Visibilidade e Controle das suas rotas na Internet

André Gustavo Albuquerque
Caroline Araújo

9 de Junho de 2022

01 Introdução ao Crosswork Cloud

02 Visão Geral do Crosswork Network Insights

03 Demonstração

Quint@s Quinze

Cisco Network Automation Approach

Enable Outcomes

Increase Agility

Reduce Strain

Closed Loop Automation

Deliver on Premises and in the **Cloud**

Crosswork Infrastructure On-Prem

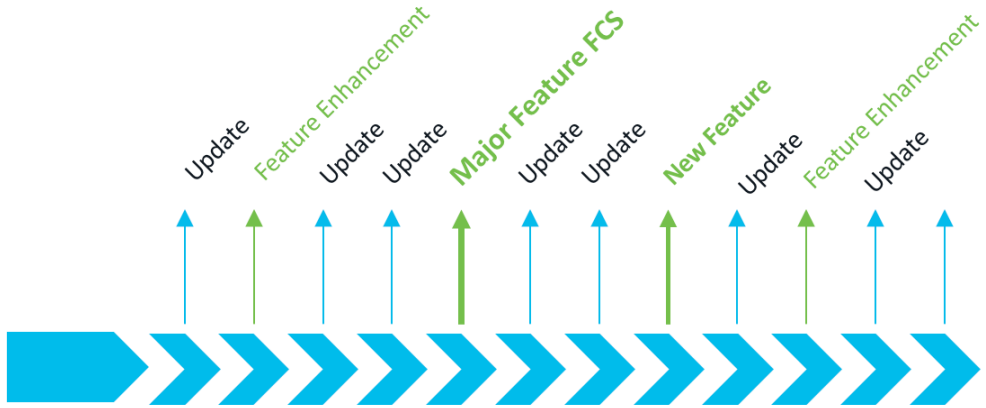
Crosswork Cloud

Closed-Loop and Outcome-Driven Automation, on Premises and in the Cloud

Cloud-Delivered Operational Intelligence

- Immediate deployment and always up-to-date
- Continuous delivery of new features and updates
- Delivers scale-out model for large-scale visibility and reporting services
- Minimal ongoing OpEx to support

A new way to consume software as a service



Continuous delivery of new features and software updates to the production cloud service.

No user testing or software maintenance required.

- Software delivered and maintained by Cisco
- Continuous (Weekly) delivery pipeline to production service
- Continuous pipeline for new features and fixes
- No customer action required for ongoing maintenance or upgrades

Crosswork Cloud: Operational Intelligence Platform

Cisco
Crosswork Cloud

https://crosswork.cisco.com

Cisco Crosswork Network Insights

Visibility and intelligence to assess network operational health

Detect network events for customers

Cisco Crosswork Trust Insights

Measure, audit and verify network hardware and software trustworthiness

Verify device trust

Cisco Crosswork Traffic Analysis

Netflow analytics
Peering Optimization

Reduce Operational Costs

Cisco Crosswork Network Insights
A Cloud based subscription service for network routing analytics

The Cisco Advantage:

