

# Cribl Edge vs Vendor-Specific Forwarder

## A vendor-neutral approach to data collection


Today’s IT and security teams need more than legacy agents built for a single platform. Tools like Splunk Universal Forwarders (UFs) were built for a different era—one with simpler environments and fewer demands. Today, they struggle with manual configurations, slow upgrades, poor adaptability to cloud-native environments, and tight vendor lock-in—slowing down modern teams that need agility and scale.

Cribl Edge is a modern, vendor-neutral agent purpose-built for today’s hybrid and cloud-native environments. It delivers control, efficiency, and flexibility while future-proofing your entire data collection strategy.






### At-a-Glance Comparison

	 Cribl Edge™	VENDOR - SPECIFIC FORWARDER
Vendor-Agnostic	Route directly to the destination(s) of your choice using out-of-the-box integrations	Limited to vendor platform only
Deployment Flexibility	Purpose built for Linux, Windows, MacOS (coming soon) and Kubernetes environments	Best suited for Linux & Windows; general support for additional OSs; Kubernetes requires heavy forwarder or custom workarounds
Configurations	Built-in centralized, version-controlled, visual configuration authoring with fleets	Configurations are slow and manual, and requires separate infrastructure for management
Advanced Data Processing	Full Cribl pipeline support for edge processing	Primary purpose is for forwarding; only can perform basic transformations
Upgrades	Centralized, push-button with target versioning, and don't require restart of endpoint	Manual upgrades; large-scale requires additional tooling
Troubleshooting & Investigation	Comprehensive health monitoring dashboard; teleport into nodes for investigation	Lack of detailed telemetry or UI-based tool to explore individual nodes
Monitoring Tools	Automatically discover and collect host & process metrics, logs, and system state data; dive into specific nodes to debug; full observability monitoring console	No autodiscovery; minimal health metrics; minimal built-in visualizations for observability

# Functionality Matrix

		VENDOR - SPECIFIC FORWARDER
DEPLOYMENT		
Footprint	Lightweight, always less than 1 CPU	Lightweight
Installation Method	Multiple easy install options: a one line install script, UI, API, bake into image, MSI on windows, package installs	Package-based (MSI, RPM, DEB, tarball); CLI-based setup
Protocol Support	Syslog, OTLP, HTTP, TCP/UDP, REST, custom APIs	TCP/UDP, limited Syslog, no native OTLP
Persistent Queue	✔ Yes	✔ Yes
INTEGRATIONS		
Sources	Windows, Linux, Kubernetes, Syslog, OTel, REST APIs, and <a href="#">60+ integrations</a>	Windows, Linux, limited Syslog
Destinations	<a href="#">Any system</a> (including any SIEM, storage, Cribl Stream, etc.)	Vendor indexers only
MANAGEMENT		
Upgrades	Native support for remote and local upgrades	Manual local upgrades, and remote upgrades require additional tooling
Mass Configurations	UI-based changes at fleet and subfleets level to layer configurations by node groupings of your choice (business unit, custom tags, etc)	Can only group by server classes, unable to group by custom metadata
Version Control	✔ Yes, native configuration version control via Git	✘ No native configuration version control
Change validation	Rich visual interface for real-time change validation	Lack built-in change validation mechanisms, requires extra tooling
Permissions	Enterprise grade authentication support (LDAP, SSO, etc); native Workspaces for multi-tenancy; RBAC at the Workspace, Product, and Group/ Fleet level for fine-grained permissioning	Limited authorization at object/data level provided via Deployment Server; No native multi-tenancy support
DATA PROCESSING		
Native Processing Capabilities	✔ Yes, native configuration version control via Git	✘ No native configuration version control
Mass Configurations	UI-based changes at fleet and subfleets level to layer configurations by node groupings of your choice (business unit, custom tags, etc)	Can only group by server classes, unable to group by custom metadata

## Functionality Matrix (continued)

		VENDOR - SPECIFIC FORWARDER
MONITORING		
Environment Health Dashboards	 Yes, comprehensive dashboard with visualizations of many key metrics and Edge node data activity tracking	 Minimal built-in dashboards
Node Exploration	Teleport into specific nodes to debug and explore system performance metrics, running processes, containers, open files, and more	Only basic logs on host
Search	 Yes, comprehensive dashboard with visualizations of many key metrics and Edge node data activity tracking	 No, requires forwarding to centralized instance

## Why Cribl Edge?



### Eliminate vendor lock-in

Break free from rigid proprietary tools with a flexible vendor-neutral agent that strengthens your negotiation power, future-proofs your data collection strategy, and supports migration from inflexible software.



### Reduce costs with a data tiering strategy

Route data directly to your SIEM, Cribl Stream for heavier processing, data lakes, or storage to lower license costs while simplifying your architecture.



### Simplify operations to increase efficiency

Enjoy a unified data collection system with modern UI-based agents that support centralized, version-controlled, and remote upgrades and configurations.

## Ready to live life on the Edge?

### Try Cribl Edge today

Spin up a full-featured sandbox with pre-configured sources and destinations.

### Get guidance on migrating agents

Read the [How-to Guide](#) on migrating agents and how to deploy Cribl Edge.

### Accelerate your Universal Forwarder migration

Leverage Cribl's [Professional Service offering](#) to quickly transition from Splunk UFs to Cribl Edge.

### ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including [Cribl Stream](#), the industry's leading observability pipeline, [Cribl Edge](#), an intelligent vendor-neutral agent, [Cribl Search](#), the industry's first search-in-place solution, and [Cribl Lake](#), a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: [www.cribl.io](http://www.cribl.io) | Try now: [Cribl sandboxes](#) | Join us: [Slack community](#) | Follow us: [LinkedIn](#) and [Twitter](#)

©2025 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries. All third-party trademarks are the property of their respective owners. OPG-0017-EN-1-0425

## Legacy forwarders can't keep up

Traditional agents, including Universal Forwarders, were designed for a different era. Modern, distributed environments require flexibility and comprehensive visibility. Whether you're looking to reduce SIEM spend, migrate away entirely, or modernize how you collect telemetry data, **Cribl Edge gives you complete control over your telemetry collection strategy.**