NetQuest

DPI Network Sensors for Cyber Threat Hunting

DISA TEM

April 16, 2025

SNS
STREAMING NETWORK SENSORS

Agenda

- Introductions
  - David Nelson, Federal Sales Director
  - Mike Seidler, VP Product Management
  - Gene Litt, CTO
  - Richard Moulder, VP Worldwide Sales and Support
  - George Siebert, Federal Engineer
- What We Want to Accomplish Today
  - Explain the concept of “Streaming Network Sensors” and what makes NetQuest Different
  - Explore Use Cases Relevant to DISA and DoD
  - Explain how we help the War Fighters in mission areas
  - Answer all questions interactively
  - Discuss any follow up actions desired
- Let’s start with a quick overview of NetQuest Corporation

About NetQuest Corporation

NetQuest
Monitoring Access Solutions

Market-Leading 10/100/400G Flow and Packet-Based Traffic Monitoring Solutions

- TRL 9 Technology, proven in DoD labs for years
- US Based, Employee-Owned company in Mt Laurel, New Jersey, USA headquarters
- 100% US-Based R&D and engineering team
- Expertise in:
  - Purpose-Built software-defined systems
  - Carrier-Class deployment-proven technology
  - Line-Rate Traffic Policy Engine with terabit-scale filtering and metadata creation
  - Built-in capability to analyze encrypted traffic-JA4+
  - Extensive experience with WAN Signals Intelligence
- ISO 9001:2015 certified

Deep expertise in ultra high-speed programmable logic, hardware and software design for mission-critical Cyber Security monitoring requirements

Emerging Cyber Threats Facing Telcos and Government Agencies

NetQuest
Monitoring Access Solutions

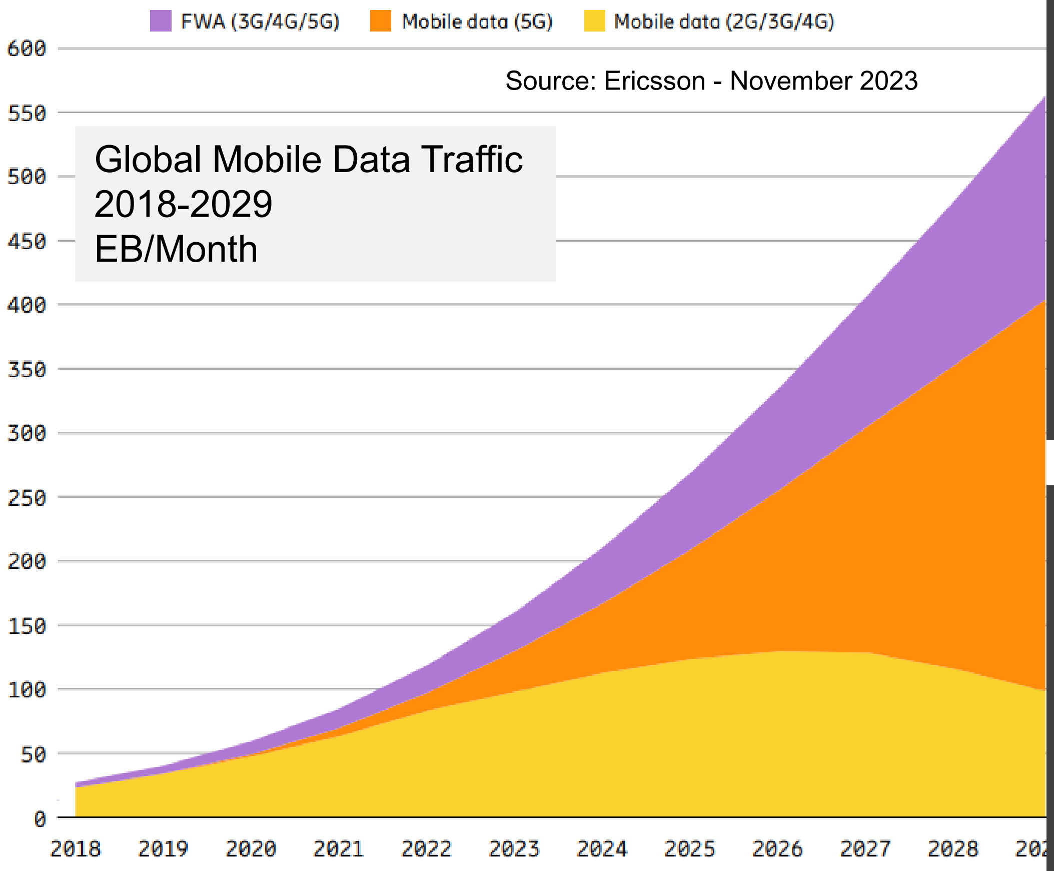
- **Advanced Persistent Threats (APTs)** from state-sponsored groups used to conduct espionage and disrupt services
- **Supply Chain Attacks** used to gain access
- **Insider Threats** enable employees to leak sensitive information
- **DDoS Attacks** disrupt services, causing downtime and financial losses
- **IoT Vulnerabilities** exploit weak security in connected devices to infiltrate networks

Hacker group known as ***Salt Typhoon***, believed to be backed by Chinese government, breached key components of US telco infrastructure

US Government is increasingly targeted by sophisticated cyber threats, posing significant risks to infrastructure, data security, and customer privacy

Why NetQuest? Security Monitoring is Under Pressure…

- Unprecedented network traffic growth
- Sampling traffic is not good enough—with AI and ML tools, more data leads to better analysis
- Scaling analysis of unsampled flow data presents significant operational challenge and cost
- Adoption of 100G+ networks strains monitoring infrastructure capacity and increases cost and complexity



Source: Ericsson - November 2023

Global Mobile Data Traffic 2018-2029 EB/Month

56GB

North America average monthly mobile data usage per smartphone in 2023 was 21GB and is expected to reach 56 GB in 2029.

