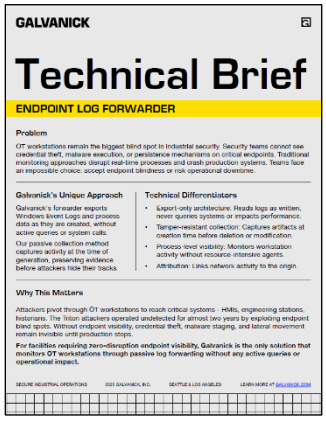
GALVANICK

carahsoft.


GALVANICK

Technical Brief

ENDPOINT LOG FORWARDER

Problem

OT workstations remain the biggest blind spot in industrial security. Security teams cannot see credential theft, malware execution, or persistence mechanisms on critical endpoints. Traditional monitoring approaches disrupt real-time processes and crash production systems. Teams face an impossible choice: accept endpoint blindness or risk operational downtime.

Galvanick's Unique Approach

Galvanick's forwarder exports Windows Event Logs and process data as they are created, without active queries or system calls.

Our passive collection method captures activity at the time of generation, preserving evidence before attackers hide their tracks.

Technical Differentiators

- Export-only architecture: Reads logs as written, never queries systems or impacts performance.
- Tamper-resistant collection: Captures artifacts at creation time before deletion or modification.
- Process-level visibility: Monitors workstation activity without resource-intensive agents.
- Attribution: Links network activity to the origin.

Why This Matters

Attackers pivot through OT workstations to reach critical systems - HMIs, engineering stations, historians. The Triton attackers operated undetected for almost two years by exploiting endpoint blind spots. Without endpoint visibility, credential theft, malware staging, and lateral movement remain invisible until production stops.

For facilities requiring zero-disruption endpoint visibility, Galvanick is the only solution that monitors OT workstations through passive log forwarding without any active queries or operational impact.

SECURE INDUSTRIAL OPERATIONS 2025 GALVANICK, INC. SEATTLE & LOS ANGELES LEARN MORE AT GALVANICK.COM

Endpoint Log Forwarder

Thank you for downloading this Galvanick technical brief. Carahsoft is the government solutions provider for Galvanick cybersecurity solutions available via NASA SEWP V, E & I, The Quilt, and other contract vehicles.

To learn how to take the next step toward acquiring Galvanick's solutions, please check out the following resources and information:

For additional resources:
carah.io/GalvanickResources

For upcoming events:
carah.io/GalvanickEvents

For additional Galvanick solutions:
carah.io/GalvanickSolutions

For additional cyber solutions:
carah.io/Cybersecurity

To set up a meeting:
Galvanick@carahsoft.com
844-445-5688

To purchase, check out the contract vehicles available for procurement:
carah.io/GalvanickContracts

GALVANICK

Technical Brief

ENDPOINT LOG FORWARDER

Problem

OT workstations remain the biggest blind spot in industrial security. Security teams cannot see credential theft, malware execution, or persistence mechanisms on critical endpoints. Traditional monitoring approaches disrupt real-time processes and crash production systems. Teams face an impossible choice: accept endpoint blindness or risk operational downtime.

Galvanick's Unique Approach

Galvanick's forwarder exports Windows Event Logs and process data as they are created, without active queries or system calls.

Our passive collection method captures activity at the time of generation, preserving evidence before attackers hide their tracks.

Technical Differentiators

- Export-only architecture: Reads logs as written, never queries systems or impacts performance.
- Tamper-resistant collection: Captures artifacts at creation time before deletion or modification.
- Process-level visibility: Monitors workstation activity without resource-intensive agents.
- Attribution: Links network activity to the origin.

Why This Matters

Attackers pivot through OT workstations to reach critical systems - HMIs, engineering stations, historians. The Triton attackers operated undetected for almost two years by exploiting endpoint blind spots. Without endpoint visibility, credential theft, malware staging, and lateral movement remain invisible until production stops.

For facilities requiring zero-disruption endpoint visibility, Galvanick is the only solution that monitors OT workstations through passive log forwarding without any active queries or operational impact.