

WHITE PAPER


Going Beyond Enterprise Security

Redefining End-User Digital Experiences Through Data-Driven Insights and Unified Observability



RAVENVISION
POWERED BY **RAVENTEK**

splunk>



Many organizational teams view IT performance data within the lens of the individual IT silos and tools for which they are responsible. This disjointed approach creates teams of IT experts looking at security, infrastructure, operations and network from varying points of view and priorities.

The challenge for organizations lies in the ability to build and maintain a resilient architecture that balances the demands of security and optimal end-user experiences. IT owners, who are responsible for maintaining stringent compliance mandates and driving key performance indicators (KPIs), must also balance competing business outcomes like security, application up time, infrastructure performance metrics, network performance metrics and cost.

LET'S EXPLORE HOW WE CAN HELP THEM...

Contents

The Power of Observability

What is Observability—Really?	5
A Bit on Splunk Observability	6
The Data Value Chain	7

Integrated Splunk Observability & RavenVISION

Assess & Plan	8
Common Data Sources	9
Build & Transform	9
Adopt & Transition	10
Automate	11

The Power of Observability

\$2.5M

Observability leaders' **average annual cost of downtime** associated with business-critical internally developed applications, **versus \$23.8 million** for beginners.*

69%

Better mean time to resolution for unplanned downtime or performance degradation, reported by observability leaders.*

**State of Observability 2022, Splunk*

What is Observability—Really?

Observability is traditionally defined as the ability to measure the internal states of a system by examining its outputs. Alternatively, in the context of enterprise IT, observability can be defined as the ability to use system generated data to measure and proactively diagnose operational and security issues across all seven layers of the Open Systems Interconnection (OSI) model while being able to monitor and respond to issues originating at each layer.

But the OSI model is missing one critical component - Layer 8: The User. Layer 8 highlights the importance of the interactions between users and the IT systems they depend on. Only by obtaining complete observability across all "8" layers can IT organizations truly predict,

prevent, respond to, and protect their ecosystem.

[RavenVISION](#), powered by RavenTek, leverages the power of Splunk Observability to achieve the visible integration of security, infrastructure, operations and network data needed to proactively drive multi-domain service efficiency.

As a certified Splunk partner and managed service provider, RavenTek delivers on business outcomes and solves real, complex problems by bringing the entire ecosystem, architecture and data into focus. By using Splunk as the backbone, RavenVISION aggregates and securely integrates multi-domain, multi-platform, multi-tool data and often dispersed, siloed datasets into actionable, contextualized insights.



A Bit on Splunk Observability

[Splunk](#) is traditionally known as a best-of-breed enterprise security information and event management (SIEM) platform that is often heavily leveraged by security operations teams but is underutilized, or completely dismissed, by other IT teams.

In a conversation with RavenTek CTO, Chris Riordan, Splunk's executive vice president of observability, Mala Pillutla stated, "A breach and an outage result in an equally bad situation." IT executives understand the technical nuances between the two; however, to business stakeholders and end users, breaches and outages mean downtime and loss in productivity.

IT organizations are challenged to proactively monitor and respond to every incident to avoid any and all negative impacts to business operations while balancing costs.

“

A breach and an outage result in an equally bad situation.”

Mala Pillutla

EVP, Observability
Splunk

RavenTek uses the RavenVISION Data Intelligence Model to identify and locate authoritative data sources across an organization. The discovery model incorporates core concepts of Zero Trust and Secure Enterprise Governance and Intelligence (SEGI), which provides a comprehensive approach to IT security and management with a focus on balancing the need for security with that of efficiency and innovation.

The discovery process starts by reviewing data requirements, current capabilities and the maturity of existing technology investments, as well as identifying gaps in the data and mapping all data seams or overlap that needs to be consolidated or optimized to build a data architecture with the highest levels of cardinality. RavenTek utilizes the discovered data in Splunk's data fusion tools to analyze and correlate disparate data and then apply and integrate ML and AI technology to guide insights and decisions.

