White Paper

Preventing the Quiet Leak: How a U.S. Government Agency Stopped Sensitive Data from Leaving Its Network with Personam

Executive Summary

A U.S. Government Agency managing critical financial reporting systems narrowly avoided a data-exposure event that could have violated federal compliance standards. One of several identical accounting servers began sending financial reports outside the network — not through an attack, but due to a misconfiguration.

Traditional monitoring tools saw nothing unusual. Personam's behavioral analytics did. By continuously comparing each server's behavior against its peers, Personam identified the single outlier in minutes. Administrators corrected the issue before any sensitive information reached an external network, preventing costly reputational and regulatory fallout.

This case illustrates how Personam exposes hidden risks, even when the cause is not malicious, by treating every deviation as worthy of investigation.

Key Takeaways:

- Peer-based behavior comparison detects configuration errors before damage.
- Continuous profiling ensures real-time compliance visibility.
- Metadata-driven analytics protect sensitive systems without disruption.

Personam turns every behavioral outlier into actionable assurance.

Customer Scenario

Organization: U.S. Government Agency
Mission: Manage secure, compliant financial reporting
Infrastructure: Cluster of Deltek accounting servers supporting federal contract operations
Objective: Maintain confidentiality and integrity of financial data across systems

The agency operated multiple accounting servers designed to perform identical functions. Each instance processed financial transactions and produced standardized reports for oversight entities. When Personam was deployed, analysts quickly saw one server behaving differently, connecting to an external IP address belonging to the software vendor.

The Challenge – When "Normal" Isn't

Government agencies face strict data-handling obligations under FAR, DFARS, and FISMA. Even benign errors can compromise compliance:

- **Misconfigurations mimic trusted activity.** Outbound connections appear legitimate.
- **Encrypted traffic hides unintended transmissions.** Conventional tools can't inspect payloads.
- **High system uniformity magnifies anomalies.** One misbehaving node may be the only warning.

The agency needed a solution that could distinguish between malicious intent and accidental risk, in real time and at operational scale.

The Technology Environment

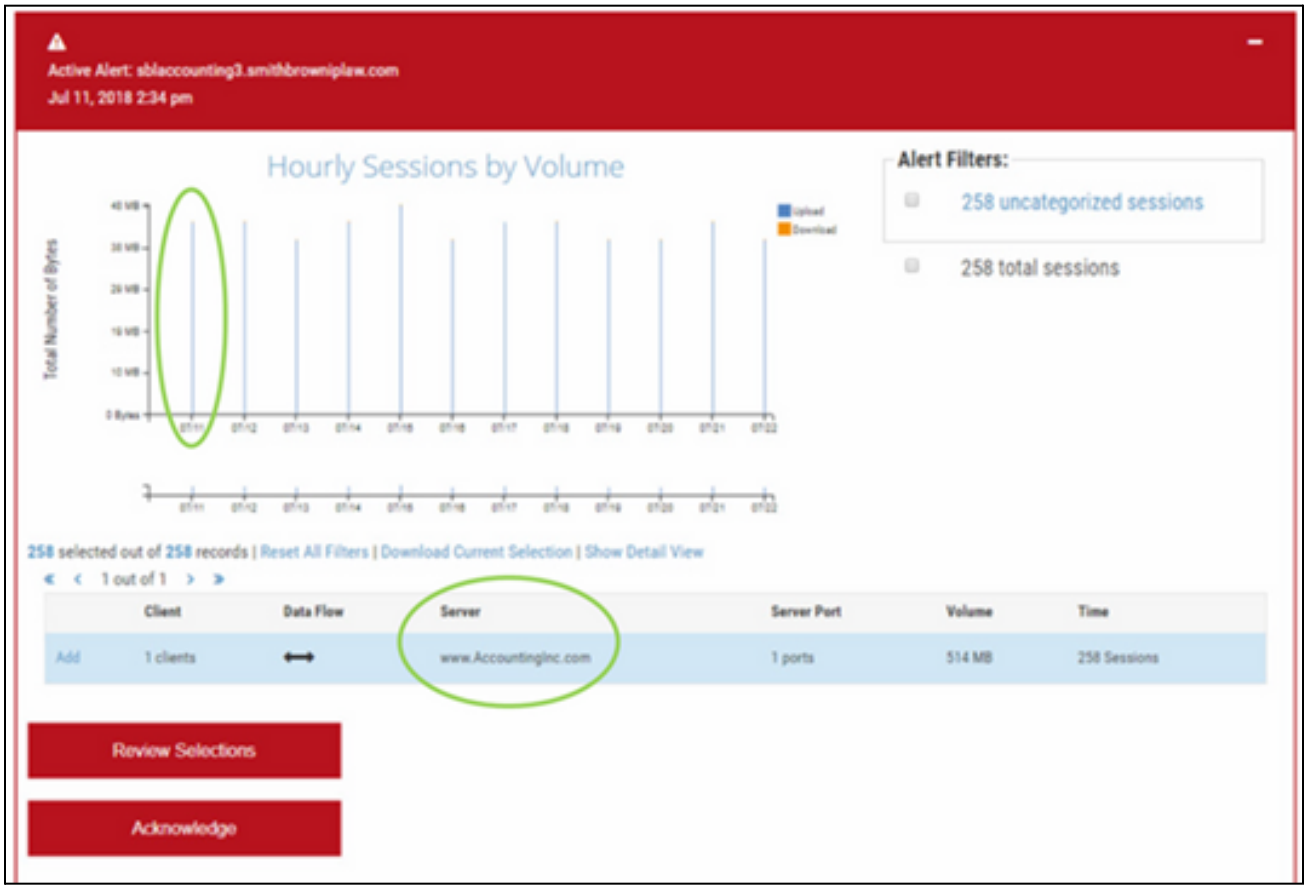
- Multiple Deltek accounting servers with identical roles
- Secure government network subject to continuous auditing
- Existing SIEM and endpoint tools unable to compare peer behavior
- Financial data transmissions governed by strict compliance boundaries

