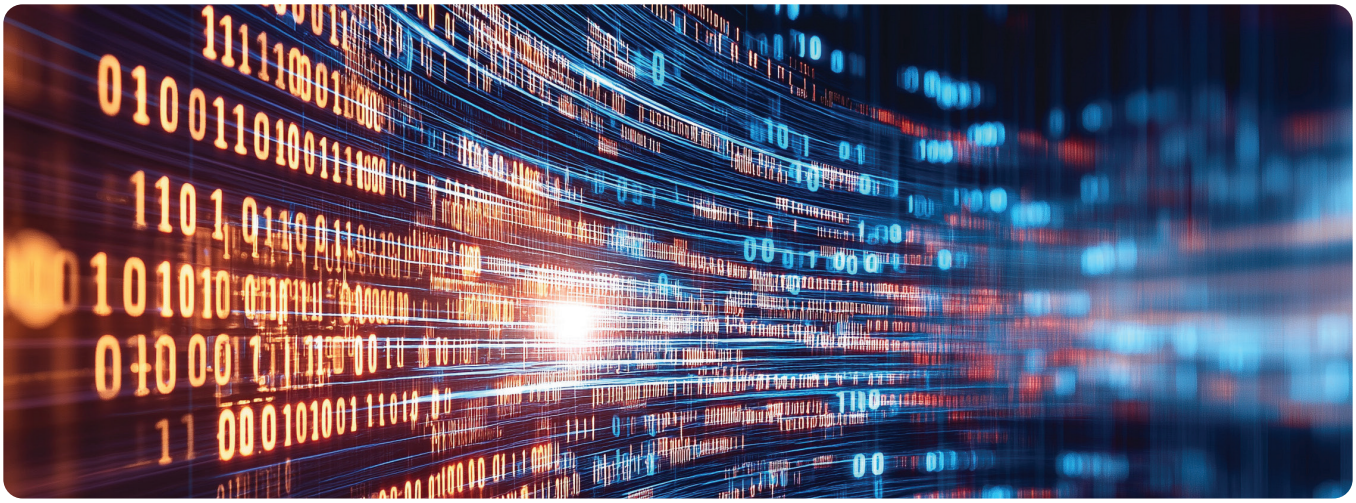
CLOUDERA

WHITEPAPER

Cloudera Maximizes SIEM Platforms

The value of strategic augmentation over replacement for government cybersecurity.



When threats accelerate, every second counts

The cybersecurity landscape for government agencies continues to escalate in complexity and scale. Recent data revealed a surge in threat activity: Domain name system (DNS) flood attacks have increased 553% from 2020 to 2023. With 59% of all ransomware attacks targeting the United States and 90% of organizations citing talent shortages as a critical vulnerability, most agencies find themselves fighting sophisticated threats with constrained resources.

A well-functioning security information and event management (SIEM) system is the central nervous system for defensive cyber operations. It provides real-time visibility, automated threat detection, and rapid incident response capabilities. For government agencies, SIEM performance directly impacts mission success. Faster and more accurate threat detection means protecting sensitive data, maintaining operational continuity, and meeting stringent compliance requirements. A well-functioning SIEM system frees analysts from manual log review to focus on strategic and proactive threat hunting.

The replacement reality check

A complete SIEM overhaul is often unrealistic in public sector environments. Budget constraints, government procurement cycles, personnel shortages worsened by recent changes, and multi-year implementation timelines with long transition periods can make wholesale SIEM replacement risky or unfeasible. Existing SIEM investments offer tremendous value. The challenge is that current SIEM playbooks contain years of institutional knowledge and tailored security expertise that agencies can't afford to discard.

Key takeaways

The challenge: Evolving threats and exploding data volumes are straining SIEM systems and the security teams managing them. Complete SIEM replacement isn't realistic for most agencies. Budget constraints, procurement cycles, and transition risks make it unfeasible. Your existing systems contain years of institutional knowledge and tailored security expertise that can't be discarded.