Intellectual Property

Speed

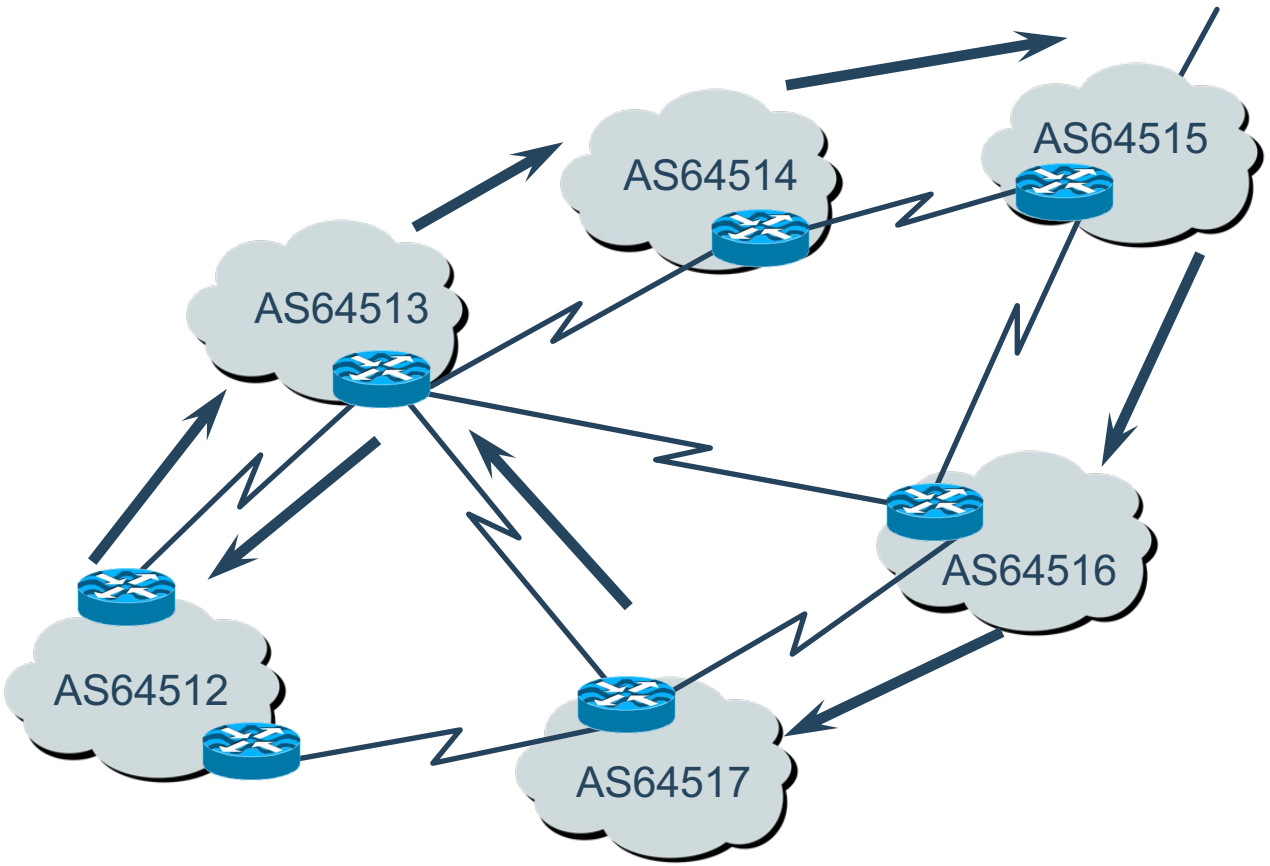
Scale

Integration

Knowledge and Experience

Crosswork Cloud:
Network Insights
(External Route Analysis)

BGP on the Internet



- “Gossip” protocol
- Trust based
- RPKI enhances trustworthiness
- Monitoring and visibility are still needed

Network Insights Functions

The mission-critical BGP security tool that every NOC must have

- Provides critical monitoring for potential route hijacking and router leaks events
- Provide early warning of BGP attacks on your peers
- Define policies to automatically alert on unexpected changes or anomalies

