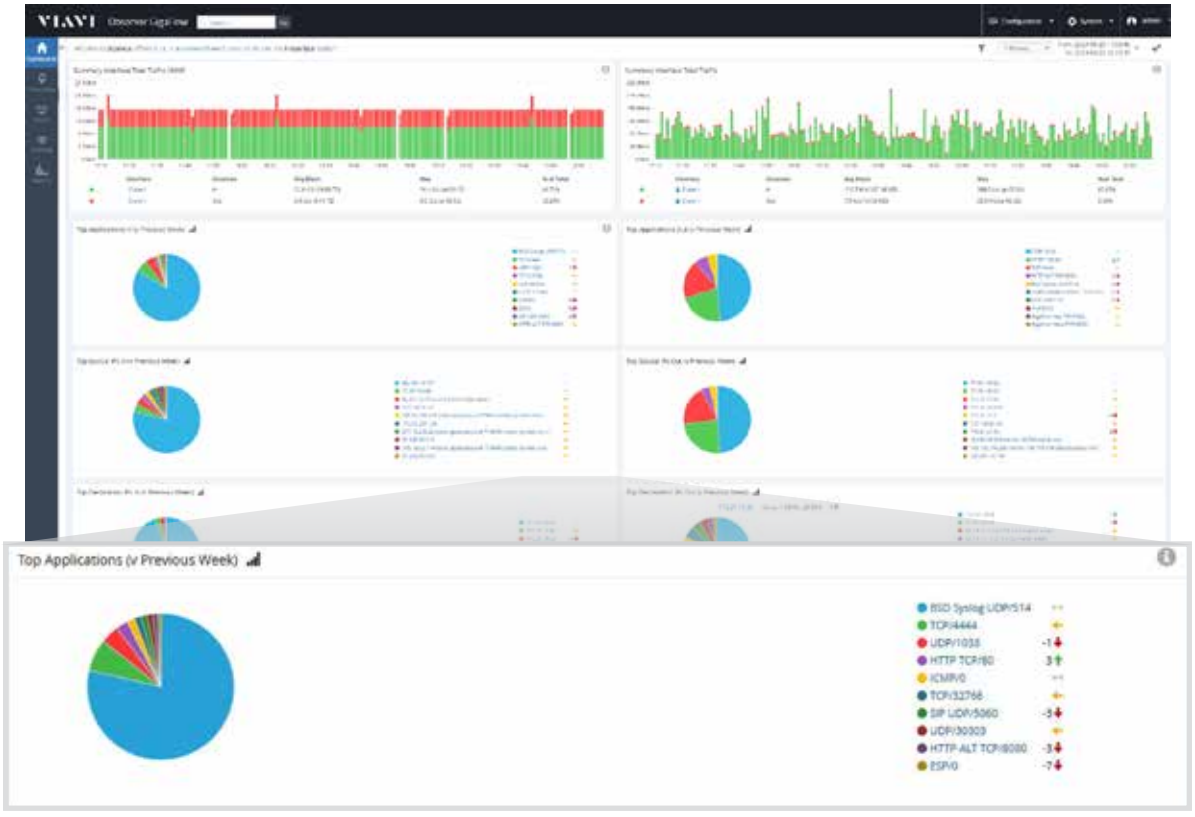
Netzwerk-Kapazitätsplanung mit Observer GigaFlow

Die Kapazitätsplanung für das Netzwerk ist ein laufender Prozess, der die kontinuierliche Bewertung der Netzwerkauslastung, der Verkehrsvolumen und der Verkehrstypen beinhaltet, um Mängel, wie Leistungsengpässe, die das Endnutzererlebnis beeinträchtigen, zu identifizieren.

Ohne die Investition in Maßnahmen zur Kapazitätsplanung besteht das Risiko, dass die Produktivität der Mitarbeiter durch die mangelhafte Netzwerkleistung sinkt, Dienstgütevereinbarungen (SLA) nicht eingehalten werden und die Erlebnisqualität des Endnutzers in Mitleidenschaft gezogen wird.

Geräte- und standortbasierte Workflows

GigaFlow vermittelt aussagekräftige Einblicke in die Nutzung und Auslastung der einzelnen Schnittstellen bis hinunter auf den Layer 2 Switch. Darin eingeschlossen sind grafische Zusammenfassungen der am intensivsten genutzten Standorte und Geräte mit weitergehender Analyse einzelner WAN-Übertragungsstrecken. Das sind ideale Voraussetzungen, um das Endnutzererlebnis an beliebigen Punkten der Konversationsstrecke allgemein einschätzen und auch die Kosten-Nutzen-Effizienz von Ressourcen beurteilen zu können, wie es beispielsweise notwendig ist, wenn Entscheidungen zum weiteren Ausbau getroffen werden sollen.