The solution: Strategic augmentation enhances your current SIEM infrastructure through intelligent data processing layers that filter, enrich, and route information. This approach preserves existing investments and institutional knowledge while adding streaming analytics, AI-driven threat detection, and automated processing capabilities.

The impact: Augmentation delivers measurable improvements without operational disruption: 90% faster threat detection, 60% reduction in storage costs, and 55% improvement in search performance. Security teams gain the capabilities they need to match today's threats while maintaining the playbooks and expertise they've spent years developing.

So how can agencies dramatically improve their defensive cybersecurity while working within these practical constraints? The answer lies in strategic augmentation rather than wholesale replacement of existing systems.

When growth outpaces capability

Many agencies are experiencing an unprecedented explosion of data volumes that their current SIEM infrastructures struggle to manage effectively. The number of data sources available also keeps increasing as agencies contend with the proliferation of Internet of Things (IoT) devices and the complexities of cloud migrations and hybrid environments. Regulatory requirements with long retention periods compound storage challenges, and as your agency grows, new threat vectors mean even more monitoring across increasingly complex attack surfaces.

Signs your SIEM needs augmentation

Security teams across government agencies can recognize the familiar indicators of a SIEM solution under stress. If your system shows any of the following, strategic augmentation may be warranted:

- Query response times are increasingly delayed.
- Analysts are overwhelmed by alert fatigue due to excessive false positives.
- Storage costs routinely exceed budget allocations.
- Time to detection is too slow to mitigate active threats.

The technical debt problem

These performance issues reflect deeper structural challenges accumulated over years of incremental system additions. Proprietary data formats lead to vendor lock-in that limits flexibility and increases costs. Siloed data prevents the comprehensive threat analysis needed to detect advanced, persistent threats that span multiple systems over time. Infrastructure constraints, meanwhile, limit real-time processing and force teams to rely on batch processing, which can introduce dangerous delays. Manual processes consume valuable analyst time on routine tasks that should be automated, preventing teams from focusing on high-value strategic activities.

Mounting operational burdens have created a cycle of delays and inefficiencies. As threats become more sophisticated, detection tools have struggled to keep up, requiring additional resources that agencies can't spare.

The augmentation approach: Maximizing existing investments

Strategic augmentation enhances existing SIEM infrastructure through intelligent data processing layers that filter, enrich, and route information. Augmenting your existing SIEM can bolster your cybersecurity position without adding to the ongoing resource drain. It can also help agencies preserve existing investments and institutional knowledge.

For agencies, augmentation can outperform replacement

Your SIEM solution is already fine-tuned to your agency's needs. Existing playbooks, custom detection rules, and analyst familiarity with current systems represent years of refined security expertise tailored to specific agency environments and threat landscapes. This accumulated knowledge is a strategic asset.

Beyond financial considerations, augmentation addresses the operational risks inherent in system replacement. Unlike replacement projects that can create security gaps during months-long transitions, agencies can deploy augmentation gradually alongside their existing systems. New capabilities are validated in controlled environments before expanding scope, ensuring continuous protection of critical security functions while systematically improving performance.

Most importantly for resource-constrained agencies, budget optimization extends the return on investment for existing systems while adding new capabilities. Rather than writing off functional infrastructure, augmentation leverages current investments as the foundation for enhanced performance. Your existing SIEM likely already works with the legacy systems your agency uses. Augmentation works with existing infrastructure and avoids the integration challenges that new SIEM deployments often encounter with established government IT environments.

Using Cloudera Flow Management to improve SIEM performance

The foundation of effective SIEM augmentation lies in implementing an intelligent data processing layer between sources and the existing SIEM infrastructure. Cloudera Flow Management operates on three core principles that address the fundamental challenges agencies face:

- Data preprocessing filters and enriches information before expensive SIEM ingestion, removing extraneous fields while adding relevant context that improves detection accuracy.
- Smart routing directs data to the appropriate destinations based on value and urgency, ensuring critical alerts immediately reach security teams while routine information flows to cost-effective storage.
- Cost optimization reduces SIEM storage expenses while improving overall data quality, enabling agencies to maintain comprehensive monitoring without exceeding budget constraints.