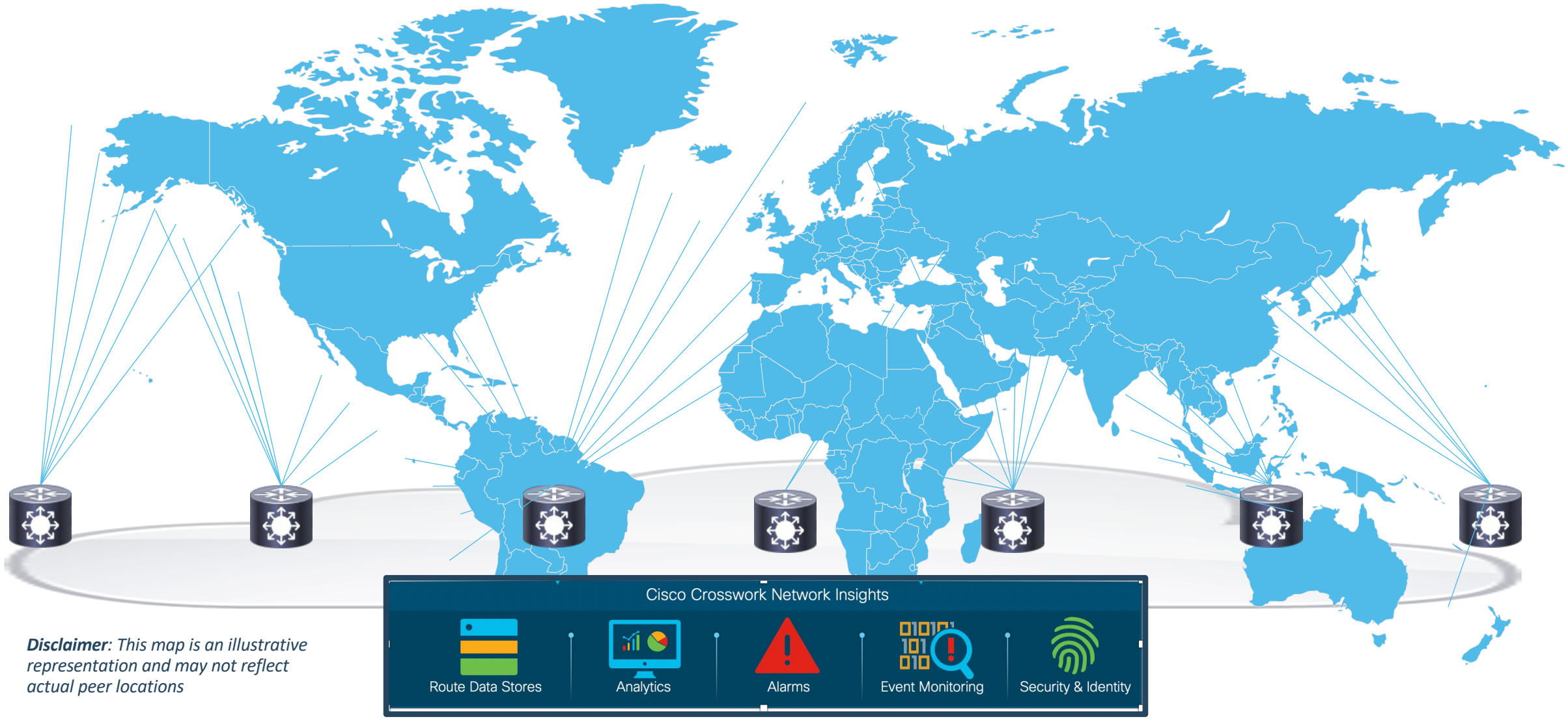
Looking Glass (current state of BGP across the globe)

- Global view of how your BGP advertisements are received
- Real time updates, BGP attacks usually last < 7 minutes
- Consolidated view of all global looking-glasses

BGP Update Log (Global BGP History)

- Forensic view of all observed BGP updates with history

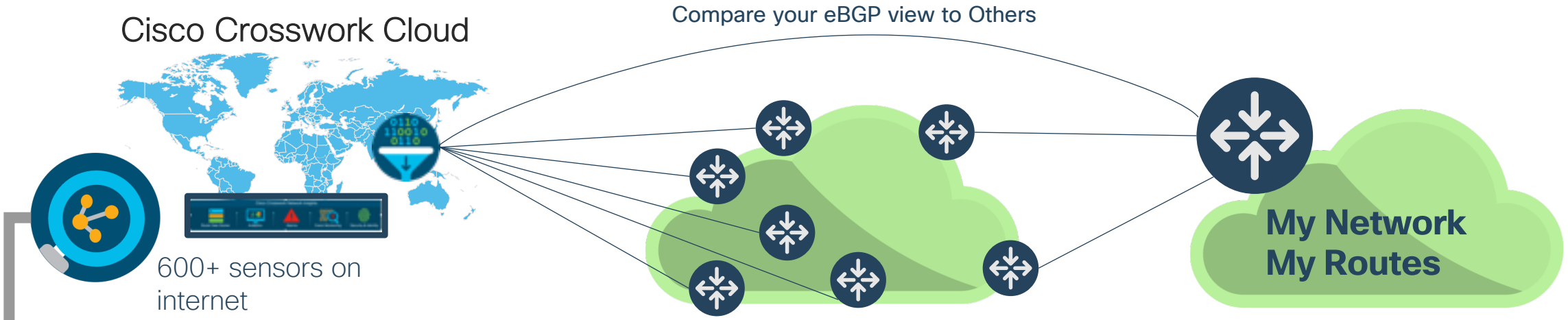
Network insights monitors hundreds of peers world-wide