73%

Video accounted for 73 percent of global mobile network traffic in 2023

Source: Ericsson Mobility Report - November 2023

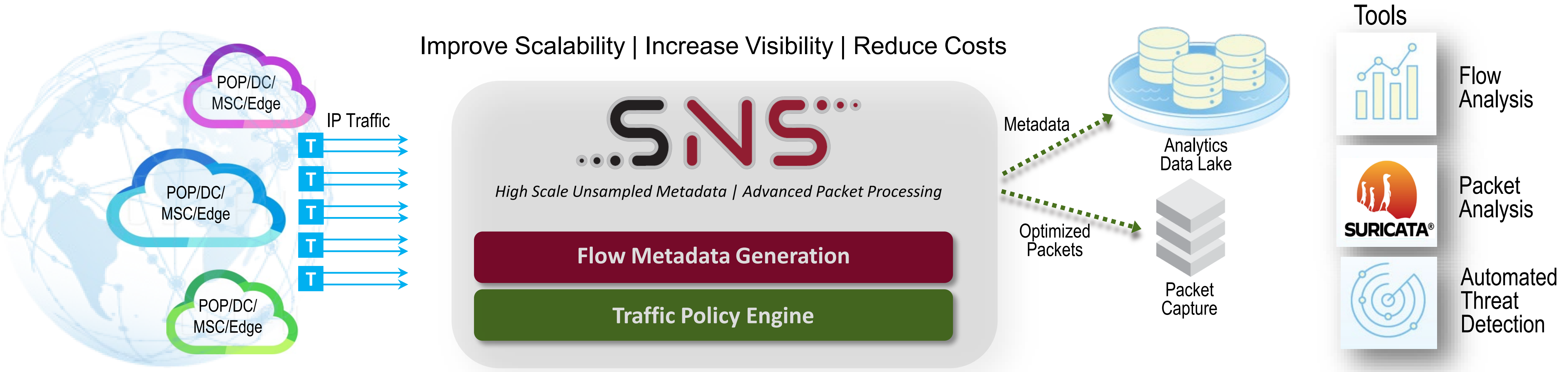
How NetQuest Helps your Mission

- Sensors for network visibility requiring massive capacity “at terabit scale”
- High-Scale **unsampled** flow metadata
- DPI-enriched flow metadata with encrypted traffic analysis and L7 Application Classification
- Traffic fingerprints enable detection of Indicators of Compromise (IoC)
- Optimize traffic delivery to existing tools

- Optimize security-focused visibility
- Enable modern cyber threat hunting techniques
- Reduce cost per bit for monitored traffic
- Meet emerging regulatory requirements

NetQuest Streaming Network Sensor

Powerful Network Intelligence for Large-Scale Security Monitoring



High-Capacity Enriched Metadata Generation

- Unsampled flow metadata for 100% visibility
- Protocol-specific metadata (TLS, QUIC, SSH, DNS, HTTP, SIP, STUN, MPLS, OSPF, BGP) & Layer 7 application classification
- Encrypted traffic fingerprinting (JA3, JA4+, HASSH)
- Flexible Metadata Categories (Flow, Telemetry, Routing, Mobile, etc.)
- Output via IPFIX or Kafka