Cloudera Data Flow integrates easily with existing SIEM platforms using standard APIs, enabling data processing enhancements that reduce response lag and improve overall system performance. By filtering and enriching data before it reaches your existing systems, Cloudera Data Flow ensures that agencies can meet stringent performance requirements and compliance mandates without overwhelming current infrastructure.

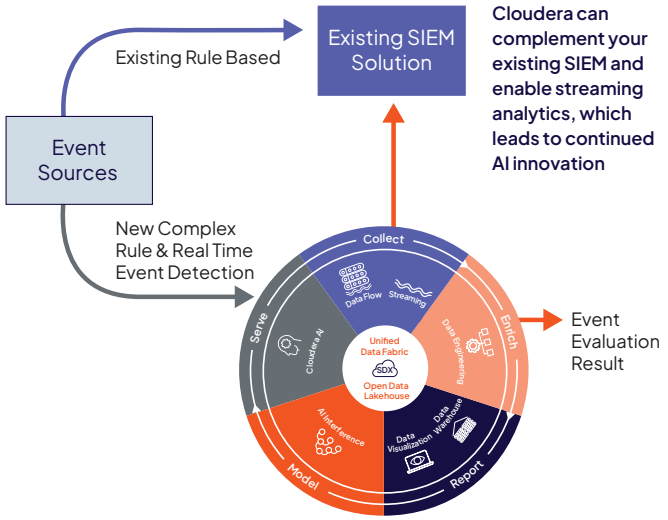
Ease of implementation

Modern augmentation solutions can drastically reduce time to deployment with drag-and-drop pipeline creation that requires minimal specialized expertise. Standards-based architecture prevents proprietary lock-in while supporting hybrid cloud deployment across the complex environments that characterize government IT infrastructure. Operational simplicity ensures minimal maintenance overhead for resource-constrained teams, allowing security staff to focus on analysis rather than system administration.

Technical implementation: Turning raw logs into actionable security insights

Data ingestion and processing architecture

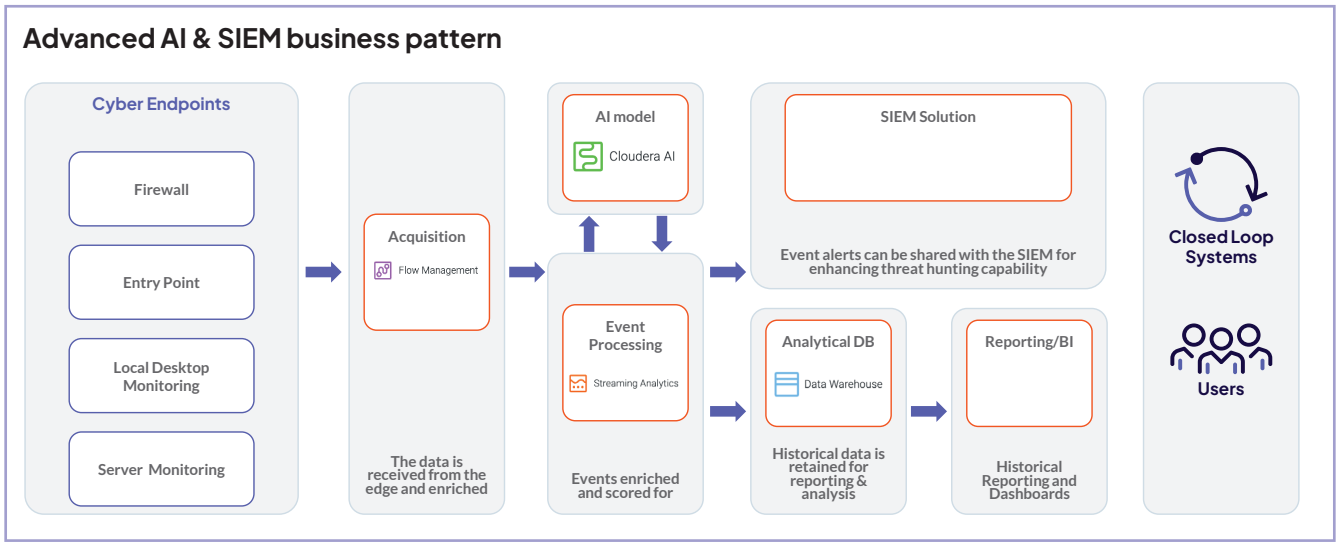
Open platform SIEM optimization solution using Cloudera Better Together



