

Falcon Flight Control: Managing Security at Scale



Drive a whole-of-state approach to cybersecurity with advanced multi-tenancy capabilities

To effectively safeguard their operations and constituents' information, states need a comprehensive approach to cybersecurity. As many consider taking a whole-of-state approach to enhance their cybersecurity posture across state government, local government and education, it certainly comes with its challenges and complexities. Sharing cybersecurity-related information, threat intelligence and best practices among agencies, counties and cities can enhance overall cybersecurity resilience. However, establishing trust and creating mechanisms for secure information sharing can be a challenge, especially when there is a lack of established relationships or concern about the sensitivity of certain information and how it's managed.

Challenges

Managing and coordinating cybersecurity incident detection and response can be challenging with a statewide attack surface composed of many organizations working in silos. Fragmentation of cybersecurity efforts across various agencies, counties and cities causes overlap and uncoordinated response. Information sharing, communication and reporting are difficult. Lack of awareness about the cybersecurity tools available to state organizations, competing priorities and policy requirements, and resource constraints complicate things even more.

Key Benefits

- Multi-level parent/child account control
- Holistic view of threats across all accounts
- Flexible policy management
- Powerful scalability, incident response and collaboration across state and local entities

Visibility with autonomy

The CrowdStrike Falcon® platform is a cutting-edge cybersecurity solution designed to empower organizations with comprehensive and proactive defense against modern threats. With its advanced multi-tenancy capabilities, the CrowdStrike Falcon® Flight Control feature enables a whole-of-state approach to cybersecurity, offering enhanced visibility, control and protection across diverse environments at the state level but still allowing local entities to maintain control of their own environment.

Multi-tenancy for enhanced efficiency

Falcon Flight Control provides a robust multi-tenancy architecture, allowing centralized management and control of cybersecurity operations across multiple entities, departments and agencies within a state. This streamlined approach can reduce complexity, lower operational costs and ensure consistent security policies and configurations by enabling teams to manage threats across the state in logically segmented separate instances within one CrowdStrike parent account. Instead of having to filter through events and data across all state organizations at once, each child account can manage its own policies and cannot see anyone else's data.


States can quickly add additional accounts in an organized way and keep county, city and departmental groups separate to meet their unique needs. This makes it much easier for managed security service providers (MSSPs) or state cybersecurity teams to organize and manage security at scale by allowing the vast IT environment to be logically segmented. This separation allows for many use cases, such as an MSSP supporting all of the separate agencies, counties and cities or a state that wishes to divide the administration of the Falcon platform by subsidiary or geography.

Unified visibility and threat intelligence

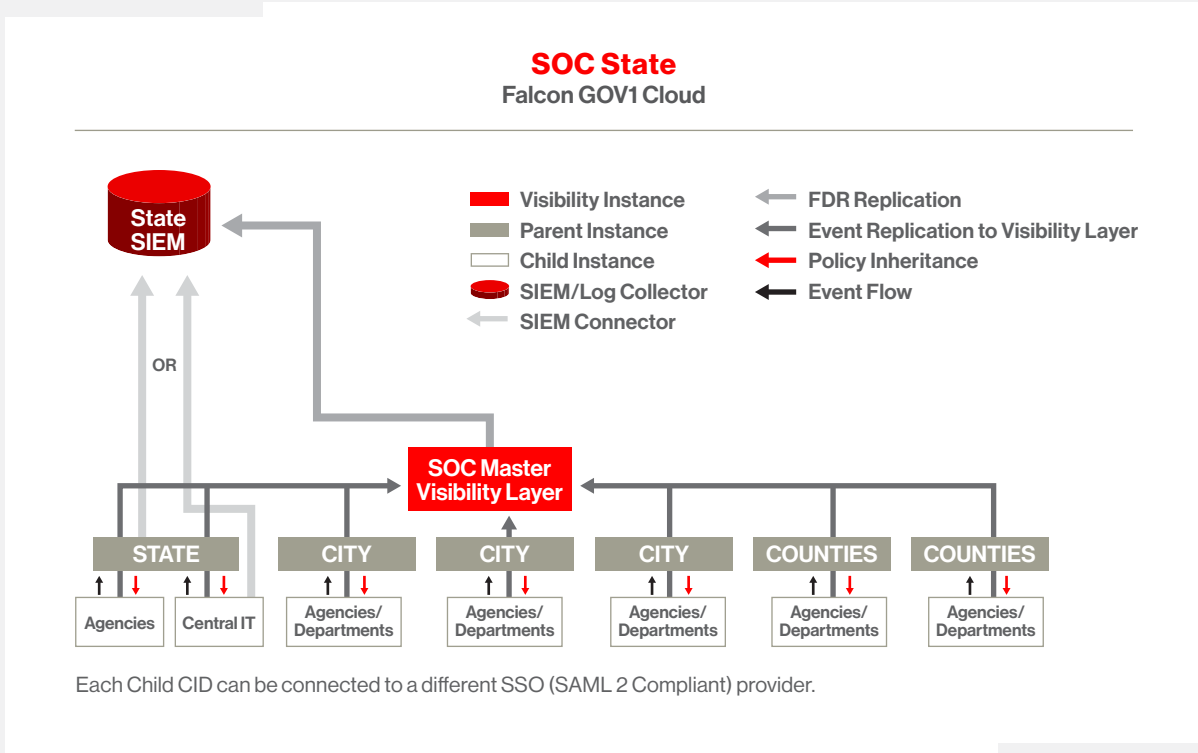
State-level security teams gain unified visibility into their statewide cybersecurity landscape. The Falcon platform aggregates and analyzes data from diverse sources, delivering comprehensive threat intelligence, real-time alerts and proactive threat hunting capabilities. This holistic view enables swift response to emerging threats and facilitates strategic decision-making.

