Niagara Networks and Endace

Blueprint for Complying with TSA Emergency Cybersecurity Requirements.

TSA emergency actions require US Airports and Aircraft Operators to implement continuous cybersecurity monitoring, detection, and response capabilities.

The Endace and Niagara Networks joint solution is proven in airport deployments for this very purpose. It enables airports to comply with TSA mandates and securely monitor, investigate, and protect against, cyber-attacks on critical infrastructure.

TSA emergency action

TSA is taking this emergency action because of persistent cybersecurity threats against the aviation sector. Disrupting operations can cause significant economic and social damage, making airports and aircraft operators a prime target for threat actors.

TSA administrator David Pekoske stated "*Protecting our nation's transportation system is our highest priority and TSA will continue to work closely with industry stakeholders across all transportation modes to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient travel*"

https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft

Airports are vast ecosystems comprising many interconnected systems, including security cameras, access control systems, baggage handling, air traffic control, and passenger Wi-Fi networks. The sheer scale and complexity of these networks creates numerous entry points for cyber attackers to exploit vulnerabilities and gain unauthorized access.

Many airports continue to be reliant on legacy systems that were not designed with modern cybersecurity in mind. These legacy technologies often lack regular security updates, leaving them vulnerable to known exploits. Integrating new technologies with legacy systems can also introduce additional security gaps and complexities.

This TSA emergency amendment requires entities to improve resiliency and prevent disruption and degradation of their infrastructure. One of the key areas of focus is to implement continuous monitoring and detection policies and procedures to defend against, detect and respond to cybersecurity threats and anomalies.

A field proven solution from Niagara Networks and Endace

This joint solution is deployed, operational, and has proven its ability to enable compliance with emergency TSA mandates at large US airports.

Niagara Networks provides an advanced visibility adaptation layer including TAPs, bypass switches, advanced network packet brokers and a unified management layer. Teams can easily and efficiently manage multiple security tools, enabling scale and flexibility while reducing operational expense and downtime across the entire spectrum of airports' digital assets.

PRODUCTS

Niagara Networks Visibility Intelligence

EndaceProbe Analytics Platform with Application Dock

BENEFITS

- Enables compliance with the TSA emergency requirements.
- Remediate any incident by leveraging weeks or months of full-packet capture at your fingertips.
- Eliminate blind spots in physical, virtual, and cloud networks to increase the overall 360-degree security posture.
- Expose and investigate threats hiding in encrypted traffic including TLS 1.3 encrypted data flows.
- Scalable traffic optimization supports terabytes of aggregation capacity, filtering, and deduplication allowing traffic to be directed to where it's needed in the right format.
- Streamlined investigation workflows from other tools your SecOps or NetOps teams use.
- One-click access to full definitive packet evidence accelerates investigation to remediation and enables accurate reconstruction of events.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.

Packet capture provides the hard evidence needed to hunt for and combat even the most serious threats. EndaceProbes provide weeks or months of 100% accurate packet capture across the entire network. Endace's scalable enterprise class packet capture provides a single, unified view of network activity across all network traffic – including on-premise, branch and cloud assets – from a single central console.

Threats hiding within encrypted communications can be exposed by safely decrypting and capturing traffic in line or out of band. Decrypted traffic can be delivered to security tools to maximize threat and anomaly detection.

An open API and turnkey integrations between Endace and your favorite security tools put packet evidence at your fingertips. One click access to full pcap data is available from all your favorite tools – SIEM, SOAR, IDS, and more.

Network and security monitoring capability can be extended by deploying instances of virtual security tools on any EndaceProbe. Hosted solutions – from partners including Cisco, Darktrace, Palo Alto Networks, Fortinet and many others – can analyze traffic at full line-rate for real-time detection.