Current SIEM architectures struggle because raw data flows directly from sources to storage and processing systems, overwhelming both storage capacity and analytical capabilities. An optimized approach positions Cloudera Data Flow as an intelligent intermediary that intercepts, processes, and routes data based on strategic value rather than simple volume.

The transformation begins with real-time filtering based on configurable criteria such as severity levels, event codes, and threat indicators. Field reduction eliminates unnecessary data points that consume storage without providing analytical value. At the same time, log aggregation combines similar events to reduce volume while preserving the analytical context necessary for pattern recognition and threat detection.

AI-enhanced event processing

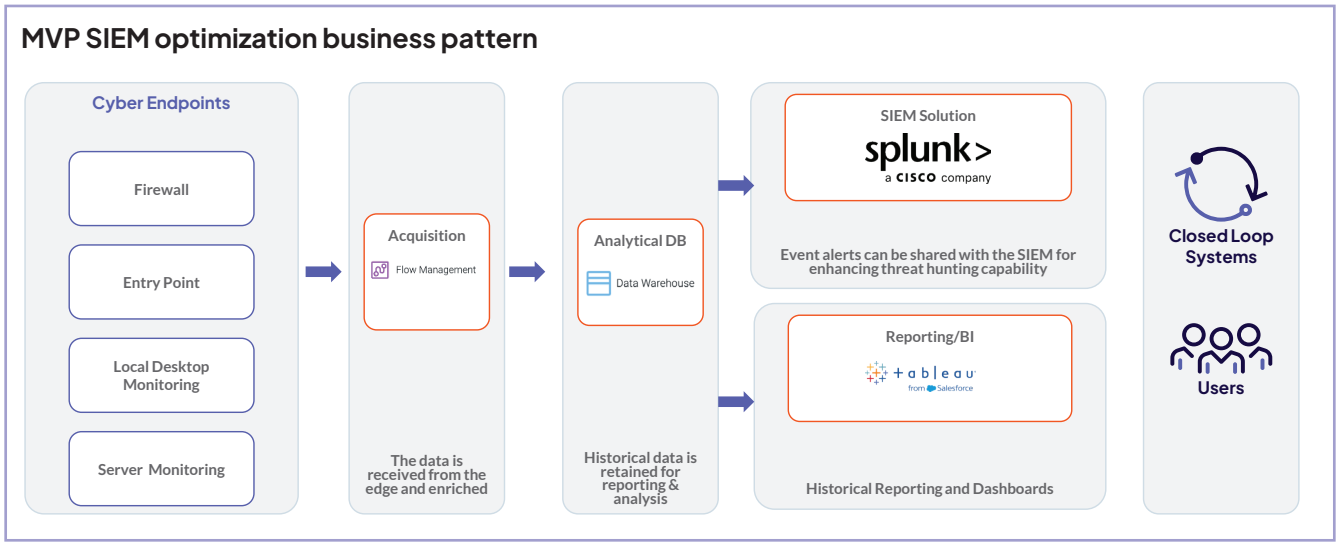


Streaming analytics capabilities enable real-time threat scoring and anomaly detection that identify potential security incidents as they occur rather than during post-incident analysis. Machine learning integration provides pattern recognition for advanced threat detection that evolves with changing attack methodologies. Meanwhile, closed-loop feedback systems ensure that AI insights continuously improve filtering and routing decisions.