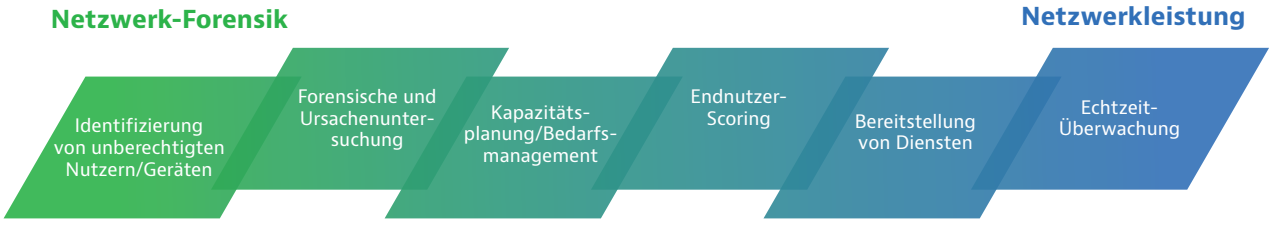


Geräte- und standortbasierte Dashboard-Anzeigen mit Angabe der Nutzung und Auslastung

Kapazitätsplanung mit tiefgehender Untersuchung zur forensischen Analyse

Mit seiner intuitiven Berichterstellung zur Kapazitätsplanung erlaubt GigaFlow den IT-Teams, die Ausgaben für WAN-Verbindungen proaktiv einzuschätzen sowie Kapazitätsstörungen rückwirkend zu beheben. Übersichtliche, farbcodierte Dashboard-Anzeigen heben die Schnittstellen hervor, die die meiste Zeit am intensivsten genutzt werden. Wenn der Verkehr an bereits überlasteten Standorten weiter ansteigt, gibt der Auslastungsbericht weitere rote und gelbe Warnungen aus. Die grafischen Zusammenfassungen der Anwendungen können den IT-Teams helfen, die Anwendung zu bestimmen, die für den Anstieg verantwortlich ist. Ausgehend von den Berichten zur Kapazitätsplanung ist es ebenfalls möglich, die Netzwerkdaten tiefgehender zu untersuchen, um forensische Analysen durchzuführen. Diese Funktion bietet sich an, um Leistungs- oder Sicherheitsprobleme zu untersuchen.

Farbcodierte Kapazitätsberichte zu den WAN-Ausgaben



Anwendungsfälle für Observer

1045.900.1221

Die Leistungsmerkmale und Vorteile auf einen Blick

- Präzise forensische Einblicke in alle Netzwerk-Konversationen im Zeitverlauf beschleunigen die Problemlösung.
- Ein umfassender Überblick über den Datenpfad des Dienstes ermöglicht es, den betroffenen Bereich selbst in komplexen hybriden IT-Umgebungen sofort einzugrenzen.
- Intuitive Berichte zur Kapazitätsplanung unterstützen die proaktive Bewertung der WAN-Nutzung.
- Ein interaktiver IP-Viewer, der die Beziehungen zwischen Nutzer, IP, MAC und Anwendungsnutzung im Netzwerk übersichtlich anzeigt.
- Neue Workflows stellen für jeden Standort und jede Geräteschnittstelle detaillierte Nutzungsdaten, die mühelos bis auf die Ebene der Forensik-Daten analysiert werden können, zur Verfügung.
- Umfassende Ermittlung von Ausgangswerten (Baselining), Kapazitätsplanung und Überprüfung der QoS-Einstellungen.

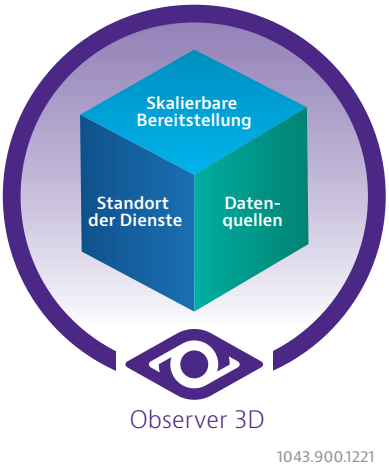
Observer 3D auf einen Blick

Observer 3D ist eine umfassende Lösung zur Leistungsüberwachung in Netzwerken (NPM), die Netzbetreiber- und Sicherheitsteams wertvolle Einblicke und Unterstützung bietet. GigaFlow ist für Observer 3D unverzichtbar, da diese Anwendung die Enriched-Flow-Metadaten, die für die Problemlösung sowie für forensische Untersuchungen benötigt werden, an Apex übermittelt.