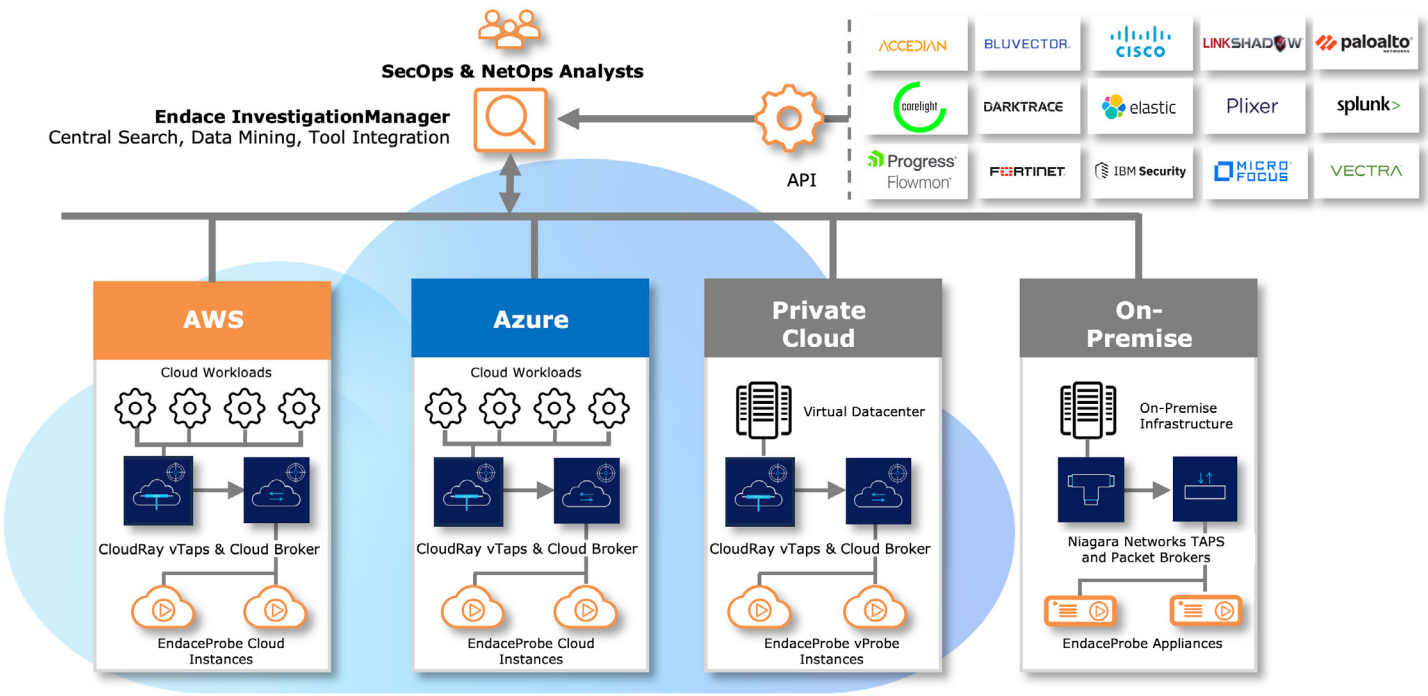
Conclusion

The joint solution from Endace and Niagara Networks gives security teams a robust solution for complying with the TSA emergency amendment. This solution provides the definitive evidence that teams need to investigate and resolve even the most complex cybersecurity threats.

Combining the two technologies lets security teams respond to alerts faster, and investigate threats with more confidence, across both their physical and cloud environments. Decryption of traffic before it is recorded gives SecOps teams visibility into threats that might otherwise be hidden in encrypted traffic.

Additionally, by hosting third-party analytics tools in the EndaceProbe's Application Dock hosting environment, customers can extend monitoring coverage without additional hardware deployments, enabling them to reduce cost by leveraging EndaceProbe hardware to deploy increased traffic monitoring and analysis capability.

Total Hybrid Cloud Visibility and Always-on Hybrid-Cloud Packet Capture



International Airport Cybersecurity Monitoring Deployment and Workflow

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com