NIAGARA NETWORKS

Application Note

ECH-Aware TLS Decryption & Intelligent Network Traffic Inspection

Decrypt What Matters. Bypass What Is Private.

Introduction

Enterprise networks are experiencing a fundamental shift in how encrypted traffic is transported, classified, and inspected. TLS 1.3 has strengthened the confidentiality of application communications, while Encrypted Client Hello (ECH), defined in RFC 9849, extends encryption to sensitive information exchanged during the initial TLS handshake.

For security and network operations teams, this evolution creates a visibility challenge. Traditional monitoring systems often rely on the Server Name Indication (SNI) to identify destinations, classify encrypted connections, and determine which security tools should receive specific traffic. With ECH, the real destination hostname is concealed from conventional passive inspection.

At the same time, decrypting every connection is neither operationally efficient nor always appropriate. Enterprises must balance security inspection requirements with privacy obligations, application compatibility, and the processing demands of increasingly high-capacity networks.

Niagara Networks addresses these requirements through its ePacketron Network Intelligence architecture, which combines advanced traffic processing, filtering, and optimization with TLS decryption capabilities. As TLS encryption continues to evolve, ePacketron extends its inspection capabilities with support for Post-Quantum Cryptography (PQC), enabling authorized TLS 1.3 decryption across supported hybrid & post-quantum key-exchange environments. With X25519MLKEM768 enabled by default and support for ML-KEM-1024, ePacketron helps enterprises maintain actionable encrypted traffic visibility while supporting the transition toward quantum-resistant communications.

For SOC and NOC teams, the Encrypted Client Hello (ECH / RFC 9849) standard creates a major visibility challenge.

Traditional monitoring systems often rely on the Server Name Indication (SNI) to identify destinations, classify encrypted connections, and steer traffic to appropriate security tools.

With ECH, the real destination hostname is concealed from conventional passive inspection.

The enhanced architecture combines ECH-aware interception, post-quantum key-exchange support & category-based selective decryption, enabling a more intelligent approach to encrypted traffic visibility.

Decrypt What Matters. Bypass What Is Private.

This principle establishes a practical approach to encrypted traffic inspection: prioritize connections that require security analysis while allowing privacy-sensitive traffic to remain encrypted according to organizational policy.

Rather than forcing every connection through the same inspection process, the architecture is designed to help security teams make informed decisions about traffic handling and deliver relevant information to downstream NDR, IDS, IPS, and monitoring systems.

The ECH Visibility Challenge

From TLS 1.3 to Encrypted Client Hello

TLS 1.3, defined in RFC 8446, provides modern encryption for communications between clients and servers. However, in a conventional TLS 1.3 connection without ECH, the ClientHello typically exposes the SNI extension. This information allows network monitoring and security infrastructure to identify the requested hostname without decrypting application payloads. For example, when a user connects to www.example.com, a conventional passive monitoring tool may observe that hostname in the TLS handshake. The tool can use the information for traffic classification, domain-based policies, and routing decisions.

ECH CHANGES THIS BEHAVIOR.

Defined in RFC 9849, ECH uses Hybrid Public Key Encryption (HPKE), specified in RFC 9180, to protect the inner ClientHello containing the actual destination hostname and other sensitive handshake information. A passive observer generally sees the outer ClientHello, which does not reliably disclose the true destination.

The operational impact

The introduction of ECH affects several established network security workflows.

Traffic classification: Hostname-based identification becomes less reliable when the true SNI is encrypted.

Security policy enforcement: Policies that depend on observing the destination hostname may require additional information or a different enforcement architecture.

Threat detection: Monitoring systems may lose a useful signal for identifying suspicious destinations and correlating encrypted connections with threat intelligence.

Traffic steering: Network Packet Brokers and visibility platforms that depend on SNI for classification cannot reliably steer ECH-protected traffic using that field alone.

ECH does not make traffic completely invisible. Network tools can still observe available IP-layer information, traffic characteristics, and other permitted metadata. However, these signals may not provide the same application-level destination context as the true SNI.

