



OWL Cyber
Defense™

HEAD-TO-HEAD COMPARISON

Owl Talon® vs. Waterfall WF-500/600

Hardware-Enforced Trust for Critical Infrastructure in the AI Era:
Why Protocol Filtering Outperforms Replication-Based Security

Hardware–Enforced Trust for Critical Infrastructure:

Why modern OT/IT environments require deterministic security that software controls alone cannot deliver.

In an era where critical infrastructure and industrial control systems face unprecedented cyber threats, operators of utilities, oil & gas, nuclear facilities, and other essential services require more than network isolation—they need verifiable trust and uninterrupted operational continuity. Moreover, as AI-driven hacking capabilities evolve, traditional, mutable software-based cybersecurity solutions grow increasingly vulnerable to exploitation and manipulation.

As cornerstones in Zero Trust architectures, hardware-enforced data diodes ensure every OT-IT data transfer is explicitly controlled, monitored, and secured—delivering deterministic protection beyond the reach of software-based solutions.

Both Owl Talon Protocol Filtering Diodes (PFDs) and Waterfall WF-500/600 Unidirectional Security Gateways align with industry best practices and compliance frameworks. However, only Owl Talon delivers FPGA-based protocol filtering at the

hardware trust boundary combined with the operational flexibility and scalability that modern critical infrastructure demands. Owl Talon’s extensible platform further differentiates its approach by enabling customers and global technology alliance partners to rapidly develop and deploy new capabilities at the speed of business, rather than waiting for traditional release cycles—all while maintaining expected and trusted end-to-end security. This agility allows organizations to adapt quickly to evolving operational and cybersecurity requirements without compromising performance or protection.

Waterfall’s unidirectional security gateways are widely used for secure replication of OT historians, SCADA systems, and other industrial data sources into IT networks, while Owl Talon focuses on a protocol-filtering data diode platform designed to support diverse OT and IT data flows with greater flexibility and innovation velocity.



BOTTOM LINE

Owl Talon provides the only unified diode platform capable of scaling from edge deployments to 100 Gbps enterprise throughput—delivering hardware–enforced protocol filtering, verifiable trust, and operational agility without sacrificing performance or security posture.



#1

Architecture and Security

Critical infrastructure operators cannot afford hidden software risks at OT/IT boundaries. Architecture determines whether a compromise in IT can pivot into control networks. Hardware-enforced protocol filtering at the diode line shrinks the attack surface, reduces misconfiguration risk, and simplifies audits. By contrast, software-heavy replication models add components to patch, monitor, and validate. For utilities, nuclear, and other essential services, a simpler, hardware-anchored architecture means fewer failure points, clearer compliance stories, and higher confidence that only expected, well-formed data ever reaches protected systems.

BOTTOM LINE

Owl Talon PFD minimizes software dependencies at the trust boundary with FPGA-hardened protocol filtering, delivering hardware-enforced trust for demanding critical infrastructure and classified use cases.

CAPABILITY	OWL TALON PFD	WATERFALL WF-500/ 600 GATEWAY
Enforcement	FPGA-based hardware protocol break enforcing deterministic, rule-based, one-way transfer with no return path.	Hardware one-way optical link paired with software-based replication modules on both sides of the diode.
Protocol Filtering	Hardware-level filtering at Layers 1–4; blocks malformed, unexpected, or malicious protocol elements in FPGA logic before they exit OT.	No hardware protocol filtering; relies on software replication agents and connector modules for supported protocols.
Security Model	Hardware-enforced isolation + FPGA logic eliminate software dependencies at boundary.	Waterfall’s architecture combines a hardware one-way link with software engines and connectors that replicate servers and devices, resulting in multiple software components that must be deployed and configured alongside the hardware.
Tamper Detection	Secure boot, TPM binding, encrypted drives, BIOS passwords, AIDE integrity monitoring, hardware alerts.	Public Waterfall documentation for WF-series gateways focuses on rack-mount industrial hardware, software logging, and certifications, but provides limited detail about specific internal hardware tamper-detection mechanisms.
Compliance	Meets U.S. Raise-the-Bar (RtB) expectations for Protocol Filtering Diodes; Common Criteria EAL4+, 9001, NERC-CIP, and defense-grade certifications.	Waterfall’s WF-600 holds Common Criteria EAL4+ certification (EAL4+, ALC_DVS.2, ALC_FLR.2, AVA_VAN.5), issued May 2025 by TrustCB B.V. under the Netherlands NSCIB scheme and recognized under CCRA Waterfall promotes gateways as helping operators comply with NERC CIP and ISA/IEC 62443; this does not equate to formal product certification across those frameworks. There is no public evidence that WF-500/600 are NCDSMO Baseline-listed or Raise-the-Bar approved as DoD/IC cross-domain solutions.
Internal Processing	FPGA-only for enforcement; minimal software in trust boundary.	Replication servers and software connectors process protocol logic.