Personam was introduced as a non-disruptive behavioral layer, analyzing NetFlow and DNS metadata across the cluster without agents or payload inspection.

The Incident Timeline

Phase	Observed Behavior	Personam Detection
1 – Baseline Profiling	All four servers operate identically	Normal variance established
2 – Behavior Shift	One server begins regular external connections to vendor IP	Out-of-family deviation flagged
3 – Verification	Traffic confirmed to contain financial report emails	Alert classified as high-risk data leakage
4 – Remediation	Configuration error corrected and verified	Leakage channel closed within hours

Personam surfaced the behavioral outlier automatically, ranking it at the top of the outlier list based on variance from peer devices.



How Personam Works

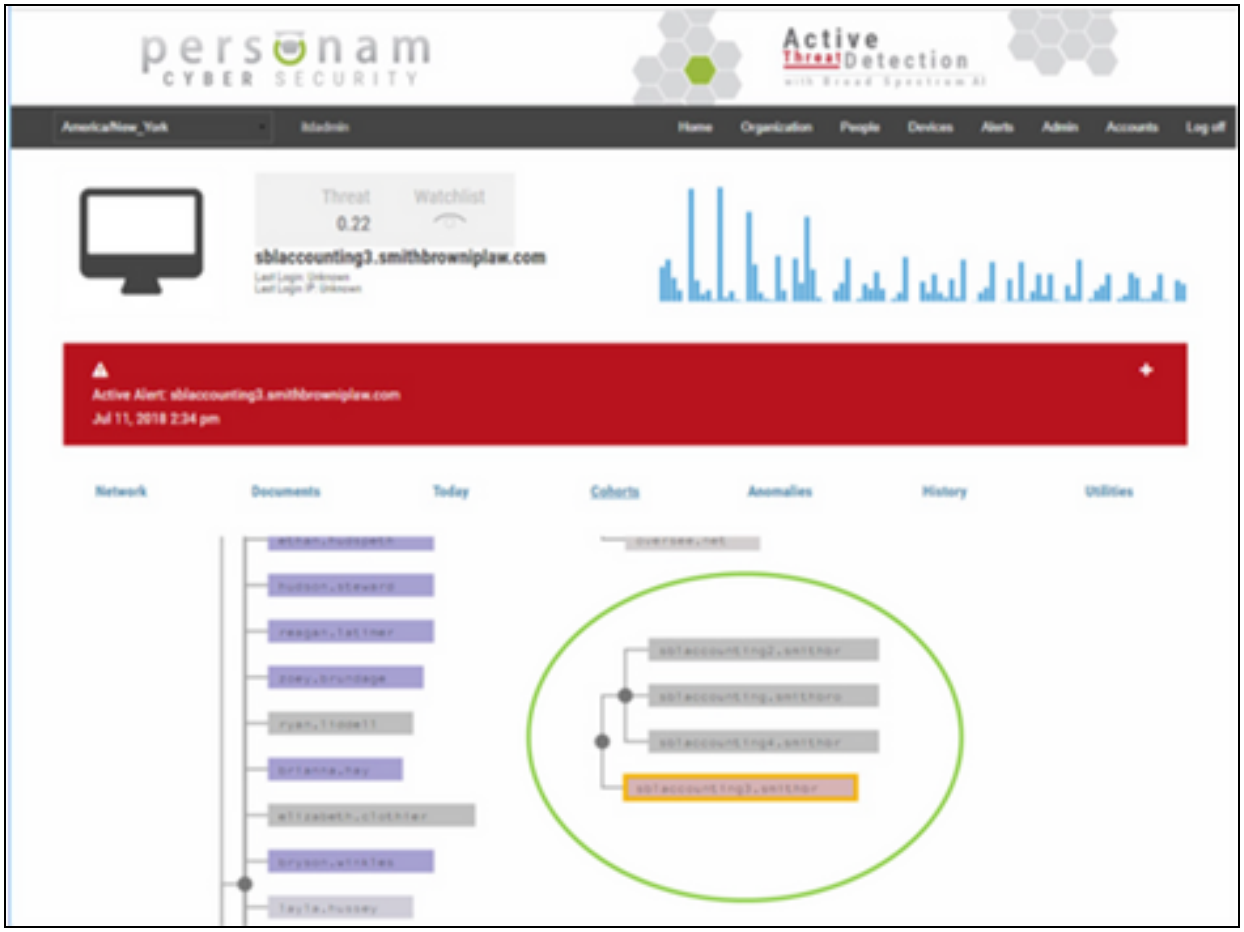
- **Profiles every device individually.** Builds continuous behavioral fingerprints for each system.

- **Compares peers in real time.** Highlights out-of-family patterns even among identical machines.
- **Scores risk continuously.** Dynamic threat index updates with every network transaction.
- **Uses metadata only.** Functions seamlessly on encrypted networks; no packet inspection required.
- **Guides response.** Provides exact connection details for rapid root-cause correction.

Why Personam Works

Challenge	Traditional Monitoring	Personam Behavioral Analytics
Detecting Misconfiguration	Requires manual review	Automated peer comparison
Encrypted Traffic	Opaque to content filters	Analyzes metadata patterns
False Positives	High noise from rules	Contextual scoring reduces noise
Operational Impact	Agent overhead	Zero-agent, passive deployment

By continuously learning expected peer behavior, Personam revealed an operational flaw invisible to signature-based tools.



Results

Sensitive Data Leakage Prevented — Zero Downtime

- Misconfigured server identified within minutes of deployment
- Root cause confirmed as erroneous email routing to external vendor address
- No data loss or compliance breach

Time to Detect: < 30 minutes
Remediation Time: < 4 hours
Financial and Reputational Impact: Avoided

Outcome – Operational Assurance Through Behavioral Insight

The incident proved that not every alert signals malice — but every alert provides insight. Personam's behavioral analysis allowed the agency to treat a simple