Granular access controls and policy management

Falcon Flight Control offers granular access controls and policy management features, enabling administrators at the county, city or agency level to define and enforce their own security policies and use policies pushed from the parent state account. Administrators can easily assign role-based access privileges to authorized users, helping to ensure data privacy, segregation and regulatory compliance within a multi-tenancy environment.



82%
of U.S. state
governments
use
CrowdStrike

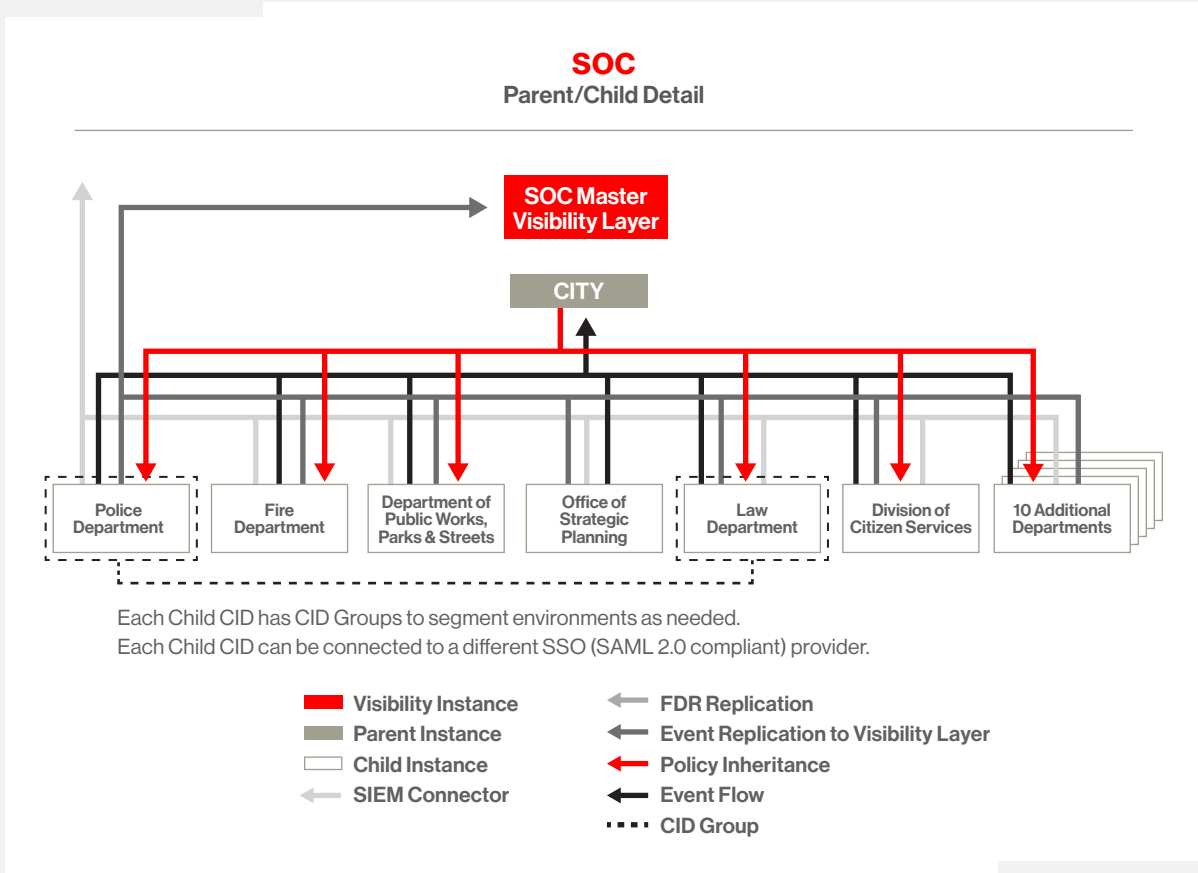


Scalability and flexibility

The highly scalable architecture of Falcon Flight Control accommodates the needs of states with diverse infrastructures and varying levels of security requirements. Whether states are managing a handful of entities or a large-scale network, Falcon Flight Control adapts to the unique demands of each environment, providing valuable flexibility and future-proofing.

Incident response and forensics

In the event of a security incident, Falcon Flight Control equips state-level cybersecurity teams with powerful incident response and forensic capabilities across all entities using the Falcon platform. This enables swift containment, investigation and remediation of threats, minimizing the impact and facilitating a rapid return to normalcy.



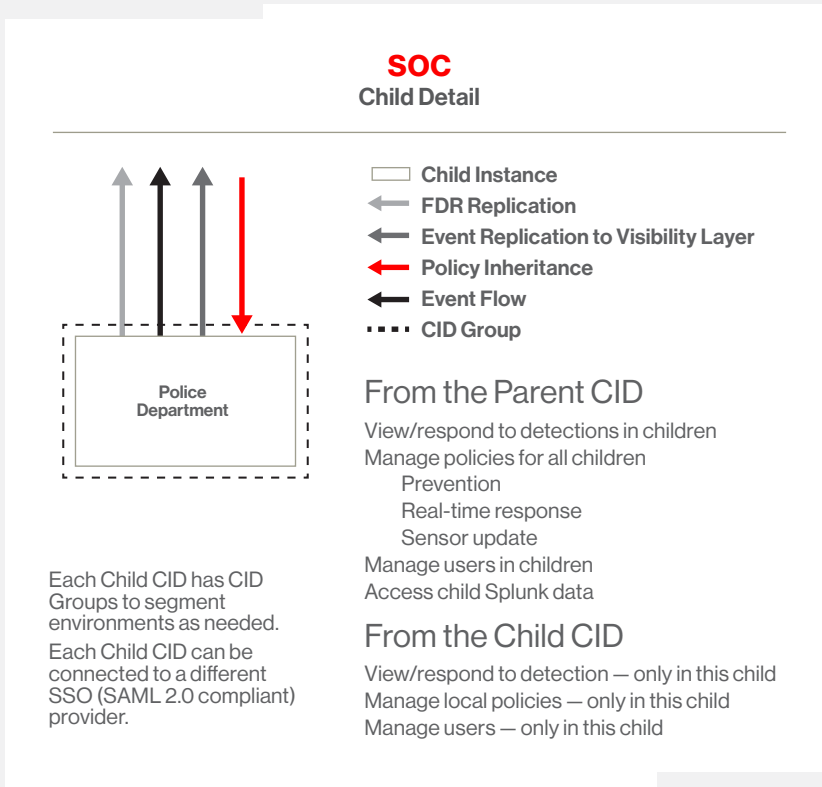
Collaborative threat intelligence sharing