#2

Throughput, Performance, and Reliability

Utilities and critical infrastructure increasingly depend on real-time analytics, centralized monitoring, and growing sensor volumes. Throughput and reliability determine whether operators see the full picture or work from stale, partial data. A diode that can't keep up becomes a bottleneck, forcing tradeoffs between security and visibility. High, predictable bandwidth with built in failover keeps historians, SOC tools, and engineering teams continuously fed with trustworthy data. For grid, pipeline, and plant operators, that means faster incident detection, smoother operations, and less risk that maintenance windows or failures interrupt critical situational awareness.

BOTTOM LINE

Owl Talon offers built-in high availability with up to 100 Gbps throughput—enabling scale without external orchestration while maintaining real-time data assurance as mission requirements evolve.

CAPABILITY	OWL TALON PFD	WATERFALL WF-500/600 GATEWAY
Throughput	Up to 100 Gbps	Up to 10 Gbps
Reliability	Supports high availability by utilizing dual data diodes for seamless failover and uninterrupted, one-way secure data transfer, providing nonstop operation in mission-critical environments.	Supports high-availability via dual ('double') gateways. HA deployments commonly include redundant connector/server instances; specific 'mirrored server' requirements depend on the use case.
Deployment Options & Environmental Fit	Available as all-in-one 1x1U rack-mountable or DIN-Rail appliances, Owl Talon One reduces SWaP for space-constrained settings. Owl Talon Torrent is offered as all-in-one 1x1U or 2x1U rack-mountable appliances to support deployments requiring high-throughput and computational capabilities.	Provides DIN-rail and rack-mounted gateway appliances; exact chassis dimensions should be confirmed directly with Waterfall's official mechanical specifications.



#3

Security in Depth

Operators face overlapping regulatory, safety, and cyber requirements. Security in depth matters because no single control is perfect—and every added box in the rack is another thing to harden and maintain. When integrity checks, tamper detection and enforcement live inside one hardened platform, teams spend less time stitching together point solutions and more time securing operations. This reduces configuration errors, speeds assessments, and improves resilience under attack. For critical infrastructure operators, integrated security layers directly translate into lower operational risk and easier demonstration of due diligence to regulators.

BOTTOM LINE

Owl Talon provides a single appliance with multiple hardware-enforced security layers—no external dependencies means no additional failure points and reduced operational complexity.

CAPABILITY	OWL TALON PFD	WATERFALL WF-500/ 600 GATEWAY
Device Integrity	FPGA hardware at the heart of its architecture enforces device integrity, ensuring one-way, protocol-filtered data transfer entirely in hardware while leveraging secure boot, TPM cryptographic binding, disk encryption, AIDE integrity monitoring, SELinux enforcement, and BIOS password protection to detect and block tampering.	Gateways combine hardware-enforced one-way isolation with software-based replication agents and connectors, adding an additional software processing layer; public material focuses largely on the rugged rack-mount hardware platform rather than detailing internal tamper-detection mechanisms.
Data Path Assurance	Provides data path assurance via single appliance with hardware-enforced, one-way data transfer, advanced FPGA-based protocol filtering, and absolute network separation, minimizing data leakage risk and operational threats.	Data path assurance depends on replica servers, connectors, and replication logic.
Operational Resilience	Built on FPGA-based hardware enforcement, dual-card high-availability failover, protocol filtering for multiple simultaneous data flows, and ease of integration within COTS infrastructure, designed for continuous, tamper-resistant, mission-critical service even in adverse conditions.	Offers single and high-availability ('double') gateway options. Specific resilience behaviors or dependencies (e.g., server synchronization or external load balancers) should be validated with the vendor for the intended architecture.