***Disclaimer**: This map is an illustrative representation and may not reflect actual peer locations*

Quint@s Quinze

External Route Analysis at Cloud Scale



BGP Polices allow You to identify when things are not behaving as expected

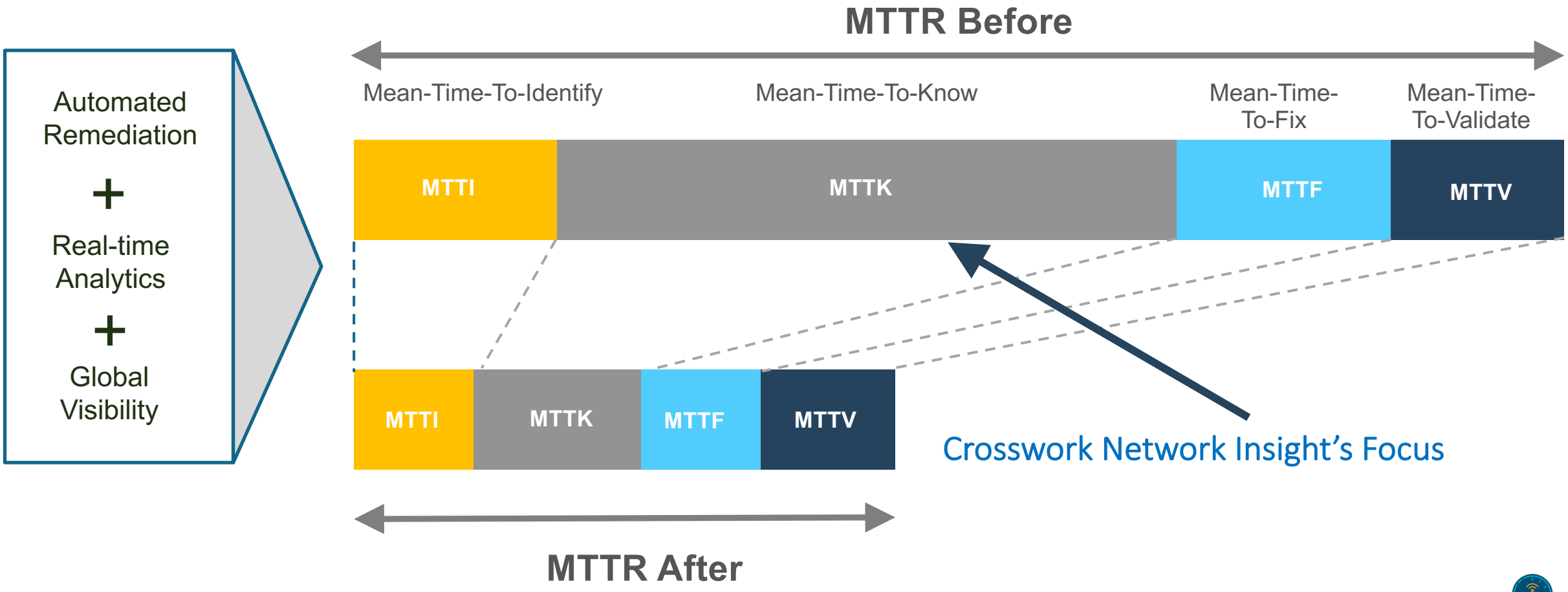
eBGP Sensor Nodes From Customers and from our own locations