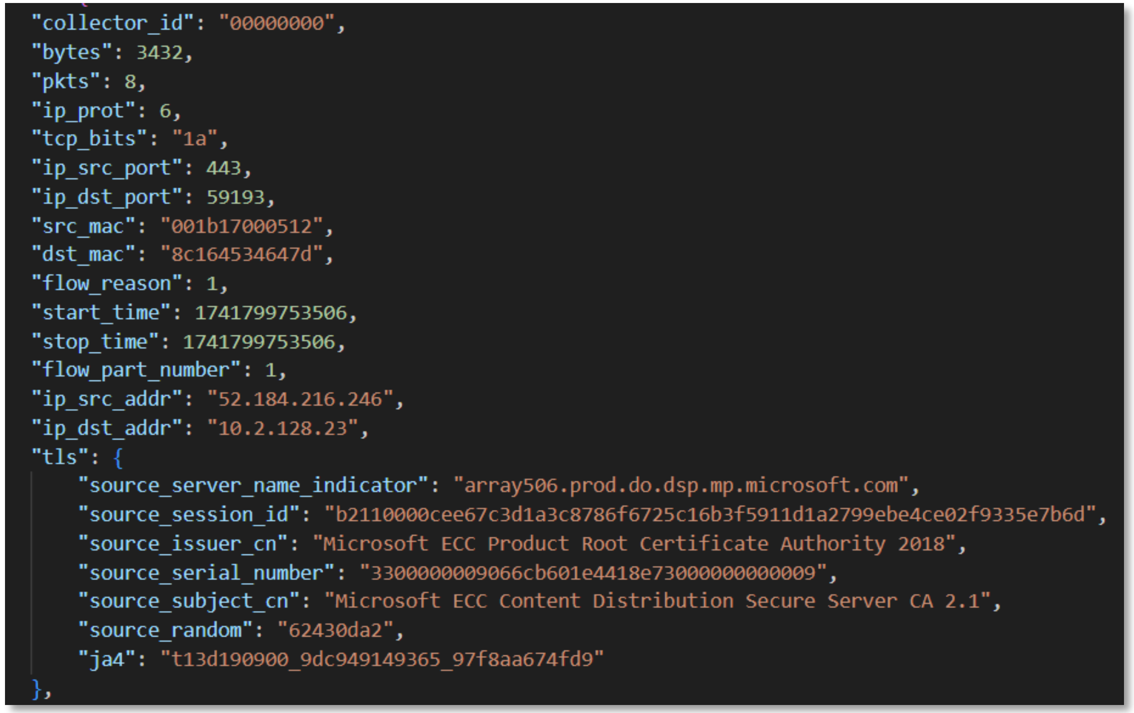
Intelligent Traffic Policy Engine

- Filter on IP Prefixes, Services, Layer 7 Applications
- Flow Slicing: Forward Packets Carrying Initial TLS/QUIC Handshakes
- Header & Tunnel Processing
  - VLAN (5), MPLS (7)
  - VXLAN, GTP, GRE, PWE3, L2TP, PPTP, IP-in-IP
- Port tagging via VLAN Insert or MAC Replacement

Network Intelligence Metadata Categories

- Flow Data
  - Standards-based Flow Records (outer or encapsulated IP metering)
  - Layer 7 DPI-based application name, category, description
  - Protocol attributes (DNS, TLS, QUIC, SSH, DTLS, HTTP, SIP, STUN)
  - Encrypted Traffic Analysis-enriched Flow Records (TLS/QUIC JA3 & JA4, HASSH, RDPF fingerprints)
- Telemetry Data
  - Ethernet Telemetry Records (interesting frame counts, e.g. MACSEC, PWE3, GRE, GTP, IP-in-IP, L2TP, PPTP)
- Routing Data
  - OSPF Hello Records, OSPF LSA Records
  - BGP Records
- Mobile Data
  - IMSI Traffic Records (Example - 5G Fixed Wireless Access traffic statistics)

UK Internet Connection Record (ICR)

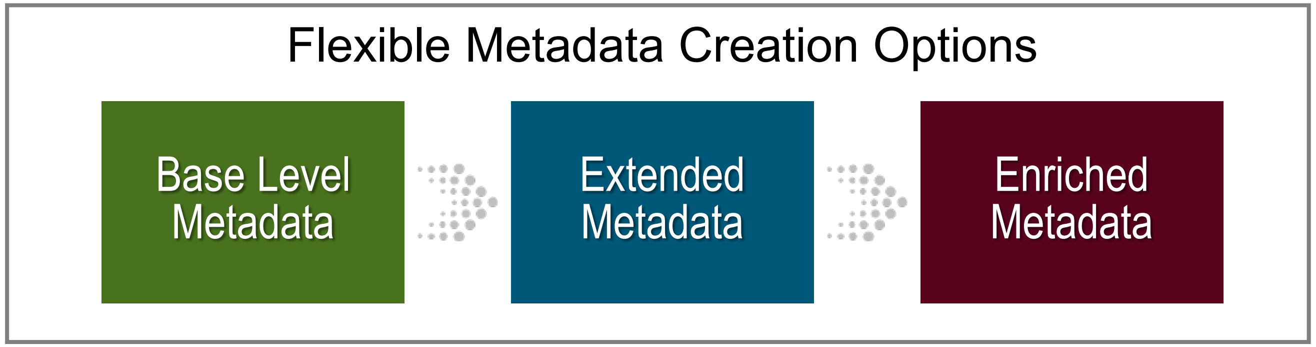


```
"collector_id": "00000000",
"bytes": 3432,
"pkts": 8,
"ip_prot": 6,
"tcp_bits": "1a",
"ip_src_port": 443,
"ip_dst_port": 59193,
"src_mac": "001b17000512",
"dst_mac": "8c164534647d",
"flow_reason": 1,
"start_time": 1741799753506,
"stop_time": 1741799753506,
"flow_part_number": 1,
"ip_src_addr": "52.184.216.246",
"ip_dst_addr": "10.2.128.23",
"tls": {
    "source_server_name_indicator": "array506.prod.do.dsp.mp.microsoft.com",
    "source_session_id": "b2110000cee67c3d1a3c8786f6725c16b3f5911d1a2799ebe4ce02f9335e7b6d",
    "source_issuer_cn": "Microsoft ECC Product Root Certificate Authority 2018",
    "source_serial_number": "3300000009066cb601e4418e73000000000009",
    "source_subject_cn": "Microsoft ECC Content Distribution Secure Server CA 2.1",
    "source_random": "62430da2",
    "ja4": "t13d190900_9dc949149365_97f8aa674fd9"
},
```

Network Sensors for Every Observability Requirement

SNS

STREAMING
NETWORK SENSORS



Flexible Metadata Creation Options

Base Level Metadata → Extended Metadata → Enriched Metadata

OMX3200

- 1:1 unsampled flow data
- Up to 16x 100GbE in 1RU
- 1.6 Tbps Traffic Processing
- Supports Base and Extended metadata
- Export via IPFIX only

