YOUR LOGO HERE

MSP-Demo THREATDEFEND FOR GOVERNMENT

DEFENDING PUBLIC SERVICES. SAFEGUARDING CITIZEN DATA. ACHIEVING REGULATORY COMPLIANCE.

Top Cybersecurity Threats Facing Government Entities

1. Nation-state and ransomware attacks on critical infrastructure
2. Data breaches exposing sensitive citizen information
3. Phishing and social engineering targeting public employees
4. Insider threats and unauthorized access to systems
5. Compliance failures (e.g., CJIS, NIST, CMMC)

Pain Points

Government

- Limited cybersecurity budgets and legacy systems
- Growing pressure to meet complex regulatory frameworks
- Remote work and hybrid networks expanding the attack surface
- Inconsistent monitoring across departments and agencies

RELEVANT THREATDEFEND MODULES

Falcon Identity Protection
Stop privilege abuse and secure remote access

Falcon Discover
Gain visibility into devices, user activity, and rogue software

Falcon Exposure Management
Continuously identify and mitigate vulnerabilities

Falcon LogScale (Next-Gen SIEM)
Real-time event correlation and threat detection

24/7 SOC Monitoring
Rapid incident response to reduce risk

Why It Matters

Cyberattacks on government agencies can disrupt essential services and compromise national security. With increasing mandates around digital security and compliance, MSP-Demo ThreatDefend equips public sector entities to proactively defend against threats while meeting strict regulatory requirements.

Take Action

Schedule a Government Cyber Readiness Review with MSP-Demo to assess vulnerabilities, validate compliance, and strengthen your cybersecurity posture across agencies.

View Website pedro.fialho@vijilan.com +1 (954) 334-9988