Enabling Continuous Monitoring with the NIST Cybersecurity Framework

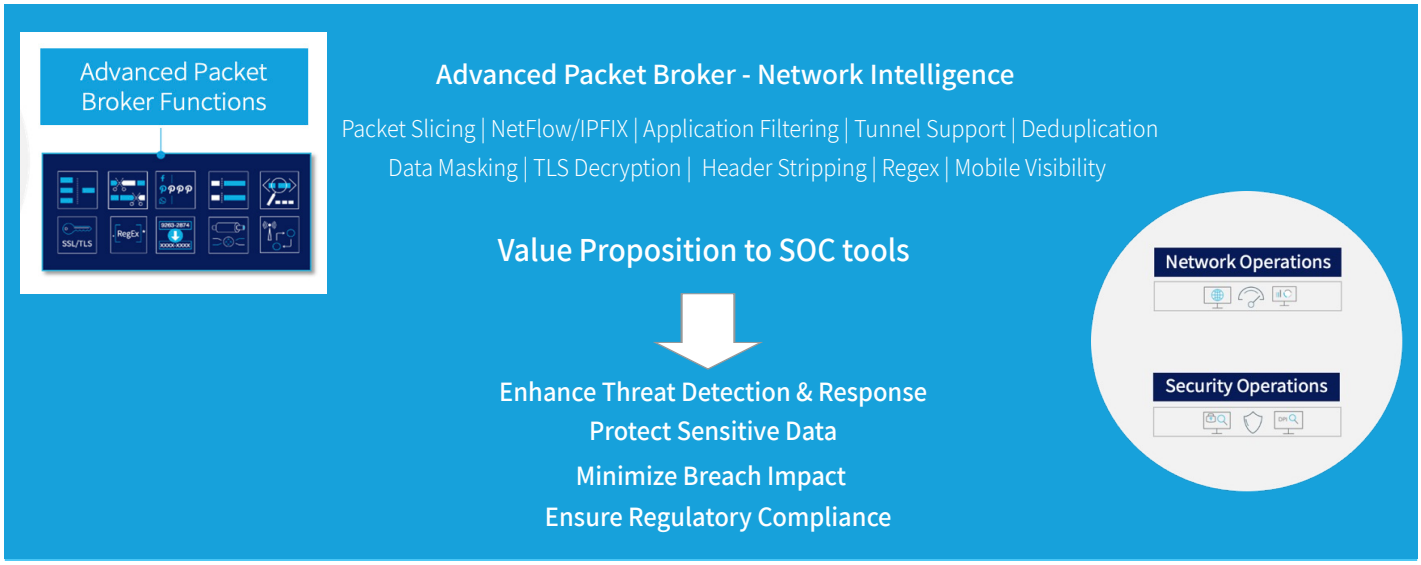
Financial Financial institutions are prime targets for cyberattacks in the era of digital banking and low-latency transactions. To protect customer data without compromising performance, they must adopt cutting-edge visibility and security strategies. Network visibility empowers NetSecOps teams with 360-degree insights to detect threats faster, prevent unauthorized access, and minimize breach impact.

Niagara Networks, based in Silicon Valley, helps leading financial institutions worldwide strengthen security with high-performance visibility and infrastructure protection. Partnering with top technology providers, our solutions deliver reliability, scalability, and cyber resilience, ensuring business continuity and customer trust in mission-critical environments. Our experience in complex projects has created superior value for our customers who deploy reliable, high-performance and flexible visibility solutions to maintain agile Network and Security operations to ensure top cyber resilience and network resiliency. As a result, high-performance and cyber resilient financial services can innovate and scale to new offerings, maintain business continuity, and customer trust.

- 100% packet flow visibility for network traffic intelligence
- NetOps and SecOps tools' efficiency
- Full visibility into encrypted traffic
- Efficient data traffic collection for forensics/SIEM
- Inline bypass for high-availability of threat prevention tools

Solution Highlights

- Advanced traffic visibility up to Layer 7 for network intelligence and improved threat detection
- Aggregation, replication, and tool optimization across physical and virtual networks
- Packet slicing, deduplication, header stripping, data masking, regex filtering
- Flexible load balancing (1:1, 1+1, n+1) for optimized tool performance
- Comprehensive tunnel handling (GTP, GRE, GENEVE, MPLS, VXLAN)
- Embedded 3rd-party tools via the Open Visibility Platform - host any virtualized security applications and monitoring tools
- TLS decryption for visibility into encrypted traffic
- Forensics-ready data collection supporting SIEM and SOC workflows
- Carrier-grade bypass for inline tools, ensuring always-on high-availability



Niagara Visibility & NIST CSF 2.0 (Continuous Monitoring)

Enhancing Threat Detection and Response:
Continuous monitoring enables proactive detection of suspicious activities, such as unauthorized access attempts or malicious traffic. With real-time visibility, organizations can swiftly block threats or isolate affected systems.

Protect your sensitive data with network visibility:
Monitoring and controlling access attempts prevents data theft and misuse, reducing breach impact and safeguarding critical information.