Enriched Flow Intelligence

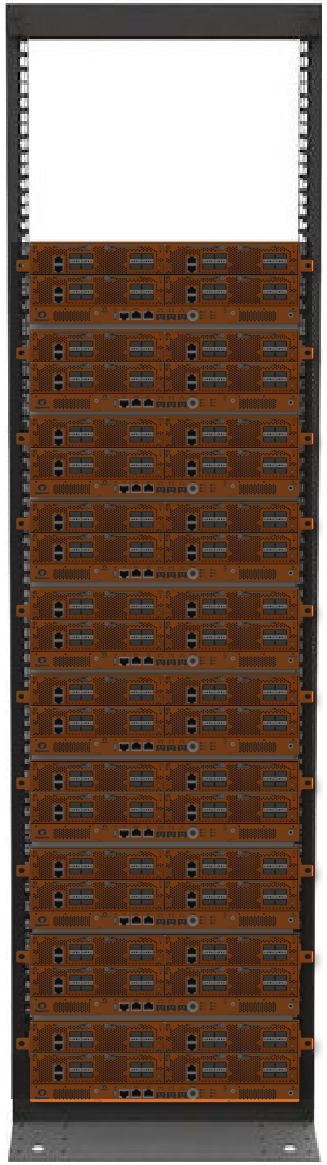
SNS750

- 1:1 unsampled flow data
- Up to 4x 100GbE in 1RU
- 400 Gbps Traffic Processing
- Enriched Flow Intelligence for Layer 4-7 visibility
- Supports Base, Extended and Enriched metadata
- Export via IPFIX or Kafka

SNS2000

- 1:1 unsampled flow data
- 4x 400GbE or 16x 100G in 2RU
- 1.6 Tbps Traffic Processing
- Enriched Flow Intelligence for Layer 4-7 visibility
- **Supports Base, Extended and Enriched metadata**
- Export via IPFIX or Kafka

NetQuest Metadata Generation is Massively More Efficient



Example Telco Datacenter Environment

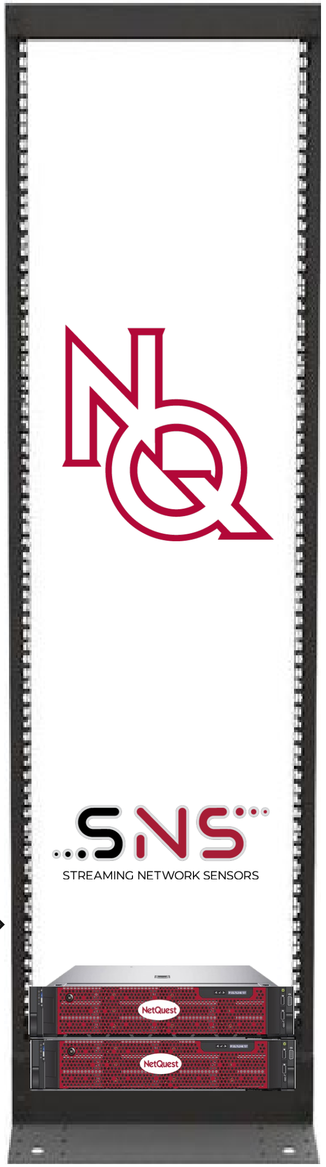
- 75x Full-Duplex 100G Links
- 2 Tbps Throughput

Metadata creation only excludes aggregation layer

Solution *X*

- 10x systems
- 30 RU
- 220G throughput per system
- 19,000 Watts
- 64,830 BTU

Save space, power, cooling, cost
Increase Visibility



- 8 fewer physical systems
- 26 less rack units
- 5x Higher capacity & throughput
- Lower power+cooling
- 80% Lower cost
- Future-ready for 400G
- No header/tunnel stripping required