Why the visibility architecture must evolve

As ECH adoption expands, enterprises will need visibility architectures that do not depend exclusively on passive inspection of unencrypted TLS handshake fields. The challenge is not simply recovering a hostname. It is maintaining effective security inspection and traffic delivery while respecting the encryption, privacy, and trust requirements of modern applications.

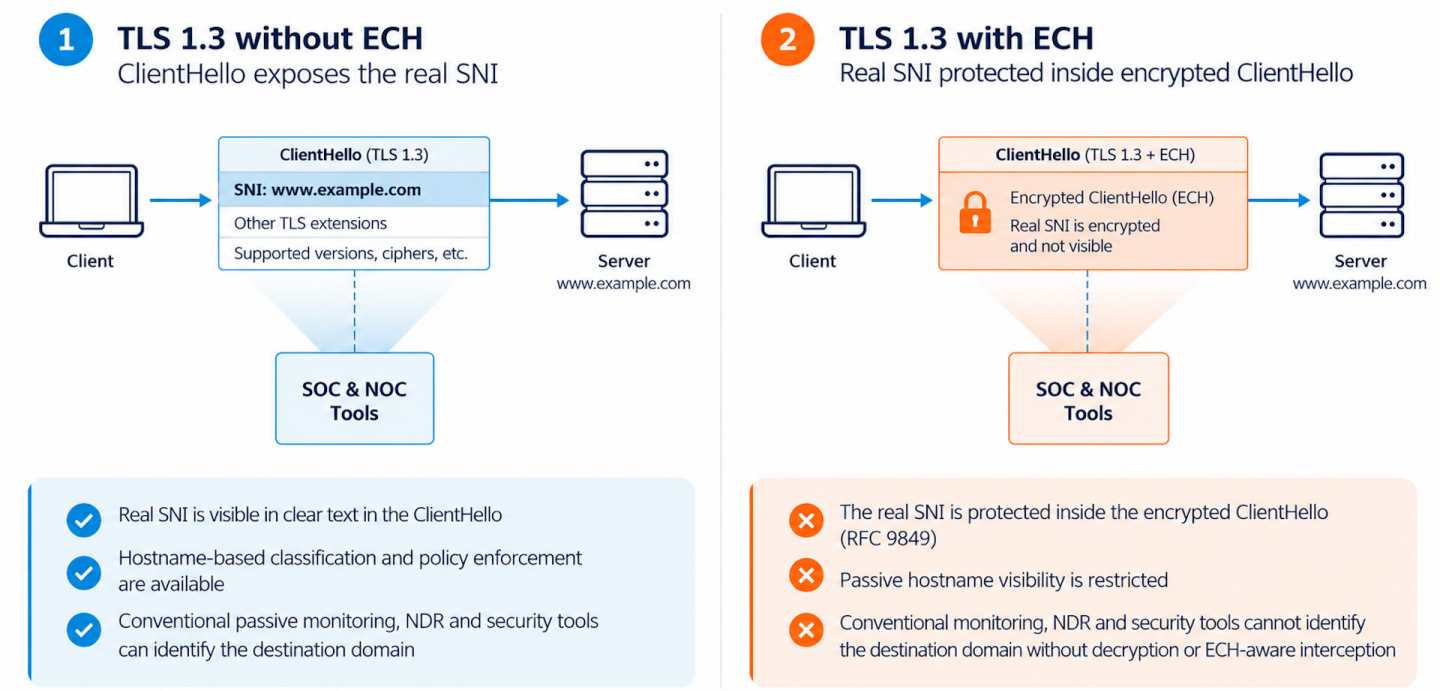


Figure 1: Traditional TLS versus ECH — TLS 1.3 with and without Encrypted ClientHello.