Als integrierte Ressource für Dashboard-Ansichten und zur Berichterstellung ist Observer Apex die zentrale globale Anlaufstelle zur Gewährleistung der Sichtbarkeit. Weiterhin dient Apex als Ausgangspunkt für die zügige Fehlerdiagnose mit vordefinierten Workflows, die mit Paketen, angereicherten („Enriched Flow“) und erweiterten („Enhanced Flow“) Datenflüssen sowie mit aktiven Tests helfen, die Ursache von Störungen zu ermitteln.

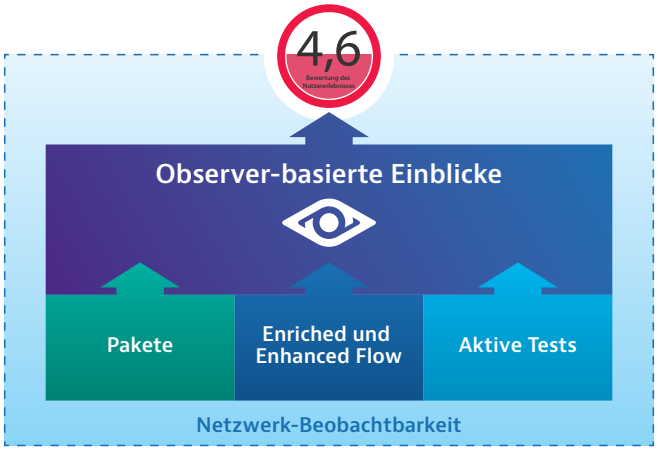
Observer 3D unterstützt die IT-Teams in dreierlei Hinsicht:

- Standort der Dienste: Observer 3D gewährleistet die Beobachtbarkeit aller Hosting-Umgebungen, wie von privaten Clouds, öffentlichen Clouds, SaaS-Anwendungen oder Nutzern an externen Standorten, in Niederlassungen oder im Rechenzentrum. VIAVI erfasst alle Dienste, unabhängig vom Standort. Besuchen Sie die interaktive Plattform, um mehr darüber zu erfahren, wie Observer 3D prädiktive Analysen nutzt, um eine proaktive Sichtbarkeit von Leistungsstörungen zu gewährleisten.



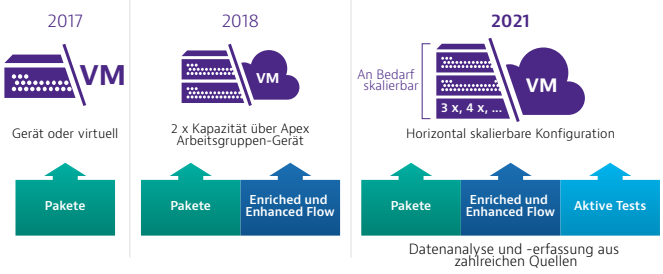
1043.900.1221

- Datenquellen: Mit Observer 3D haben Sie die Wahl zwischen einer Kombination aus Paketdaten, angereicherten und erweiterten Datenflüssen, Einblicken in aktive Tests sowie generierten Metadaten, um Leistungsstörungen und Sicherheitsbedrohungen nahtlos und zeitnah zu beheben. Automatische, rollenbasierte Workflows erleichtern unabhängig vom Daten- und Quellentyp die Analyse der Netzwerkdaten zur forensischen Analyse.



1041.900.1221

- Skalierbare Bereitstellung: Sie können klein beginnen und das System mühelos erweitern, wenn Ihr Unternehmen wächst und sich die Überwachungsanforderungen und der betriebliche Bedarf ändern. Darin eingeschlossen ist die flexible Bereitstellung mit unseren Lösungen 24T oder ObserverONE sowie auch die flexible Preisgestaltung mit unseren neuen gestaffelten Preis- und Abo-Modellen. Bei VIAVI haben Sie alle Möglichkeiten. Sie kaufen einfach, was Sie brauchen, wann immer Sie es brauchen. Nutzen Sie dafür Ihr vorhandenes Budget für Betriebs- oder Investitionsausgaben, sodass Sie die Beobachtbarkeit uneingeschränkt auf den Finanzbedarf abstimmen können.



1042.900.1221

VIAVI Solutions

Kontakt +49 7121 86 2222

Sie finden das nächstgelegene VIAVI-Vertriebsbüro auf viavisolutions.de/kontakt

gigaflow-br-ec-nse-de
30187611 904 0122