NetQuest Solution

- 2x Systems
- 4 RU
- 1.6 Tb throughput per system
- 3,000 Watts
- 10,218 BTU

Nation-State Threat Monitoring

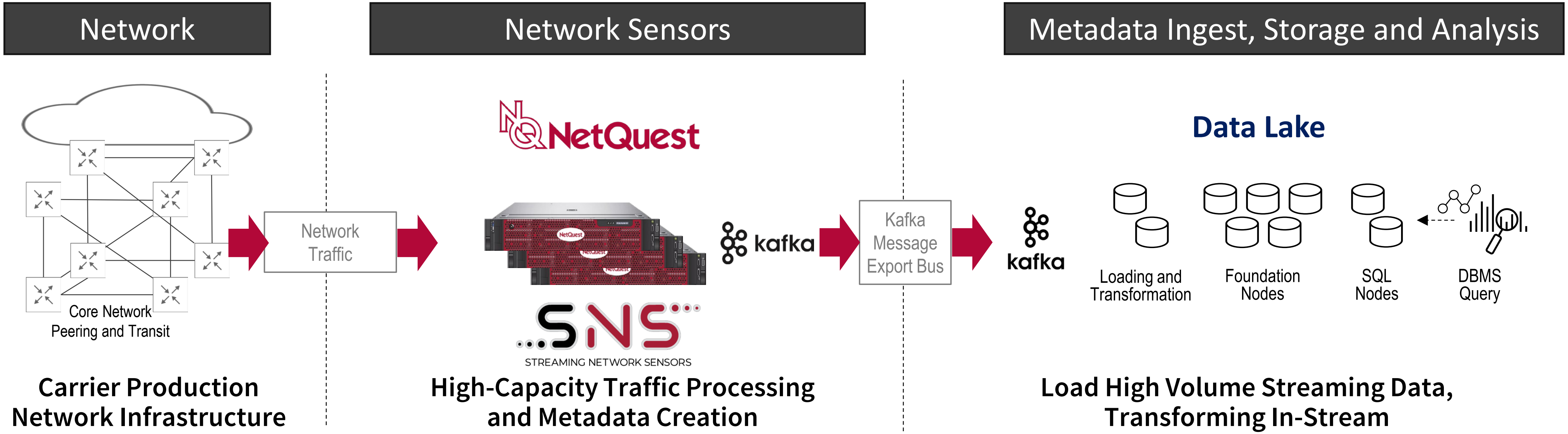
1:1 Flow Metadata Generation at Scale

NetQuest

STREAMING NETWORK SENSORS

Use Case: National Threat Monitoring - Internet Connection Records

- Cyber threat hunting solution enabling Government Agencies to overcome challenges of network traffic security monitoring at massive scale
- Real-time, high-capacity network traffic metadata creation (Internet Connection Records), delivery and analysis to provide mission-critical insights and government-mandated intelligence



Network

Network Sensors

Metadata Ingest, Storage and Analysis

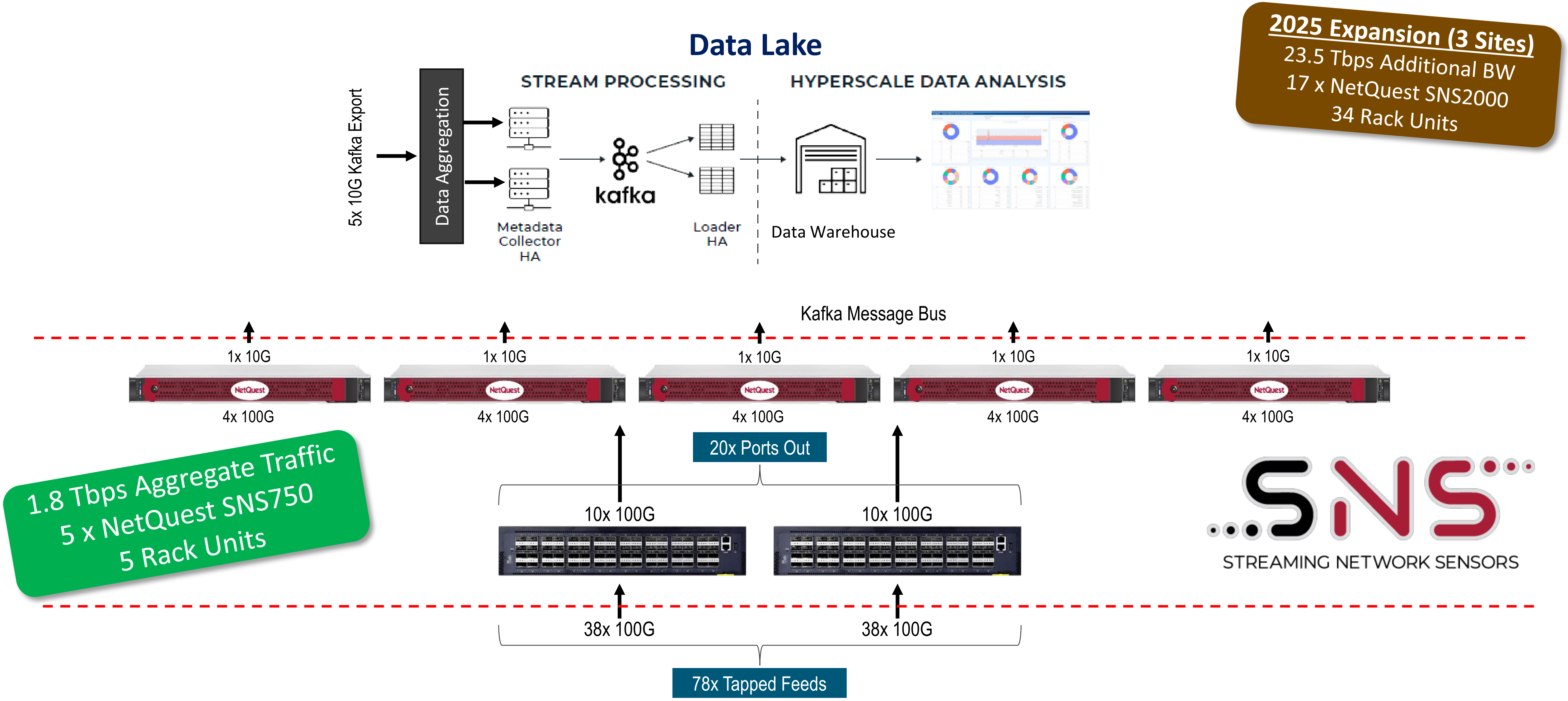
Carrier Production Network Infrastructure

High-Capacity Traffic Processing and Metadata Creation

Load High Volume Streaming Data, Transforming In-Stream

National Threat Monitoring: Current Field Deployment

2025 Expansion (3 Sites)
23.5 Tbps Additional BW
17 x NetQuest SNS2000
34 Rack Units



1.8 Tbps Aggregate Traffic
5 x NetQuest SNS750
5 Rack Units

Traffic Fingerprinting for Cyber Threat Hunting

JA4+ TLS, QUIC and TCP Fingerprinting

NetQuest

STREAMING NETWORK SENSORS

JA4+ Encrypted Session Fingerprinting for Threat Hunting

What It Does:

