

## ThunderCat and Devo Partnership

ThunderCat Technology is a Service-Disabled Veteran Owned Small Business that delivers technology services and solutions to government organizations, educational institutions, and commercial companies. ThunderCat brings an innovative approach to solving customer problems in and around the datacenter.

ThunderCat, an SDVOSB with multiple contract vehicles, holds industry specific certifications and provides industry leading resources to help federal and commercial customers achieve their mission.

Our results-oriented consultative approach and a creative ideology provide immediate value to customers. We are active with various veterans' charities and are founded and owned by a combat wounded veteran who truly believes in giving back to the community.

### The Devo Platform

Release the Full Potential of All Your Data for Logging, Security, and IT Operations Needs

SOC analysts have a lot on their plates. Poor visibility across the defense surface, isolated threat alerts with no context, low-fidelity alerts coming in at a high volume, and slow investigations that span multiple tools make it nearly impossible for teams to respond to threats fast enough. With 78% of security professionals indicating that "working in the SOC is very painful", it is critical for analysts and SOC managers to be empowered to succeed.

In an effort to speed and improve analyst workflows, organizations across the Public Sector are relying on Devo to address

common use cases including centralized logging, SIEM, compliance, fraud detection and more using the Devo cloud-native SaaS solution. The Devo Platform and its integrated Devo Security Operations application empowers SOC leaders and analysts to view and respond to the entire threat landscape in minutes, not days or weeks. Devo isn't just for security teams, all teams—IT included—can use the same instance of Devo for use cases too, to take advantage of the same cloud-native flexibility, speed, and scale.

### Accelerate Your Shift to the Cloud and Your Compliance with the EO

- As a cloud-native solution, Devo enables successful shifts to the cloud
- Devo is a fiscally accessible tool for organizations looking to quickly move to EL3, complying with OMB Guidance and Executive Order 14028

### Build A Modern Foundation for Your SOC

- Get full visibility into all your data with Devo—400 days hot—for faster, more accurate threat investigations
- Use Devo's embedded threat intelligence platform to enrich with threat context and to guide analysts
- Devo's entity analytics point analysts to

anomalous behaviors, surfacing threats to your organization automatically

- Devo's incident response and investigation workflow enables your team to respond rapidly
- Automated Devo enrichments and third-party integrations inform your SOC analysts, enabling them to streamline their triage, investigation, and hunting workflows

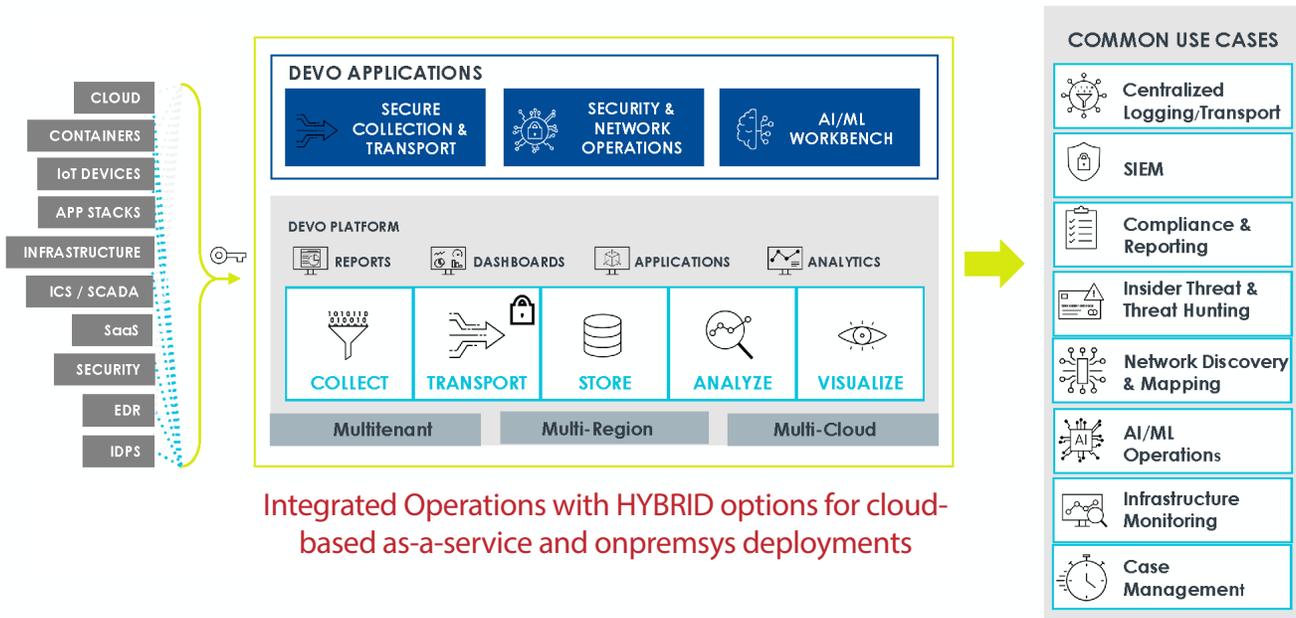
### Transform the Way You Monitor IT Operations

- Devo brings logs, metrics and trace data together, providing the visibility and analytics to troubleshoot and resolve end-to-end problems

### Key Discriminators

- CloudOne deployed with ATO for NIPR and SIPR. Operational monitoring at AFCERT and eSOC.
- 20-50 times faster than existing machine data solutions.
- Linearly Scalable architecture requiring fewer compute resources.
- 90% savings compared to competitors- Devo reduces the overall EC2 storage footprint.

## Devo is The Platform for Data Collection, Transport, Analytics and Integrated Operations



Integrated Operations with HYBRID options for cloud-based as-a-service and onpremsys deployments

“Devo has been a fantastic partner in transforming the way our SOC analyzes and acts on data. Not only is their technology superior to the incumbent, the solution is approachable, affordable, scalable and has an unprecedented time-to-value.”

### Devo Customer Success Selects

#### U.S. Air Force

- Devo is the U.S. Air Force’s Global SIEM for bases worldwide
- Beat out Splunk, Elastic, Exabeam, ArcSight
- Reduced repetitive analyst tasks by 20,000 hours annually, freeing them to focus on more important tasks

#### Accenture Federal Services (AFS)

- AFS uses the Devo Platform to collect all log traffic, correlate and set up alerts to monitor and looking for any suspicious behavior for their core set of network devices and key systems. Acting as a MSSP, AFS’ EITaaS program provides a multi-tenant managed SIEM service to DoD
- Evaluated the big choices that most other companies use. 400 days of hot data and the user experience are key differentiators
- Formatted dashboards the way they need it and when they meet with internal audit, we show them the dashboard and they have all the information that they need

t 210.296.4576 | [vholtmann@thundercattech.com](mailto:vholtmann@thundercattech.com)