The ePacketron Approach to ECH-Aware TLS Inspection

Extending Network Intelligence into encrypted traffic

ePacketron delivers up to 600 Gbps* of accelerated packet processing, enabling high-performance Network Intelligence that transforms, filters & optimizes network traffic before it reaches downstream security & monitoring tools. Its architecture combines advanced packet-processing capabilities, including intelligent filtering, traffic optimization & TLS decryption, to enhance encrypted traffic visibility while maximizing the efficiency of existing security infrastructure.

* Note: The 600 Gbps refers to overall packet-processing capacity, not TLS decryption throughput.

The ECH-aware enhancement extends this approach to encrypted connections whose destination information is no longer available through conventional passive SNI inspection. Rather than relying solely on observable handshake metadata, the proposed architecture uses authorized active interception to obtain the destination information required for policy enforcement and inspection.

ePacketron ECH-Aware Network Intelligence Solution

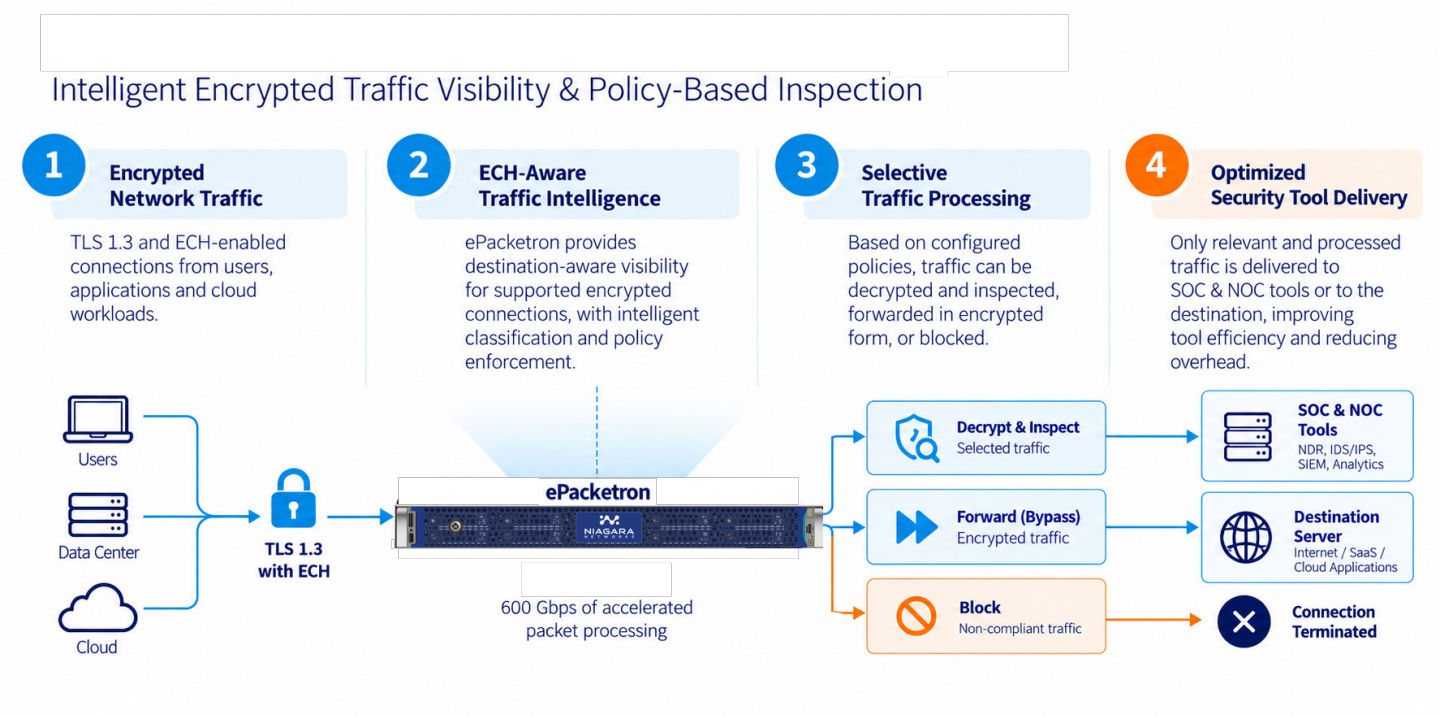


Figure 2: ePacketron ECH-Aware Network Intelligence Solution.