- Evolution of JA3/JA3S TLS fingerprints
- JA4 computation derives the fingerprint from cryptographic elements of the TLS/QUIC handshake process
- Matched against fingerprints of known malicious clients/servers
- Rapidly identifies harmful activities
- Broad adoption by Threat Intelligence sources and Threat Detection vendors

JA4+ Fingerprinting Use Cases

Scanning for threat actors
Botnet detection
C2 Communication
Session hijacking prevention
Location tracking

NetQuest's Streaming Network Sensor computes JA4+ fingerprints in real-time at terabit scale and includes in metadata records

SNS
STREAMING NETWORK SENSORS

JA4+ Fingerprint Suite for Cyber Threat Hunting

NetQuest
Monitoring Access Solutions

JA4	TLS Client
JA4S	TLS Server Response
JA4T	TCP OS/Device/Application
JA4TS	TCP Server Response
JA4H	HTTP Client
JA4L	Light Distance/Latency Measuring

Application	JA4+ Fingerprints

Chrome	JA4=t13d1518h2_8daaf6152771_e5627efa2ab1 (TCP)
	JA4=q13d0310h3_55b375c5d22e_cd85d2d88918 (QUIC)

IcedID Malware Dropper	JA4H=ge11cn020000_9ed1ff1f7b03_cd8dafe26982

IcedID Malware	JA4=t13d201100_2b729b4bf6f3_9e7b989ebec8
	JA4S=t120300_c030_5e2616a54c73

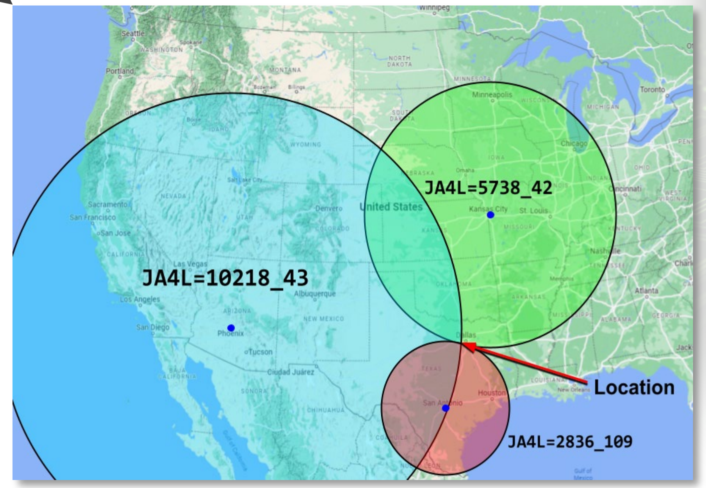
Sliver Malware	JA4=t13d190900_9dc949149365_97f8aa674fd9
	JA4S=t130200_1301_a56c5b993250
	JA4X=000000000000_4f24da86fad6_bf0f0589fc03
	JA4X=000000000000_7c32fa18c13e_bf0f0589fc03

Cobalt Strike	JA4H=ge11cn060000_4e59edc1297a_4da5efaf0cbd
	JA4X=2166164053c1_2166164053c1_30d204a01551

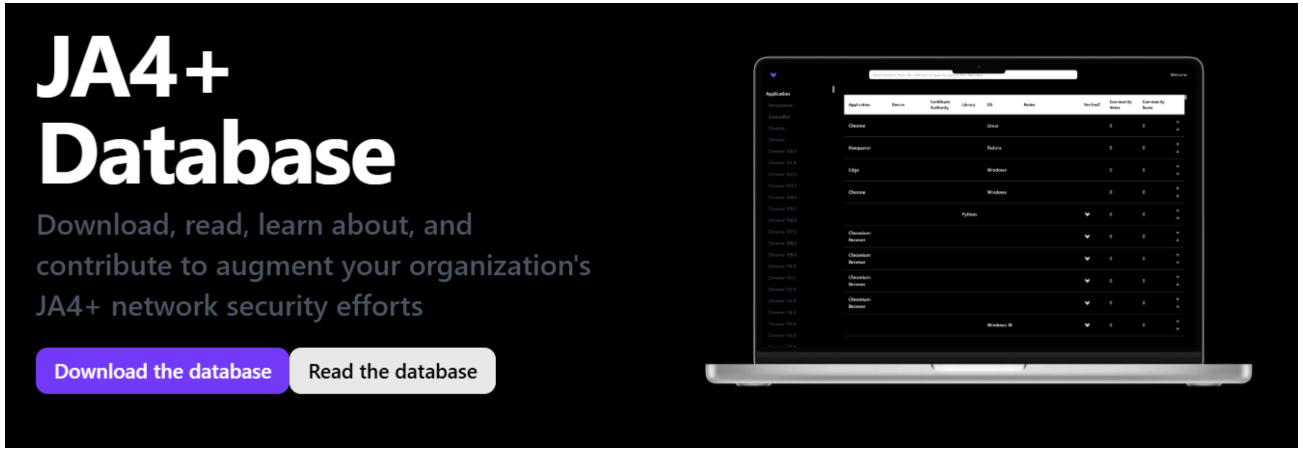
SoftEther VPN	JA4=t13d880900_fcb5b95cb75a_b0d3b4ac2a14 (client)
	JA4S=t130200_1302_a56c5b993250
	JA4X=d55f458d5a6c_d55f458d5a6c_0fc8c171b6ae

Evilginx	JA4=t13d191000_9dc949149365_e7c285222651
Reverse SSH Shells	JA4SSH=c76s76_c71s59_c0s70