Having worked with many large IT organizations over his career, Chris Riordan, understands the organizational challenges IT managers face when attempting

to share data across teams and environments to realize operational efficiencies. He states, "Often, organizational change is attempted at the people or process level. However, I have found that starting at the data level, and focusing on quality and real-time access to that data, enables organizations to promote real change through data-driven decisions."

Being able to make data-driven decisions starts with visibility of your data. Federal, state and local agencies need more than just visibility - they need complete, unified observability to understand and detect data gaps and data overlaps created by data silos. Complete, unified observability provides the ability to predict, prevent, respond to and protect against complex data challenges and these challenges are only getting more complex as more organizations move to cloud and micro-services. A new opportunity is on the forefront for agencies and organizations alike to reach beyond legacy 'monitoring' and evolve into 'visibility' and further into 'observability' to become champions of operational excellence, create amazing digital experiences and build resilient cyber operations.



Chris Riordan
CTO, RavenTek

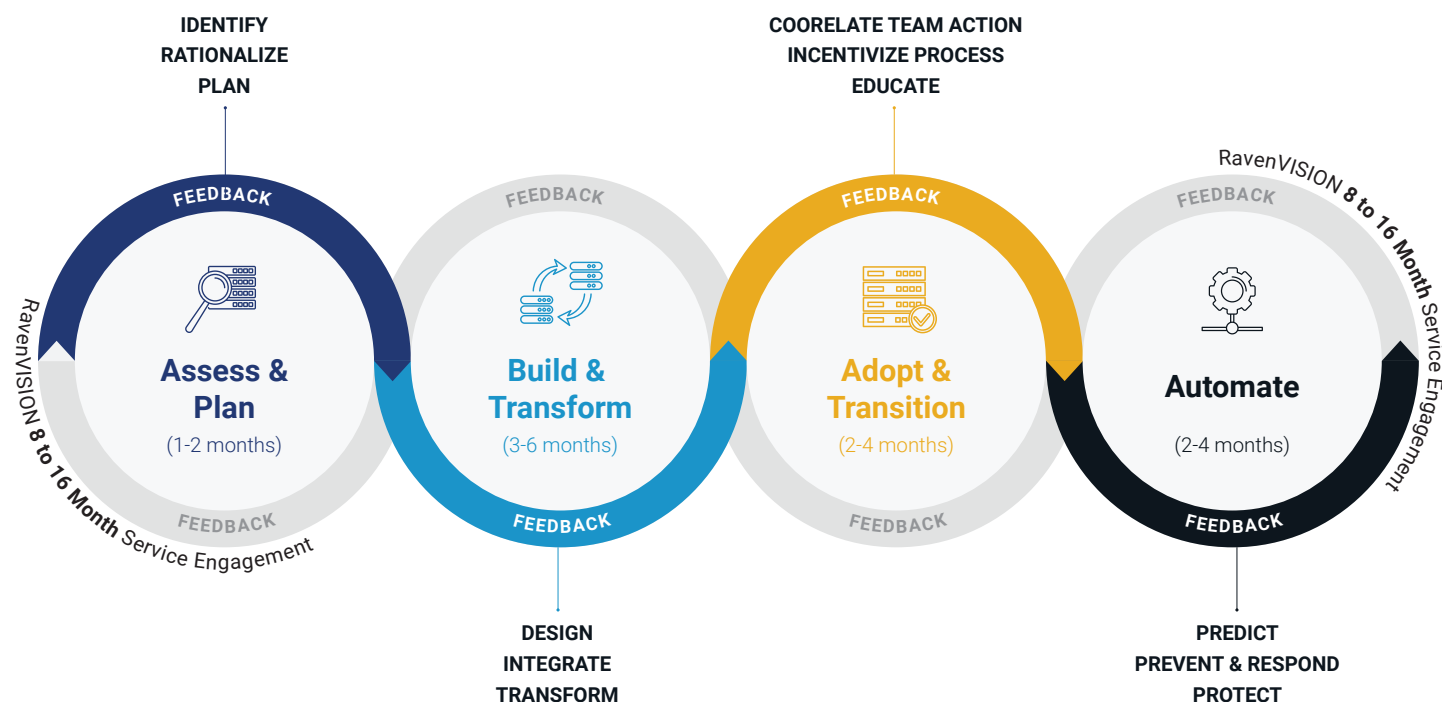
I have found that starting at the data level, and focusing on quality and real-time access to that data, enables organizations to promote real change through data-driven decisions.”