Ensuring Compliance with Regulations:
Regulations such as GDPR, PCI-DSS, and EMV demand robust security. Network visibility provides the evidence required to demonstrate compliance with regulatory frameworks.

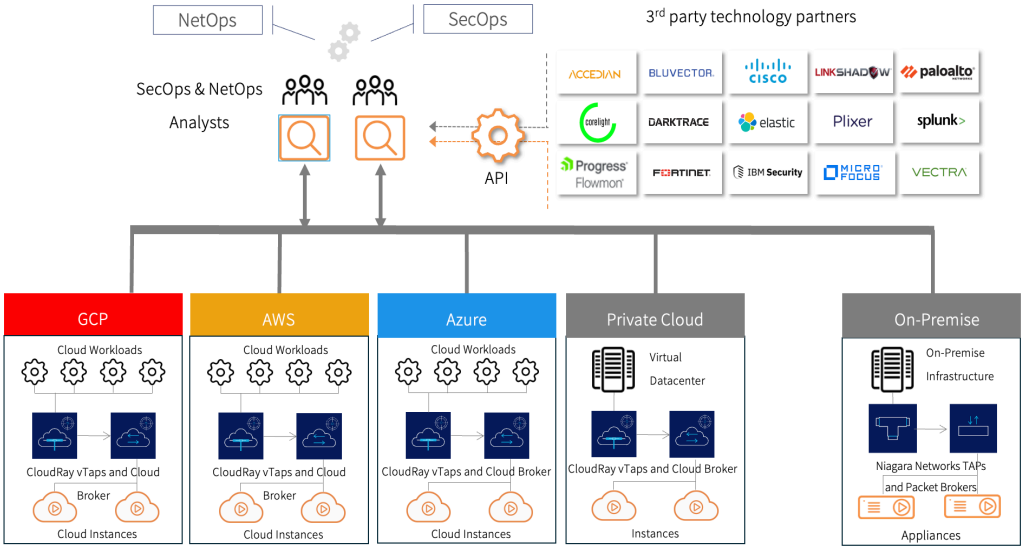
Conclusion

Continuous monitoring is a core requirement of the NIST Cybersecurity Framework 2.0, ensuring that adverse events are detected early and acted upon before they escalate. Traditional methods such as SPAN ports or mirroring are no longer sufficient for today's high-bandwidth and hybrid environments, where blind spots and encrypted traffic can mask threats.
Niagara Networks addresses this challenge by delivering complete, real-time visibility across physical, virtual, and cloud infrastructures. With advanced capabilities such as inline bypass, TLS decryption, packet slicing, and traffic aggregation, Niagara enables NetOps and SecOps teams to continuously monitor all traffic flows, detect anomalies, and ensure compliance. This visibility directly supports the Detect (DE.CM) category of NIST CSF 2.0, helping organizations monitor networks, external services, and computing resources without compromise.

NIST CSF 2.0 Subcategory	How Niagara Visibility Helps
DE.CM-01 – Monitor networks and services	Niagara's advanced packet brokers and TAPs provide 100% traffic visibility (wired, wireless, cloud) so SOC teams can detect anomalies, unauthorized connections, or abnormal flows in real time.
DE.CM-06 – Monitor external service providers	Aggregates and inspects traffic from ISPs, cloud, and remote services, ensuring no blind spots in outsourced or third-party environments.
DE.CM-09 – Monitor computing resources & data	Advanced features like TLS decryption, packet slicing, and data masking allow visibility into encrypted sessions, email/web/file traffic, and authentication events—helping detect malware, exfiltration, or misconfigurations.

NIAGARA NETWORKS

Visibility Solutions Positioned at Strategic Point of Any Network Infrastructure



Streamline & scale networks, services and security posture

Save CAPEX
reduce cost of tools and infrastructure optimization

Reduce risks by enabling visibility and access to 100% of traffic across any infrastructure and enable 100% of network/ tools **uptime**

Niagara Networks is dedicated to enhancing infrastructure security through the use of physical and virtual TAPs and packet brokers. Our cutting-edge technology allows for a seamless flow of network traffic, ensuring uninterrupted network security. With our solutions, you can easily scale up to incorporate future security advancements by simply adding a plug-in. Additionally, our system off-loads resource-intensive processes from traditional infrastructure, resulting in increased IT efficiency and optimized performance.

Discover more @ niagaranetworks.com

Advanced Network Packet Broker | Inline Bypass | Cloud Intelligence Platform | Network TAP | Network Intelligence **Open Visibility** | Visibility Orchestration

ABOUT NIAGARA NETWORKS

Niagara Networks™ is a Silicon Valley based company that pioneered the Open Visibility Platform™ to bring desperately needed agility to network security.

Niagara Networks provides high-performance, high-reliability network visibility and traffic delivery solutions for the world's most demanding service provider and enterprise environments.

We Design, Develop & Manufacture our Products in the Silicon Valley, USA.

NIAGARA NETWORKS

48430 Lakeview Blvd,
Fremont, CA 94538, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529