JA4L
Measure physical distance by measuring latency between packets at session setup



JA4+ Database for Threat Hunting Community Collaboration



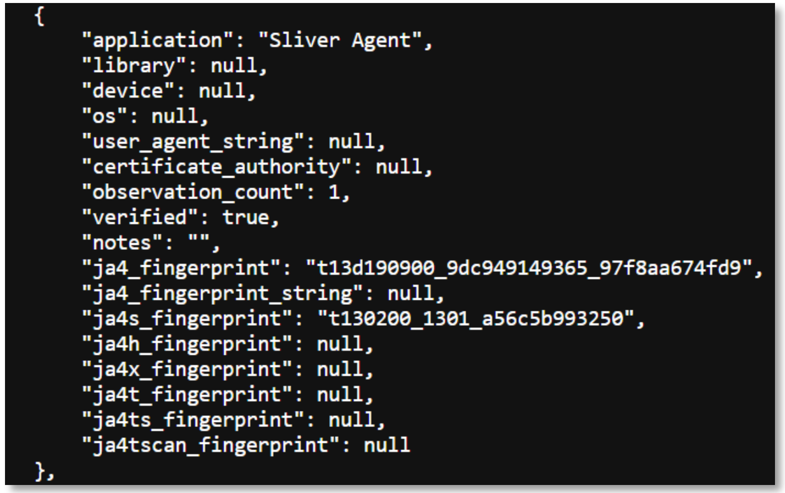
JA4+ Database

Download, read, learn about, and contribute to augment your organization's JA4+ network security efforts

https://ja4db.com/

NetQuest is partnering with FoxIO to enable innovative, high-value next- generation encrypted session fingerprinting at scale

John Althouse
Co-Founder FoxIO



```
{
    "application": "Sliver Agent",
    "library": null,
    "device": null,
    "os": null,
    "user_agent_string": null,
    "certificate_authority": null,
    "observation_count": 1,
    "verified": true,
    "notes": "",
    "ja4_fingerprint": "t13d190900_9dc949149365_97f8aa674fd9",
    "ja4_fingerprint_string": null,
    "ja4s_fingerprint": "t130200_1301_a56c5b993250",
    "ja4h_fingerprint": null,
    "ja4x_fingerprint": null,
    "ja4t_fingerprint": null,
    "ja4ts_fingerprint": null,
    "ja4tscan_fingerprint": null
},
```