The Data Value Chain

RavenVISION leverages RavenTek’s Data Value Chain to create repeatable processes using a value-focused methodology for continuous integration and delivery of relevant data to gain real, empirical insights. The process integrates existing investments in Splunk and other technologies to build an efficient data platform with the mission to set and reach incremental, achievable goals.

The RavenVISION Data Value Chain is a service offering that follows 4 phases:

1. Assess & Plan
2. Build & Transform
3. Adopt & Transition
4. Automate



Leveraging Integrated Splunk Observability in the RavenVISION Data Value Chain



Assess & Plan

- **Identify:** Work across all teams to discover and analyze existing data sources
- **Rationalize:** Complete tools and data rationalization to identify visibility gaps and overlap
- **Plan:** Develop Observability data integration roadmap & schedule

Splunk Enterprise and Splunk Cloud solutions provide a comprehensive approach to security and operational data management in complex multi-cloud environments. These solutions allow you to:

- Leverage schema on the fly to aggregate data across environments and build a successful unified location for disparate structured and unstructured metrics, traces, and logs posture
- Enable the ability to normalize and manage critical data across various cloud service providers (CSPs) — including AWS, Azure and GCP — as well as platforms, applications and product implementations to better understand your complete data inventory
- Adopt, operationalize, and secure multiple cloud technologies across your infrastructure
- Conduct effective security investigations and analysis across multi-cloud services
- Empower better visibility and understanding of data across multi-cloud environments for better investigation, alerting, remediation and reporting
- Normalize and manage data across hybrid and cloud infrastructures to better analyze and detect threats, vulnerabilities and operational risks
- Control costs by understanding data requirements, optimizing utilization of multiple tools providing similar data and scaling as demands grow



Common Data Sources

- Network flow data: router/switch counters, firewall logs
- Virtual servers: VM Logs, ESXi logs
- Cloud services: AWS data sources such as EC2, EMR, S3
- Docker: logging driver, syslog, apps logs
- Containers and microservice architectures: logs, container metrics and events
- Third-party services: SaaS, FaaS, serverless
- Control systems: vCenter, Swarm, Kubernetes
- Dev automation: Jenkins, Sonarcube
- Infra orchestration: Chef, Puppet, Ansible
- Signals from mobile devices: product adoption, users and clients, feature adoption
- Metrics for business analytics: app data, HTTP events, SFA/CRM
- Signals from social sentiment analytics: analyzing tweets over time
- User experience analytics: app logs, business process logs, call detail records
- Message buses and middleware

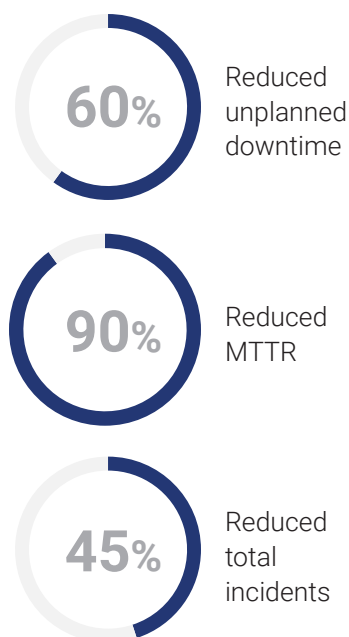


Build & Transform

- **Design:** Architect existing and new data source integrations to fill gaps and eliminate overlaps in data
- **Integrate:** Integrate data flows into Observability data warehouse
- **Transform:** Transform and correlate data into actionable reports, alerts, visualizations, and reports

