CERTES

Certes for Federal Agencies

Assume Breach. Protect the Data. Prove Control.

CHALLENGE

Federal Agencies Face Escalating Risk. Even Behind the Firewall.

Federal systems are under relentless attack — from foreign adversaries, insider threats, and zero-day exploits. Even with cloud-first strategies, endpoint controls, and zero trust architectures, attackers are logging in — not breaking in. And when that happens, it's the data that's most vulnerable. Without real-time protection of data in transit, traditional tools can't stop exfiltration, impersonation, or destruction.

SOLUTION

Certes Delivers Deterministic Data Protection. Built for Mission-Critical Environments

Certes DPRM (Data Protection & Risk Mitigation) protects what other tools can't see. Unlike perimeter firewalls, endpoint agents, or inline decryption, Certes wraps critical data flows, like Active Directory traffic, in quantum-safe encryption and enforces policy-based isolation between trusted systems. Even if the network is compromised, your data remains invisible, untouchable, and unusable.

Why Federal Agencies Choose Certes

Certes delivers crypto-agile, post-quantum-ready protection and policy-enforced segmentation for the most sensitive data in transit, including Active Directory replication, identity services, and government workloads across hybrid and tactical environments. With Certes:

- Active Directory becomes resilient to enumeration, ticket forging, and impersonation.
- Segmentations are cryptographically enforced: no trust in network boundaries.
- Even compromised endpoints can't see or interact with critical systems.
- Air-gapped workloads can replicate and recover securely via virtual isolation zones.

Certes Advantages for U.S. Federal Agencies

Post-Quantum Ready, Mission-Grade Protection

- PQC-ready encryption to protect classified and sensitive data beyond today's threat curve.
- Supports quantum-safe strategy mandates for long-term national security.

Active Directory, Secured by Design

- Protects AD traffic (Kerberos, LDAP, DNS) from exposure and tampering.
- Stops enumeration tools like Mimikatz or BloodHound at the network level.
- Ensures domain controllers only talk to pre-approved endpoints.

Zero Disruption, Full Control

- Certes operates as a transparent overlay: no endpoint agents, no inline devices.
- Exclusive, full control of encryption keys remains with the agency, not a third party, satisfying mandates for control and auditability.
- Works across cloud, Internet, MPLS, tactical radio, or 5G environments.

CryptoSegmentation for Zero-Trust Control

- Segments are enforced with cryptography, not VLANs or ACLs.
- Prevents lateral movement even if credentials or devices are compromised.
- Create secure enclaves for Active Directory, backup systems, cloud workloads, and more.

Virtual Airgaps Without Hardware

- Enforces virtual separation between workloads across any transport.
- Enables recovery traffic, replication, or failover without breaking isolation.
- Keeps backup traffic encrypted, policy-bound, and invisible to attackers.

Prove Control with Real-Time Assurance

- Certes Five Pillars (Policy, CryptoSegmentation, Scalability, Visibility, Observability) provide audit-ready compliance.
- Prove protection of critical flows without decrypting content.

Mission-Critical Use Cases

DoD & Intelligence

Enforce data segregation and mission assurance across secure and tactical networks.

Justice & Law Enforcement

Meet CJIS mandates for full encryption key ownership and auditable control.

Civilian Agencies

Protect inter-agency communications and backup data flows over SD-WAN.

Cloud & Zero Trust Initiatives

Ensure data integrity across hybrid, multi-cloud, and zero-trust architectures.

Cloud Deployments

Under the shared responsibility model, cloud providers secure infrastructure, not your data. Certes ensures agencies control their data and keys at all times, preventing exposure in cloud or hybrid environments.

Secure tomorrow's data today

Don't just modernize your network, protect the data flowing through it. Certes empowers federal agencies to reduce cyber risk, meet compliance, and ensure operational continuity – even in untrusted network environments.

www.certes.ai