#4

Protocol Support and Adaptability

OT environments rarely stand still—SCADA upgrades, new historians, cloud analytics, and vendor changes are constant. Protocol flexibility determines whether a security control enables modernization or blocks it. A platform that can add or adjust protocol support in software lets operators adopt new tools without ripping and replacing hardware or opening unsafe workarounds. This matters for utilities and industrial operators that must keep plants running while modernizing. Fast protocol updates reduce project risk, avoid stranded assets, and keep security aligned with evolving operational and regulatory demands.

BOTTOM LINE

Owl adapts quickly to new protocols and use cases through an extensible Talon platform, uniquely enabling trusted partners and resellers to customize capabilities with their own software—delivering new functionality at the speed of business without sacrificing end-to-end security or requiring forklift upgrades.

PROTOCOL TYPE	OWL TALON PFD	WATERFALL WF-500/ 600 GATEWAY
Transport	TCP, UDP (unicast, multicast, broadcast)	TCP, UDP
File Transfer	RFTS, SFTP, TCP-PA, HSTCP-PA, HTTPS	SFTP, FTP/FTPS
Industrial/OT	OPC (DA/A&E/UA), Modbus, AVEVA PI Transfer, IEC 104, VTScada, Syslog, DNP3	Publishes datasheets for OPC DA/UA, Modbus, GE iFIX, DNP3, ICCP, IEC 104, Syslog, SNMP, Remote Screen View, SMTP, and Omni Flow. For OPC A&E/HDA, AVEVA PI Transfer, and EDS.
Monitoring	Syslog, SNMP, Remote Screen View	Syslog, SNMP, Remote Screen View
Web, Time, Email	Remote Desktop, NTP, SMTP, HTTPS	Publishes an SMTP connector; NTP support is not confirmed in current public datasheets.



#5

Flexibility and Overall Value

Budgets are tight, teams are small, and assets must stay in the field for years. Flexibility and value determine lifecycle cost, not just purchase price. A solution that fits multiple use cases (edge, plant, enterprise), consolidates protocols, and centralizes management reduces hardware sprawl and training burden. Longer lifecycles and in-place upgrades avoid disruptive forklift projects and repeated certification efforts. For critical infrastructure decision makers, this means fewer devices to buy and maintain, smoother expansions, and a clearer business case: stronger security that actually lowers total cost over the life of the system.

BOTTOM LINE

Owl Talon delivers lower lifecycle costs, longer deployments, centralized control—paying for itself in operational efficiency and reduced replacement cycles.

CAPABILITY	OWL TALON PFD	WATERFALL WF-500/ 600 GATEWAY
Management	Modern, web-based interface enabling fast, simple setup and management for even complex multi-protocol data flows with centralized visibility across all deployments.	WF-series gateways provide a web-based interface for local configuration/monitoring; public sources do not describe comprehensive centralized multi-appliance management.
Cost/ Efficiency	COTS hardware and flexible software tiers coupled with the ability to handle multiple industrial and enterprise protocols simultaneously enable Owl to deliver SWaP and cost savings without sacrificing capability or speed; 5-7 year product lifecycle reduces upgrade cycles and lowers total cost of ownership.	Offers rack-mount and DIN-rail gateways. Public sources do not disclose licensing structures or typical hardware refresh cycles; confirm with Waterfall.
Strategic Value	With backwards compatibility, containerized third-party integration, rapid protocol updates, and reliable long-term operation, Owl Talon offers low lifecycle cost and strategic adaptability for evolving mission requirements. Additionally, Owl supports extensibility of Owl Talon capabilities via trusted resellers and customers' technology partners.	Ideal for OT organizations needing historian replication and strict one-way isolation; less adaptive and slower to evolve for dynamic deployments when compared to Owl Talon's agile, modular architecture and protocol update capabilities.