Falcon Flight Control encourages collaboration and information sharing among different entities within a state. By securely exchanging threat intelligence and indicators of compromise (IOCs), organizations can leverage collective knowledge to enhance their overall security posture and proactively defend against sophisticated adversaries.

Integration and orchestration

The Falcon platform seamlessly integrates with existing security infrastructure, enabling state entities to leverage their current investments while enhancing their overall capabilities. The platform also supports orchestration of security workflows, automating repetitive tasks and ensuring consistent responses across the multi-tenancy environment.

CrowdStrike empowers states that choose the Falcon endpoint protection platform with a whole-of-state cybersecurity approach, enhancing the way security teams defend against modern threats. With its advanced multi-tenancy capabilities, the CrowdStrike Falcon solution offers unified visibility, granular access controls and collaborative threat intelligence sharing, enabling states to better stay ahead of adversaries and protect critical assets. Embrace CrowdStrike to help safeguard your state's digital ecosystem and secure a resilient future.



Follow us:

- [Blog ›](#)
- [Twitter ›](#)
- [LinkedIn ›](#)
- [Facebook ›](#)
- [Instagram ›](#)

[Learn about CrowdStrike Falcon® Insight XDR and how CrowdStrike can help you implement a whole-of-state approach.](#)

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.



[Learn more](#)

[Start a free trial today](#)