

SPLUNK SECURITY SOLUTION · FEDERAL

One unified platform. Every mission.

CMA's proven Splunk Security solution unifies Department-wide compliance and component-level security operations on a single platform.

THE CHALLENGE

The customer need: oversight and autonomy at once

DEPARTMENT LEADERSHIP

Central oversight

Government-wide compliance reporting and one view of threats that cross component lines.



AGENCIES AND PROGRAMS

Mission autonomy

Their own detections, dashboards and investigations, tuned to the systems they run.

Most platforms force a choice. CMA's Splunk Security solution unifies both on one platform.

THE SOLUTION

A unified Splunk Security platform in four blocks

**Hardened platform**

Splunk Enterprise or Splunk Cloud Platform with Enterprise Security, security-hardened.

**Detection content**

Correlation searches and risk-based alerts mapped to NIST 800-53 and MITRE ATT&CK.

**Visibility**

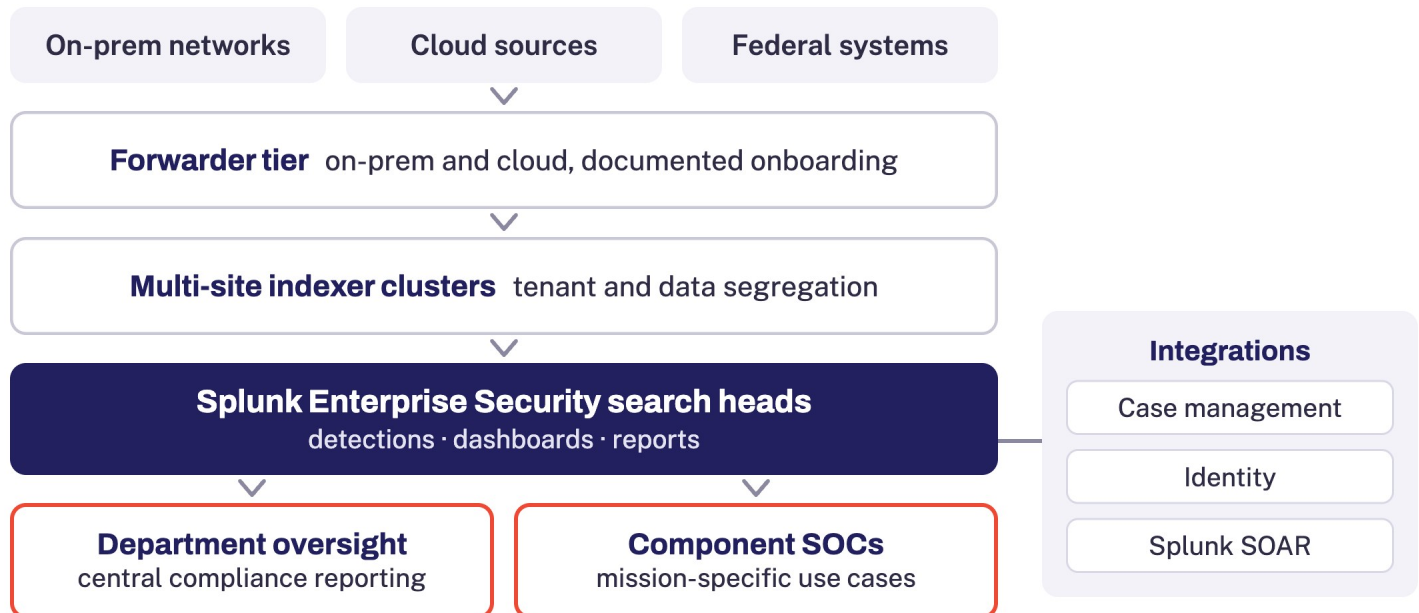
Pre-built threat monitoring dashboards and audit-ready compliance reports.

**Integrations**

Case management, identity, endpoint and network tools, plus optional Splunk SOAR.

HOW IT WORKS

One Splunk Security platform serves headquarters and components alike



PROVEN EXPERTISE

A cabinet-level federal department

10+ yrs running Splunk across the Department

2018 enterprise license agreement, shaped with CMA team members

2022 pattern packaged by CMA as a repeatable solution

Today it spans more components, data sets and use cases. The same pattern also runs at a federal transportation security agency.

CUSTOMER OUTCOMES

What agencies get

- ✓ **Compliance-ready reporting** from one central SIEM
- ✓ **Component autonomy** inside segregated tenants
- ✓ **Consistent detections** mapped to NIST and ATT&CK
- ✓ **Less alert noise**, faster investigation and response
- ✓ **Room to grow** without rebuilding

Talk to CMA, your Splunk Security advisor

Get a briefing on how a unified Splunk Security platform can meet your agency's mission.

www.cmai.com