External view of your network as seen by others

Our Goal: Minimizing & Preventing Downtime

Real Time Visibility

Mean-Time-To-Repair (MTTR) – Key KPI impacting customer experience

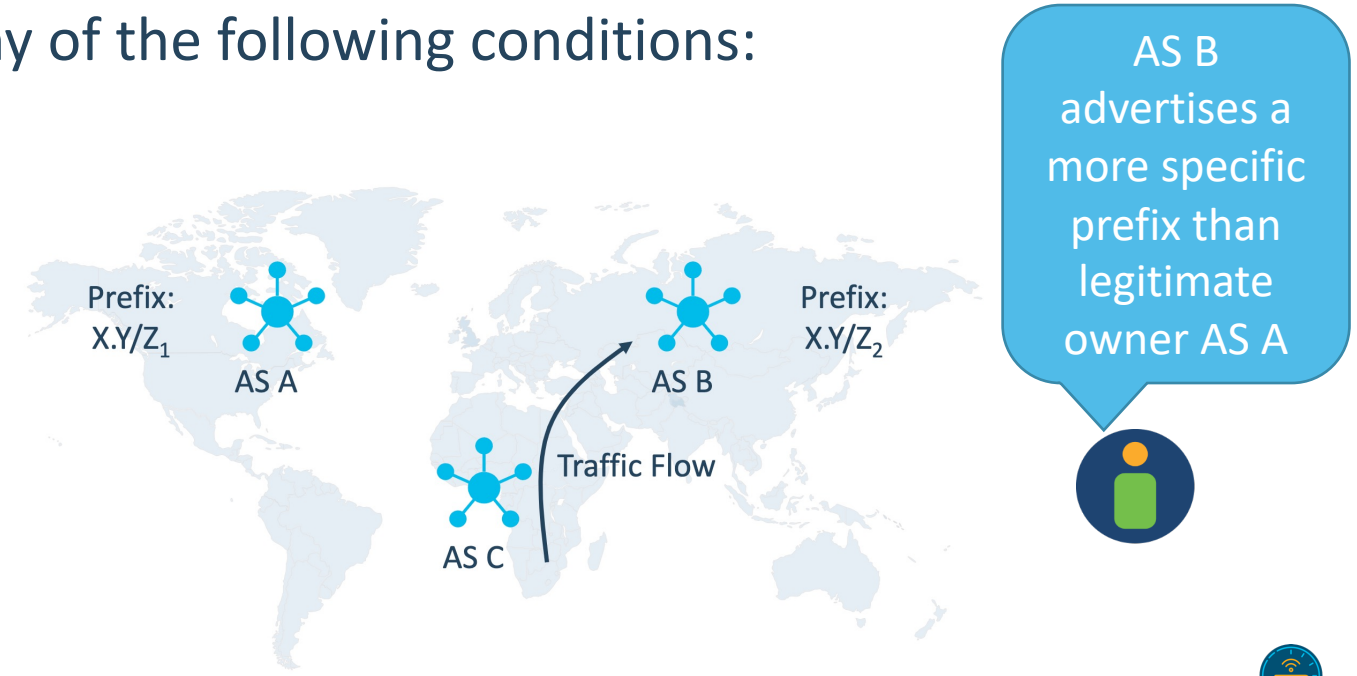


Quint@s Quinze

Use Cases

Use Case: Route Hijack Detection

- Route Hijacks can be performed in many ways. Some are malicious, some are accidental.
- Layered BGP Policy Alarm Architecture allows setting monitoring criteria to match peering Architecture.
- Our Alarm Conditions may test for any of the following conditions:
  - ASN Origin Violation
  - Unexpected Longer Prefix Match
  - ROA/RPKI Failure/Mismatch
  - Upstream ASN violation
  - Valid AS Path Violation
  - Man in the Middle Detection*