Splunk IT Operations / ITSI enable you to:

- Seamlessly integrate data across the organization to give all stakeholders a clear picture of what's happening and why
- Ingest data once and leverage it across use cases to get a handle on tool proliferation
- Apply purpose-built cloud solutions for IT, DevOps and security to manage, secure and optimize all aspects of the organization
- **Protect performance and availability:** Reduce unplanned downtime by 60%
- **Realize efficient IT management:** Reduce alert noise by 95% and mean time to repair (MTTR) by 90%
- **Experience end-to-end service visibility:** Prevent service degradations 30 minutes in advance and reduce total incidents by 45%





Adopt & Transition

- **Correlate Team Action:** Use correlative analytics to identify data interaction and impact across teams
- **Incentivize Process:** Drive efficiency and reduced MTTR through data synergy in incident response
- **Educate:** Encourage team data use for decision making, and train ML to use cases

Splunk Unified Observability enables:

- **Infrastructure Investigation & Monitoring:** Monitor and manage hybrid, multi-cloud environments as well as your existing data center infrastructure with a unified, enterprise-wide solution
- **Business Service Insights:** Tie together tech and business data to ensure the health of critical business services and delight your customers
- **Full-stack Observability:** Accelerate innovation with Splunk's Microservices APM that provides a directed approach to troubleshooting for maximum DevOps performance
- **Unified Cloud Security:** Modernize and optimize security operations, strengthen cyber defenses and reduce risk exposure
- **Spot problems with full-fidelity tracing and find out why they occurred** with Splunk's proprietary investigative capabilities





Automate

- **Predict:** Apply AI to ML use cases starting repetitive incident processes
- **Prevent & Respond:** Apply data-driven Security and Operations automation playbooks to enhance your Prevent and Respond posture leveraging measurable KPI's to demonstrate quantitative results
- **Protect:** Increase proactive intelligence fusion for threat hunting and protection as well as enhance reliability of Zero-trust Policy Administrators, and Compliance scores

Splunk ML toolkit/SOAR/Premium Addons/UBA/Synthetics allow you to:

- Go beyond monitoring with advanced analytics fueled by Unbounded Machine Learning, collaboration and automation — all from a single platform
- Collect, process, distribute and gain insights from data in milliseconds with real-time stream processing
- Automate incident response and threat remediation to augment your team's resources and resolve issues significantly faster
- Better predict what's going to happen in the future through high-quality observability systems with learning algorithms that can understand the past health of your services and applications
- Fully ingest all the data about your organization so that machine learning models get accurate perspectives of historical and real-time data
- Predict high-likelihood, potential future events and harnesses the power of AI through ML to achieve predictive intelligence. AI-driven analytics Advances in AI can benefit you by doing the following:
 - » Reducing event clutter and false positives with multivariate anomaly detection
 - » Automatically concealing duplicate events to focus on relevant ones and reducing alert storms
 - » Easily sifting through vast amounts of events by filtering, tagging and sorting
 - » Enriching and adding context to events to make them informative and actionable
- Monitor applications automatically utilizing synthetic transactions to predict and detect problems before users realize them
- Baseline, trend, analyze, detect, and predict user behavior to inform operational decisions and detect security threats among the user base





As part of RavenVISION, the RavenTek team applies its expert knowledge in a wide array of industry tools and technologies, as well as proprietary API integrations and visualization tools, to provide a faster time-to-value. The observability dashboards can be delivered through the RavenVISION Splunk app or through a customized front-end dashboard that leverages COTS technologies. Neither of these are sold or licensed as a product and are strictly delivered as part of a RavenTek service offering.

To learn more about this service offering, visit raventek.com/ravenVISION



RavenTek provides digital transformation and cybersecurity solutions and services to mission critical organizations worldwide. As a Veteran and Native-American-owned business, we combine small-company agility with big-company stability—applying our team’s industry expertise to understanding client business needs and delivering the right solutions, at the right time.

Learn more at raventek.com

© Copyright 2023 RavenTek. All Rights Reserved.