Architecture Objective: Enable actionable visibility into ECH-protected traffic through intelligent classification, selective TLS inspection & high-performance traffic processing, while supporting privacy-aware bypass policies & optimized security tool delivery.

Unlike approaches that rely on blocking ECH or forcing connections to fall back to non-ECH TLS, the ePacketron architecture is designed to support ECH-aware visibility & selective TLS inspection in compatible enterprise environments.

By combining destination-aware traffic intelligence, policy-based inspection & up to 600 Gbps* of accelerated packet processing, ePacketron is designed to help organizations maintain actionable visibility into encrypted traffic while optimizing delivery to downstream security & monitoring tools.

* Note: The 600 Gbps refers to overall packet-processing capacity, not TLS decryption throughput.

Deployment and trust requirements

ECH-aware TLS interception requires an active inspection architecture with appropriate network placement, certificate trust & client compatibility. Unlike passive network monitoring, active interception establishes the necessary TLS processing context to support authorized inspection. Deployment requirements depend on the client implementation, certificate validation, ECH negotiation behavior & enterprise security policies. Applications using certificate pinning or other interception restrictions may require alternative inspection policies or encrypted bypass. ECH-aware inspection should therefore be implemented within a controlled enterprise environment, with clearly defined security policies & supported deployment configurations.

Post-Quantum TLS 1.3 Inspection

Extending Encrypted Traffic Visibility into the Post-Quantum Era

As enterprises prepare for the transition to Post-Quantum Cryptography (PQC), TLS 1.3 is evolving to support quantum-resistant key establishment. The adoption of post-quantum algorithms introduces new requirements for network security infrastructure, particularly for organizations that rely on TLS decryption to maintain visibility into encrypted application traffic.

Niagara Networks' ePacketron extends its TLS inspection capabilities to support post-quantum key exchange, enabling authorized TLS interception across separate client-side & server-side connections. Post-quantum key-exchange groups are enabled by default on both TLS legs, with X25519MLKEM768 as the preferred hybrid configuration, combining classical X25519 key exchange with ML-KEM-768. The solution also supports ML-KEM-1024 when negotiated with compatible peers.

