

The File System Is the **Vulnerability**.

AsterionDB Removes It.

ACTIVE THREAT

VOLT TYPHOON

PRC State-Sponsored
APT
Inside US Networks
Since 2021

THE THREAT

Volt Typhoon — a PRC state-sponsored APT — has been **embedded inside US energy, water, and communications networks since 2021**. It does not use exotic malware. It uses native OS tools to enumerate file systems, move laterally, and position for future disruption — confirmed by FBI, CISA, and Dragos.

THE GAP

Every conventional security tool — EDR, SIEM, network monitoring — is built on top of the file system. These tools monitor activity inside it, **but monitoring activity inside the file system does not remove the file system as a traversal pathway**. The adversary moves through it regardless. **Eliminate the file system and you eliminate the path.**

HOW THE ATTACK WORKS

Volt Typhoon's Kill Chain

01	Edge Device Compromise Exploits unpatched VPN or router CVEs to gain initial network foothold via Living-Off-the-Land (LOTL) tools — no malware required.	EXPOSED
02	File System Enumeration Discovers document stores, SCADA configs, credentials, and network maps using native OS commands invisible to EDR and endpoint tools. NoFS: no discoverable paths exist.	✓ BLOCKED
03	Lateral Movement Traverses IT toward OT using discovered paths and stolen credentials. NoFS: no discoverable paths exist. Movement stops here.	✓ BLOCKED
04	IT/OT Boundary Crossing Seeks SCADA configs and operational documents to pivot into the control loop. No file-system assets exist to find or exploit.	✓ BLOCKED
05	Pre-Conflict Persistence Embeds dormant capability for future activation. Oracle-native audit surfaces anomalous sessions in real time — no dark corners.	✓ BLOCKED

THE ASTERIONDB SOLUTION

Structural Defense — Not Another Layer

No-File-System (NoFS) Architecture

All data and documents move out of the file system into the Oracle database. No file paths exist. Volt Typhoon's enumeration finds nothing — reconnaissance fails before lateral movement begins.

Zero Trust at the Data Layer

Assets are invisible until database-enforced credentials are verified. There is no file you can see before you have permission. Pre-access reconnaissance is architecturally impossible.

Oracle-Native Audit & Access Control

Every session and data movement is logged in Oracle's audit infrastructure. LOTL behavioral anomalies surface in real time — meeting NERC CIP, NRC, and TSA mandates natively.

Uniform Cloud · On-Premises · Edge Deployment

- ☐ The IT/OT boundary is enforced at the database layer, not the network perimeter. OT sensor data and operational documents are governed identically. The control loop is no longer reachable via file paths.

Electric Utilities

NERC CIP-003-9 · CIP-015-1

File-based lateral pathways between IT and OT substation networks structurally eliminated. Oracle audit satisfies CIP-015-1 without added tooling.

Nuclear Power

NRC 10 CFR 73.54

Millions of controlled documents moved out of file system. NRC "high assurance" standard met structurally. Real-time audit supports 1-hour incident reporting.

Oil & Gas Pipelines

TSA SD Pipeline-2021-016

SCADA configs protected from file-system enumeration. Compliance records in Oracle environment meet TSA Sensitive Security Information requirements.

Water & Wastewater

CIRCA 2026 · EPA

Ransomware finds no file system to encrypt. CIRCA 2-year evidence preservation met natively. HMI configuration data protected at the data layer.

Defense & Comms

CMMC 2.0 · IL4/5/6

CUI removed from file-system exposure. Oracle IL6 accreditation baseline. Salt Typhoon's file-based lateral movement path is eliminated.

5+

Years Volt Typhoon has persisted inside US critical infrastructure networks

0

Discoverable file paths in an AsterionDB NoFS deployment

5

Issued patents protecting the AsterionDB Converged Computing Architecture

IL6

Oracle accreditation baseline across cloud, on-premises, and edge

The adversary is already inside. The file system is how they move.

AsterionDB replaces the file system with a Zero Trust, Oracle-native converged platform — structurally defeating lateral movement before it begins. No file system. No discoverable paths. No attack surface.

LEARN MORE

<https://asteriondb.com>

CONTACT

sales@asteriondb.com