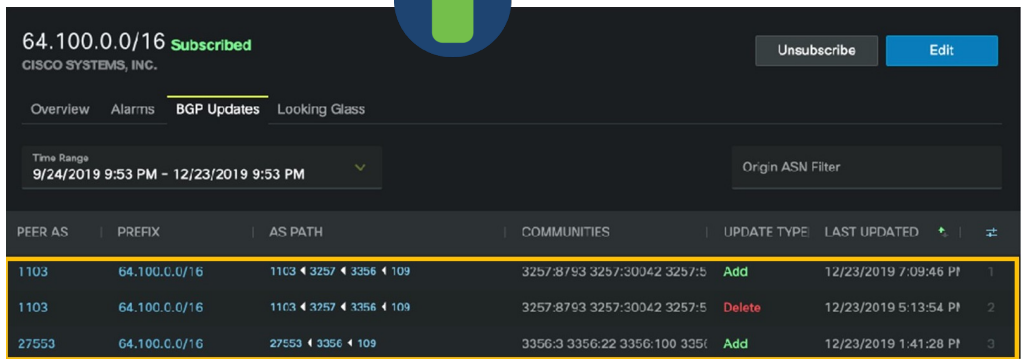
Use Case: Route Leak Detection

- Route Leaks may occur in many ways; may be accidental.
- Layered BGP Policy Alarm Architecture allows monitoring criteria to match peering architecture intent.
- Alarms allow testing for any of the following conditions:
  - Upstream AS Change (whitelist / blacklist)
  - ASN Origin Violation
  - Prefix Aggregate Change
  - Unexpected Longer Prefix Match
  - AS Path Length Violation (too short / too long)
  - Prefix Advertisement (for detecting unintended advertisements)
  - Peer Router Prefix Violation (whitelist / blacklist)*

Use Case: Forensic Route Analysis

- Routing Events are often short-lived in the order of 3-5 minutes. Often BGP event is resolved before the support tickets are reviewed.
- Our core differentiation - we collect and store up to 90 days of forensic BGP data records. BGP Update Search let customers look at historical information to identify time series events of importance.
- Useful for:
  - Security Operations, Network Operations
  - Commercial Disputes
  - Evaluating Peering Candidates

What Happened to 64.100.0.0/16 Prefix last Thursday?



Quint@s Quinze

Policies & Alarms

Policy Overview

- Policies define threshold values for alarm activation.
  - Alarms may be in “active” or “cleared” state.
- Two types of policies – Prefix Policy and ASN Policy
  - Each Prefix may be monitored by only one Prefix Policy, however same policy may be used for many prefixes
  - Each ASN may be monitored by only one ASN policy, however same policy may be used on multiple ASNs
- Policies can contain one or more rules.
- Each rule may have one or more endpoints. Endpoints can be reused across rules and policies

Alarm Types

	Supported
AS Origin Violation	✓
SubPrefix Advertisement	✓
Prefix Withdrawal	✓
ROA Failure	✓
Upstream AS Change	✓
Parent Aggregate Change	✓
Unexpected AS Prefix	✓
AS Path Length Violation	✓
Prefix Advertisement	✓
Valid AS Path Violation	✓

REST API Access

- Automate monitored prefixes and ASNs using REST API
  - Enables onboarding of prefixes/ASNs – for ex bring your own IP
- Automate and integrate alarms info with other tools
  - Enables single plane of glass applications to get visibility
  - Enables Auto Remediation tools to be run when routing incidents are detected by Network Insights.
- Automate administrative items – add/delete users and policy configurations, end points etc.

DEMO

Free Tier & Trial

https://crosswork.cisco.com

CrossworkCloud

Login

CrossworkCloud

A SaaS solution that provides operational insight and validation of network health and security with the agility and scale of the cloud.

Network Insights

Network and BGP analysis to maintain routing health by monitoring for route leaks and hijacks.

tch Video | Find Out More

Traffic Analysis

Visualize, analyze, and optimize network traffic at distributed peering points.

Watch Video | Find Out More

Trust Insights

Gain operational visibility to preserve the trustworthiness of your network infrastructure.

Watch Video | Find Out More

Request Free Account

Interested in experiencing how Cisco Crosswork Cloud can help evaluate the routing health and telemetry of your network? Sign up for a free product account of Cisco Crosswork Cloud.

Contacts | Resellers | Documentation | Terms & Conditions | Privacy Statement

Quint@s Quinze

Dúvidas?

Quint@s Quinze

Muito Obrigado!