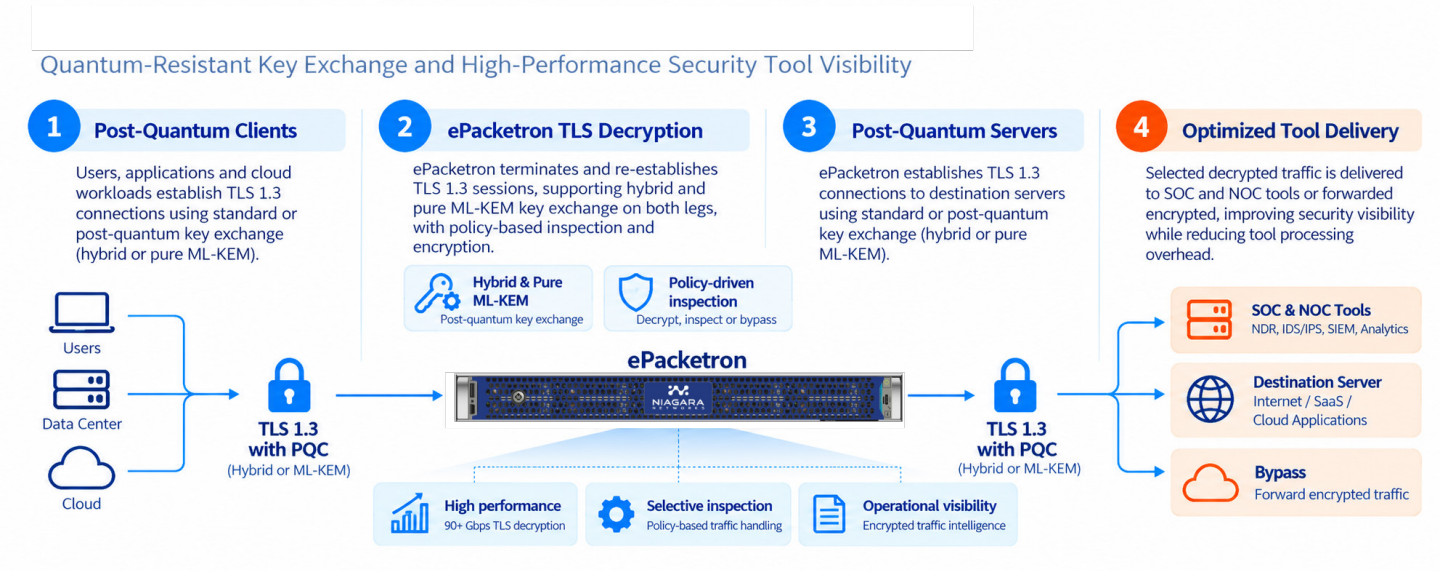


Figure 3: Post-Quantum TLS 1.3 Decryption with ePacketron.

By integrating post-quantum key-exchange support with ECH-aware decryption, selective inspection & high-performance Network Intelligence, ePacketron helps enterprises maintain security-tool visibility as encrypted communications evolve. Selected decrypted traffic can be delivered to downstream SOC & NOC tools, while connections excluded from inspection remain encrypted according to configured security policies.

Architecture Objective: Preserve actionable TLS visibility across supported classical, hybrid & post-quantum key-exchange environments while enabling policy-driven inspection, privacy-aware bypass & optimized security-tool delivery.

Deployment consideration: Post-quantum TLS negotiation depends on compatible client & server implementations, supported cryptographic groups, certificate trust & the configured interception architecture. PQC key-exchange support does not imply that every application or encrypted connection can be intercepted.

Decrypt What Matters. Bypass What Is Private.

Traditional TLS inspection architectures may decrypt broad categories of traffic before passing them to security tools for analysis. Although this approach provides access to encrypted payloads, it can introduce unnecessary processing overhead, expose sensitive information, and increase the operational burden on security infrastructure.

A more effective approach is to apply policies that determine which connections require decryption and which should remain encrypted. Category-based selective decryption is designed to combine destination classification, reputation intelligence, and customer-defined policies to support these decisions.

Privacy-Aware Decryption Bypass

Many enterprises handle encrypted communications involving financial information, medical records, legal services, and other confidential data. Decrypting these connections without a specific security justification may create unnecessary privacy exposure and complicate compliance management.

Privacy-aware bypass policies can allow designated traffic categories to remain encrypted while continuing through the appropriate network forwarding path. Examples include banking services, healthcare portals, legal applications, and other privacy-sensitive destinations defined by the organization. This approach can support data minimization, privacy-by-design principles, and internal security governance policies.

Importantly, category-based bypass is a configurable security policy, not a universal regulatory requirement. Organizations must determine the appropriate treatment of traffic based on applicable laws, risk assessments, and internal policies.

Threat-Driven Selective Decryption

While some categories should remain encrypted, other connections may require closer inspection. Suspicious destinations, phishing infrastructure, malware distribution services, and command-and-control communications can exploit encrypted channels to conceal malicious activity. Threat-driven selective decryption enables inspection policies to prioritize these higher-risk connections.

Depending on the supported deployment architecture and organizational policy, suspicious traffic may be decrypted for deeper analysis, blocked, or forwarded to designated security infrastructure. This enables security teams to focus inspection resources on traffic that presents greater risk instead of processing every encrypted connection equally.

Category and reputation intelligence

Integrating web categorization and reputation intelligence into ePacketron TLS decryption and packet-processing engine introduces an additional layer of Network Intelligence, enabling more contextual & selective traffic inspection. By combining destination classification, threat reputation & organizational security policies, ePacketron can support more informed decisions about which traffic should be decrypted, inspected, bypassed or blocked. This approach is designed to improve security visibility while reducing unnecessary decryption, protecting sensitive communications & optimizing downstream security tool performance.