Conclusion

Across the operational metrics of performance, adaptability, compliance, and lifecycle economics, Owl Talon PFDs stand alone as the solution built for both today's critical infrastructure challenges and tomorrow's evolving threat landscape. With broader throughput range, deep FPGA-based protocol filtering at the trust boundary, integrated high availability, and more flexible deployment options than replication-centric alternatives, Owl Talon is purpose-built for Zero Trust architectures in high-consequence OT/IT environments. For utilities, oil & gas operations, nuclear facilities, water treatment plants, manufacturing operations, and other critical infrastructure operators, Owl Talon delivers.

Ready for uncompromised security, operational resilience, and long-term value?

Connect with Owl Cyber Defense to see how Owl Talon PFD protects your critical operations and future-proofs your infrastructure.



Scan the QR code
to contact us.





Market Context

The analyst estimates for the data-diode / unidirectional-gateway market vary. For example, Precedence Research reports ~\$551M (2024) → ~\$1.85B (2034) (~12.85% CAGR), while Fortune Business Insights projects ~\$1.75B by 2034 (~12.2% CAGR), with North America around ~32–39% depending on methodology. Driven by strong defense spending, early adoption of critical infrastructure protection standards, and stringent regulatory mandates including NERC CIP, NIST guidelines, and Raise The Bar compliance requirements.

Owl Cyber Defense maintains a leadership position in this fragmented, specialized market where security assurance and certifications create significant barriers to entry. Key competitive drivers include hardware-enforced trust, compliance with military-grade cybersecurity standards, protocol flexibility, and integration capabilities with modern SOC/SIEM platforms.

From a competitive-analysis perspective, the data-diode and unidirectional-gateway market can be viewed as including: (1) specialized hardware-only diodes; (2) enterprise gateway appliances that rely on replication architectures, such as those offered by Waterfall and others; and (3) platforms that emphasize FPGA-based protocol filtering. Owl's position in segment (3) directly addresses the evolving demand for adaptability, reduced SWaP, and rapid protocol updates—critical factors for modern zero-trust architectures and cross-domain operations in both government and critical infrastructure environments.



References

https://waterfall-security.com/wp-content/uploads/WF-500_Datasheet.pdf

<https://waterfall-security.com/technology-and-products/wf-600/>

<https://www.scribd.com/document/648790832/WF-500-Datasheet>

<https://industrialcyber.co/news/waterfalls-wf-600-unidirectional-security-gateway-brings-unbreachable-protection-to-ot-ics-networks/>

<https://www.helpnetsecurity.com/2023/03/20/waterfall-security-solutions-wf-600/>

<https://waterfall-security.com/wp-content/uploads/Waterfall-for-GE-iFIX.pdf>

<https://www.commoncriteriaportal.org/nfs/ccpfiles/files/epfiles/NSCIB-CC-2400089-01.1-CR.pdf>

<https://waterfall-security.com/wp-content/uploads/2023/09/WF-600-Brochure.pdf>

<https://waterfall-security.com/wp-content/uploads/2023/08/Waterfall-for-DNP3-New.pdf>

<https://waterfall-security.com/wp-content/uploads/2023/03/Waterfall-for-IEC-60870-5-104.pdf>

<https://waterfall-security.com/technology-and-products/>

<https://www.prnewswire.com/news-releases/waterfall-unidirectional-security-gateways-earn-common-criteria-eal4-certification-1644-301735975.html>

General market taxonomy references for unidirectional gateways/data diodes:

<https://www.cognitivemarketresearch.com/unidirectional-gateways-market-report>

<https://dataintel.com/report/unidirectional-gateway-market>



Owl Cyber Defense Solutions, LLC, headquartered in Columbia, MD, leads the industry in data diode and cross-domain network cybersecurity solutions for faster, safer and smarter decision making. We create solutions tailored for high-risk sectors including the military, government and critical infrastructure. Our advanced technologies enable secure, near-instantaneous collaboration, bridging network barriers to protect critical missions. With a focus on scalability and interoperability, Owl ensures that organizations can maintain secure, reliable, and compliant communication channels against evolving cyber threats.

For more information on Owl, or to schedule a demo, visit www.owlcyberdefense.com.