5G Multi-Access Edge Threat Monitoring

Use Case: 5G Multi-Access Edge Threat Monitoring

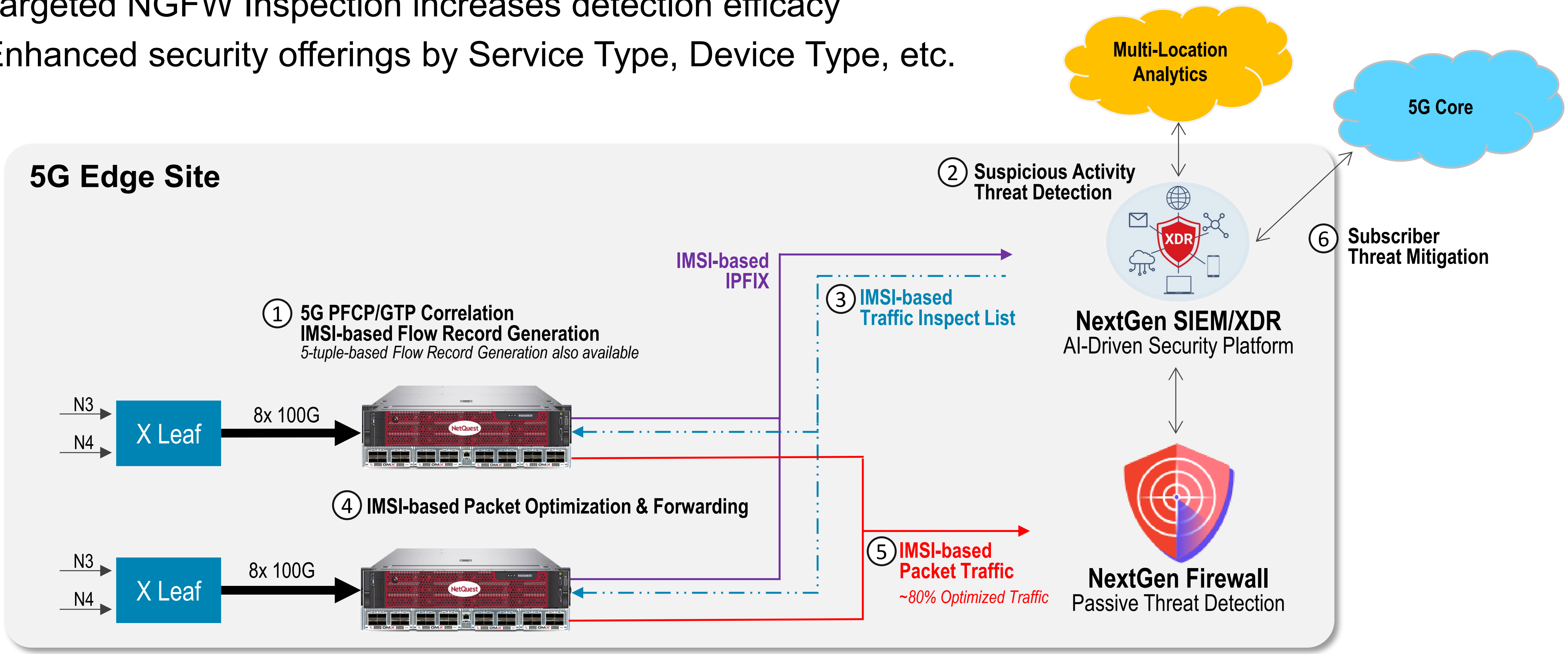
NetQuest

5G Security Monitoring Challenges

- Network Traffic Growth
  - 5G+ / Fixed Wireless Service, Video Streaming, Online Gaming, AR/VR, IoT
- Enhanced Network Services
  - Enhanced Mobile Broadband, Ultra-Reliable Low Latency, Massive Internet of Things
- Expanding Machine to Machine Use Cases
  - Industrial IoT, Robotics Automation, Smart Everything with ML/AI
- 5G Edge Computing
- Increasing Security Threats
- Tool Capacity Constraints & Encryption Limit Visibility

Detecting & Mitigating 5G Service-Affecting Threats

- Optimize Subscriber Threat Detection & Mitigation
  - IMSI-based Flow Records dramatically reduce flow volume for suspicious activity detection
  - IMSI-based packet targeting & optimization dramatically increases scale
  - Targeted NGFW Inspection increases detection efficacy
  - Enhanced security offerings by Service Type, Device Type, etc.



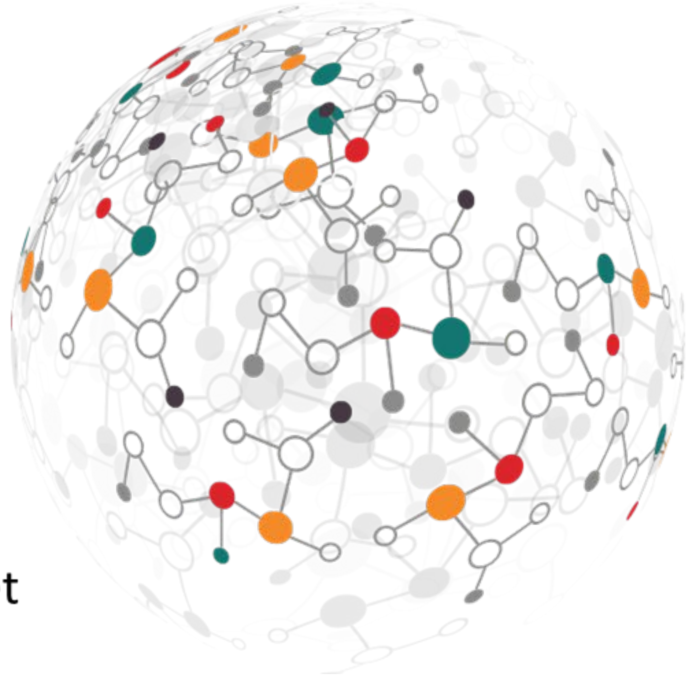
Multi-Location Analytics
5G Core
5G Edge Site
2 Suspicious Activity Threat Detection
XDR
NextGen SIEM/XDR
AI-Driven Security Platform
6 Subscriber Threat Mitigation
IMSI-based IPFIX
3 IMSI-based Traffic Inspect List
1 5G PFCP/GTP Correlation
IMSI-based Flow Record Generation
5-tuple-based Flow Record Generation also available
N3
N4
X Leaf
8x 100G
NetQuest
4 IMSI-based Packet Optimization & Forwarding
5 IMSI-based Packet Traffic
~80% Optimized Traffic
NextGen Firewall
Passive Threat Detection
N3
N4
X Leaf
8x 100G
NetQuest

The NetQuest Advantage

NetQuest
Monitoring Access Solutions

While Others Claim Highest Performance and Capacity, NetQuest Actually Delivers It!

- ✓ Unsampled Flow Metadata at Scale
- ✓ Highest Capacity & Throughput
- ✓ Single-Pass Packet Processing
- ✓ Comprehensive Metadata Set



- ✓ Enriched Metadata at Scale
- ✓ Lowest Power and Space
- ✓ Software-Defined Flexibility
- ✓ Deployment-Proven

Integrated Full Packet Delivery

Next Steps

1. **Lab Testing/CRADA**

2. **Demonstration: Virtual or at our HQ in Mt Laurel, NJ**

Closing Remarks

What We Accomplished Today

1. Explained the concept of "Streaming Network Sensors" and what makes NetQuest Different
2. Explored Use Cases Relevant to DISA and DoD, including monitoring 5G and large scale networks
3. Explained how we can help the War Fighters in mission areas, monitor everything everywhere; turn unstructured data into AI and ML readable structured data; deliver insights about encrypted traffic
4. Answer all questions interactively
5. Discuss any follow up actions desired

Final Questions?

Contacts:

David A Nelson, Federal Sales Director

dnelson@netquestcorp.com

703-9898072

Mike Seidler, VP Product Management

617-529-9209

mseidler@netquestcorp.com

Gene Litt, CTO

609-304-8848

glitt@netquestcorp.com

Rich Moulder, VP Sales

603-203-3350

rmoulder@netquestcorp.com

Key Points about NetQuest

1. Product Maturity Level: TRL 9 (estimated)
2. US Based Company, all SW developed in USA, TAA components, configured and built in the USA
3. Proven at a DoD lab/large carriers
4. Field tested at numerous carriers at scale
5. Ready to go anywhere needed
6. Access to many different Federal Contracts through partners