ECH-Aware Classification

For ECH-protected connections, destination classification depends on the availability of reliable destination information. Because ECH conceals the actual hostname, classification may require supported interception capabilities or alternative destination-identification methods. Consequently, policy enforcement must account for the availability & reliability of destination intelligence before applying category-based inspection decisions.

Value Proposition: Enable intelligent, policy-driven TLS inspection that prioritizes security-relevant traffic, respects privacy requirements & reduces unnecessary processing overhead.

Example category-based policy matrix

Traffic category	Illustrative policy	Value
Financial services	Bypass decryption	Minimize exposure of sensitive financial information
Healthcare	Bypass decryption	Support privacy requirements
Legal & confidential	Bypass decryption	Preserve confidentiality
Malware & phishing	Block or decrypt & inspect	Support threat prevention & detection
Command-and-control (C2)	Block or inspect	Reduce malicious communication
Unknown or suspicious	Selective inspection	Improve threat investigation
Trusted business applications	Bypass decryption or forward	Reduce processing overhead

Note: These policies are illustrative and require appropriate customer configuration & Niagara Networks' technical engineering support.

Intelligent decryption policy workflow



Figure 4: Intelligent decryption policy workflow.

High-Performance Network Intelligence

Security visibility without unnecessary processing

Decrypting encrypted traffic requires substantial processing resources. TLS handshakes, cryptographic operations, connection state management, and traffic forwarding all contribute to the demands placed on inspection infrastructure. As network capacity increases, organizations need architectures that preserve traffic performance while providing security tools with the information required for effective analysis. ePacketron addresses this challenge through a high-performance Network Intelligence architecture designed to process and optimize traffic before delivery to downstream systems.

Selective processing and fast-path forwarding

Not every encrypted connection requires payload inspection. Traffic that is approved for bypass can remain encrypted, avoiding unnecessary TLS termination and re-encryption operations.

Connections selected for inspection can be directed through the appropriate TLS processing path, while other traffic continues through a more efficient forwarding path. This separation can help reduce processing overhead and preserve capacity for security-relevant traffic.

Optimized traffic delivery

The goal is not simply to maximize raw decryption throughput. It is to deliver the appropriate level of inspection while preserving overall network and security-tool efficiency.

TLS decryption is only one component of the broader network visibility challenge. Security tools must also receive traffic in the appropriate format and volume. ePacketron's advanced packet-processing capabilities include filtering, packet slicing, deduplication, and other traffic optimization functions. Combined with selective TLS processing, these capabilities can help organizations reduce unnecessary traffic delivery and improve utilization of downstream monitoring and security infrastructure.

Performance considerations

Evaluating TLS inspection performance requires more than a single throughput figure. Important measurements include:

- Decryption throughput: The sustained traffic capacity processed through TLS inspection.
- New connections per second: The rate at which new connections can be established.
- Full TLS handshakes per second: The rate of complete cryptographic handshake operations.
- Concurrent connections: The number of active TLS sessions maintained simultaneously.

These metrics should be evaluated independently because performance depends on traffic characteristics, cipher suites, connection behavior, packet sizes, and inspection configuration.

Enterprise Use Cases

Use Case 1 - Privacy-Sensitive Enterprise Traffic

Challenge: Large enterprises handle encrypted communications across financial, healthcare, legal, and other sensitive applications. Blanket TLS decryption can expose confidential data unnecessarily and create additional privacy governance requirements.

Proposed solution: Category-based bypass policies allow designated traffic to remain encrypted while other connections continue through the appropriate inspection workflow.

Business outcome: Organizations can reduce unnecessary access to sensitive payloads, support privacy policies, and allocate inspection resources more selectively.

Use Case 2 - Threat Detection in Encrypted Traffic

Challenge: Attackers increasingly use encrypted communications to distribute malicious content, contact command-and-control infrastructure, and conceal suspicious network activity. ECH further limits the availability of hostname information used by conventional passive monitoring systems.