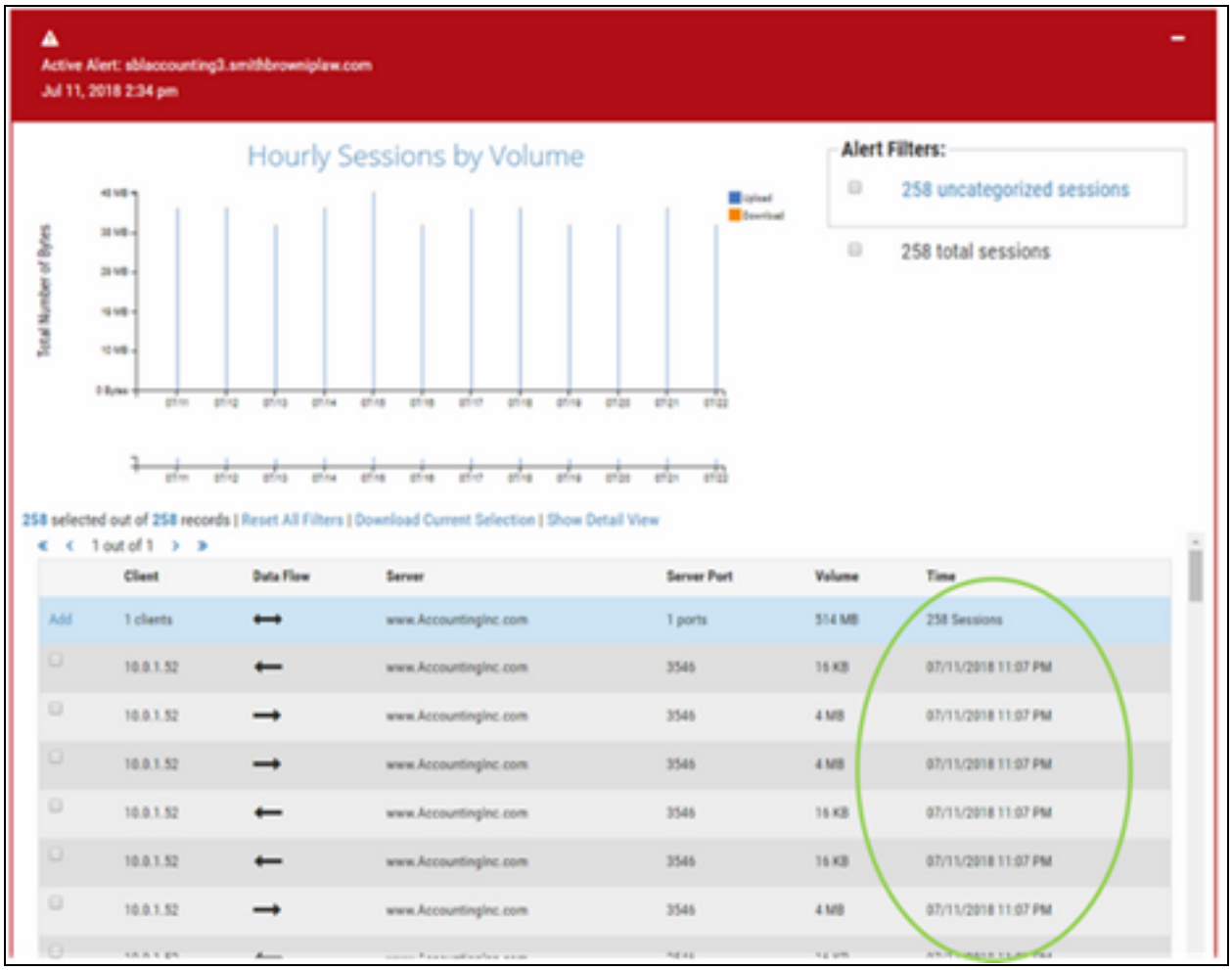
configuration error with the urgency it deserved, preventing unintended data transmission and demonstrating a culture of continuous security assurance.

Comparative Metrics

Metric	Before Personam	With Personam
Detection of Misconfigured Servers	Manual / Reactive	Automated / Real-Time
Time to Detect	Days or Weeks	Minutes
Time to Remediate	Multi-team effort	Single analyst / same day
Data Leakage Risk	Unknown until audit	Prevented in real time
Compliance Assurance	Periodic	Continuous behavioral monitoring

Broader Impact

In complex networks, mistakes and misconfigurations create the same symptoms as malicious activity — data moving where it shouldn't. By treating every outlier as an opportunity for visibility, Personam bridges the gap between cybersecurity and operational reliability.



Government agencies, financial institutions, and critical infrastructure providers use Personam to find the unknowns their tools were never designed to see.

Conclusion

This case demonstrates that behavioral analytics is as valuable for preventing accidents as for stopping attacks. By profiling every system and comparing peers continuously, Personam detects the subtle deviations that signal risk, malicious or not.

Contact

Personam.ai | learning@personam.ai | (703) 249-9585