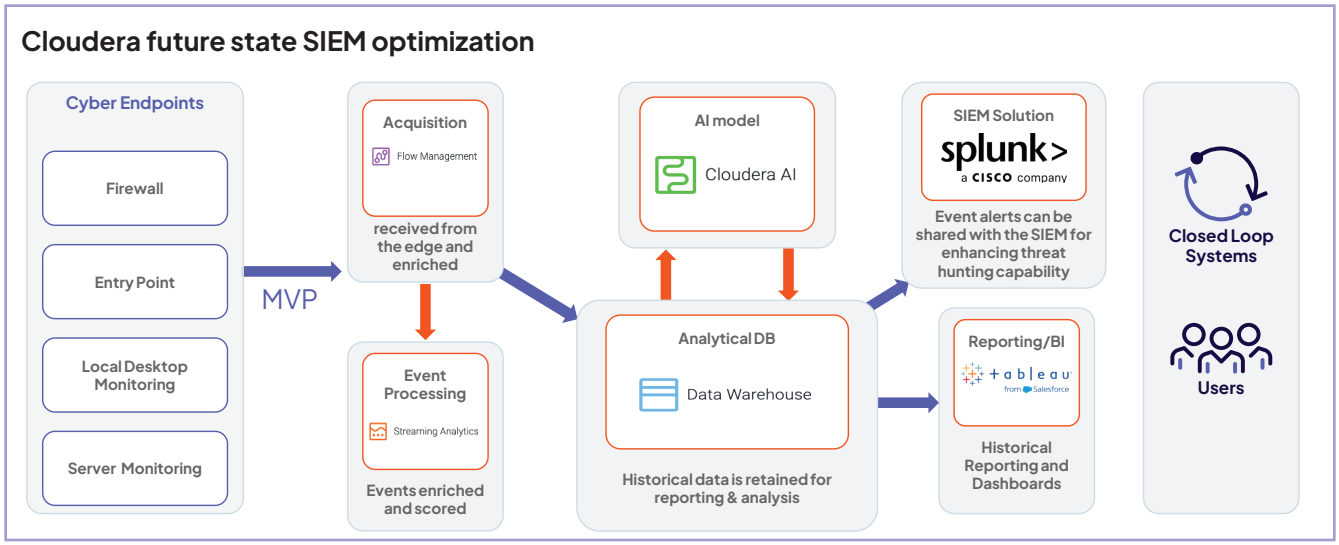
This intelligent processing layer transforms the traditional reactive model of SIEM operations into a proactive threat detection system that identifies and prioritizes security events based on actual risk rather than simple volume or predetermined rules.

Integration patterns for existing infrastructure

Implementation flexibility allows agencies to begin with minimum viable product (MVP) deployments that demonstrate value quickly while building a foundation for more sophisticated capabilities.



MVP Implementation focuses on immediate impact through direct integration with existing SIEM systems via standard APIs, basic filtering and aggregation that reduces data volume and improves quality, and historical data retention in cost-effective storage that maintains compliance requirements without straining budgets.



Advanced Implementation builds on proven foundations to include full AI/ML pipelines for predictive analytics that identify threats before they fully manifest, multi-destination routing that sends appropriate data to SIEM systems, data lakes, and compliance platforms simultaneously, and real-time dashboards and alerting capabilities that operate independently of SIEM systems while integrating seamlessly with existing workflows.

Measurable outcomes

The theoretical benefits of SIEM augmentation translate into concrete, measurable improvements that directly impact agency security posture and operational efficiency.