Proposed solution: ECH-aware interception, combined with category and reputation intelligence, can help identify eligible connections that require deeper inspection. Selected decrypted traffic can then be delivered to downstream security tools for analysis, subject to supported product capabilities.

Business outcome: Security teams can improve inspection focus and make better use of existing detection infrastructure without requiring blanket decryption.

Use Case 3 - High-Capacity Security Infrastructure

Challenge: High-speed networks generate large traffic volumes that can place significant demands on TLS inspection systems and downstream security tools. Processing unnecessary traffic consumes resources that could otherwise support more important security workloads.

Proposed solution: Combine selective TLS processing with ePacketron's traffic filtering, transformation, and optimization capabilities. Traffic that does not require decryption can bypass cryptographic processing, while selected traffic receives the appropriate inspection treatment.

Business outcome: Organizations can improve processing efficiency, reduce unnecessary security-tool workloads, and support scalable network visibility architectures.

Deployment Considerations

ECH-aware TLS inspection introduces technical and operational requirements that must be considered during solution design.

Network placement

Passive monitoring can observe available metadata but cannot independently decrypt ECH-protected handshake information. Active interception requires a suitable deployment architecture with control over the relevant TLS connection path.

Certificate trust

TLS interception generally requires appropriate certificate trust relationships between enterprise clients and the interception system. Organizations must ensure that these trust relationships are deployed and managed securely.

ECH compatibility

Client behavior, ECH configuration, retry handling, and certificate validation can influence interception compatibility. Not all applications or browsers necessarily support the same interception workflow.

Application certificate pinning

Applications using certificate pinning or other anti-interception controls may reject substituted certificates. These applications may require bypass policies or alternative security controls.

Privacy and governance

Selective decryption policies should reflect organizational risk requirements, applicable privacy regulations, and approved inspection practices. Policy decisions should be documented, reviewed, and updated as business and security requirements evolve.

Integration with security infrastructure

The inspection architecture should support the appropriate delivery of selected traffic to existing security and monitoring tools. Design considerations include traffic volume, inspection capacity, forwarding requirements, tool compatibility, and failure handling.

Conclusion

Intelligent Decryption for the Next Generation of Network Visibility

As encryption technologies evolve, enterprises need security architectures that maintain actionable visibility without compromising operational efficiency or privacy objectives. ECH represents an important change in TLS traffic visibility, limiting the destination information available to conventional passive inspection. At the same time, increasing network capacity and growing security workloads make indiscriminate decryption increasingly difficult to justify.

Niagara Networks' ePacketron Network Intelligence architecture provides a foundation for advanced traffic processing, transformation, and optimization. By combining ECH-aware interception, post-quantum TLS 1.3 key-exchange support, selective decryption & category-based intelligence, ePacketron extends high-performance Network Intelligence into the next generation of encrypted traffic visibility.

The guiding principle is clear:

Decrypt What Matters. Bypass What Is Private.

By prioritizing security-relevant traffic, supporting privacy-aware bypass policies, and optimizing delivery to downstream security tools, organizations can build more efficient and adaptable network visibility architectures.

High-Performance Network Intelligence That Transforms & Optimizes Traffic Before Downstream Tools.

Explore the product page. >

About Niagara Networks

Niagara Networks is a Silicon Valley-based company delivering high-performance, reliable network visibility and traffic delivery solutions for mission-critical environments. Our solutions empower Security and Network Operations Centers (SOC/NOC) with complete visibility and actionable intelligence across physical, virtual, and cloud networks. As a former division of Interface Masters, we provide all the building blocks for an advanced Visibility Layer, including packet brokers, bypass switches, network TAPs, and unified management software, offering a single pane of glass for simplified visibility infrastructure. For more information please visit us at www.niagaranetworks.com.

Copyright © 11/ 2026 Niagara Networks™. All rights reserved. Product specifications are subject to change without notice or obligation

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