Performance improvements from real deployments

Mean time to detection is the most critical security metric in defensive cybersecurity. In deployments with large federal agencies, Cloudera's augmentation approach has reduced average detection time from over an hour to just minutes, transforming response capabilities. These gains result from intelligent filtering that surfaces genuine threats while suppressing false positives, allowing security teams to focus on actual incidents rather than noise.

Smart filtering reduces the volume of data sent to SIEM storage without missing critical security events. This comes from preprocessing that removes redundant information, preserving security-relevant context and enabling agencies to maintain comprehensive monitoring while controlling storage costs.

In addition, agencies using Cloudera have seen SIEM search durations cut by 50% or more. Faster searches support deeper investigations and faster remediation, reducing the likelihood of threats advancing undetected.

Over a five-year period, these combined efficiencies have resulted in significant cost savings through reduced storage requirements and enhanced analyst productivity. These savings create budget flexibility that agencies can redirect toward additional security or mission-critical programs.

Scalability for emerging mandates

Hybrid cloud flexibility enables deployment across on-premises, cloud, and edge environments that characterize modern government IT infrastructure. FedRAMP-authorized solutions, such as Cloudera, meet stringent federal security requirements while supporting emerging compliance mandates. As federal initiatives like Joint All-Domain Command and Control (JADC2) require increased data integration across agency boundaries, augmented SIEM platforms provide the secure foundation for information sharing. They also prepare agencies for AI-driven security innovations that can adapt to evolving threats without system replacement.

Cloudera: Meeting mandates without operational disruption

Federal agencies operate under increasingly complex compliance requirements that demand robust security and operational continuity. Cloudera's FedRAMP Moderate and GovRAMP Moderate authorizations and TX-RAMP Level 2 certified solutions give agencies at all levels the confidence to deploy across sensitive environments. Agencies at all levels can deploy Cloudera's data processing capabilities across sensitive environments without compromising their security posture or regulatory standing.

Seamless transition through parallel operation

During transition periods, agencies maintain full security coverage through their existing SIEM while Cloudera processes identical data streams to improve search performance and cost optimization. Security teams can compare results side-by-side, ensuring Cloudera delivers results before expanding deployment. This parallel operation also enables smoother onboarding when agencies need to integrate new security systems. Cloudera can feed data to existing and new platforms simultaneously, eliminating the typical integration challenges that create operational gaps during technology transitions.

Supporting today's operations and tomorrow's innovations

Government agencies need defensive capabilities that match the sophistication of modern threats while working within real-world operational constraints. By enhancing existing infrastructure rather than replacing it, agencies can significantly improve threat detection speed, reduce operational costs, and build foundations for AI-driven security innovations—all while preserving institutional knowledge and maintaining continuous protection.

The results demonstrate the impact: 90% faster threat detection, 60% reduction in data storage costs, and 55% improvement in search performance. Cloudera's augmentation approach delivers the defensive capabilities you need for mission success.

Visit Cloudera to learn more and schedule an appointment today: cloudera.com/publicsector

FedRAMP™ GovRAMP TX-RAMP CERTIFIED

CLOUDERA

Cloudera, Inc. | 5470 Great America Pkwy, Santa Clara, CA 95054 USA | cloudera.com

Cloudera is the only data and AI platform company that large organizations trust to bring AI to their data anywhere it lives. Unlike other providers, Cloudera delivers a consistent cloud experience that converges public clouds, data centers, and the edge, leveraging a proven open-source foundation. As the pioneer in big data, Cloudera empowers the public sector to apply AI and assert control over 100% of their data, in all forms, delivering unified security, governance, and real-time predictive insights. Over 200 top global government agencies rely on Cloudera to transform decision-making and ultimately boost bottom lines, safeguard against threats, and save lives.

To learn more, visit Cloudera.com and follow us on LinkedIn and X. Cloudera and associated marks are trademarks or registered trademarks of Cloudera, Inc. All other company and product names may be trademarks of their respective owners.

 WP-GBR 01 October 15, 2025