

Supercharge Security with Real-Time Threat Detection and Automation

Your attack surface is expanding—your visibility should too. Dataminr amplifies Splunk's powerful data analytics and automation platform with AI-powered external threat detection, combining actionable alerts with your security telemetry. When risks emerge, receive instant alerts to take proactive action and automate response within your existing Splunk environment.

Data Gaps Are Growing—And So Is the Risk

THIRD-PARTY VISIBILITY

40%

of compliance leaders say a significant portion of their third-party relationships are high risk¹

SKILLED STAFF SHORTAGES

50%

of organizations cite a shortage of skilled staff as the biggest barrier to effective threat hunting²

EXPANDING ATTACK SURFACES

30B

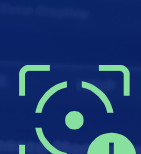
IoT devices will be in use by 2030, increasing the cyber-physical attack surface³

Expand Visibility with an External View



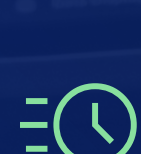
Limited third-party monitoring

Lack of visibility beyond organizational boundaries



Disconnected physical and cyber security

Siloed systems miss threats that cross domains



Vulnerabilities that demand urgent action

Teams can't keep pace with fast-moving risks



Alert overload and prioritization gaps

Too many alerts and no idea what's important



Slow, manual remediation processes

Delayed responses give attackers more time to exploit



Reactive detection and delays

Threats surface late due to outdated legacy intel

How Dataminr + Splunk Help You Mitigate Risk

Dataminr real-time alerts connect directly with Splunk Enterprise, Splunk Cloud, or Splunk SOAR, making it easy to visualize threats, automate response, and take action faster—all within the tools your team already uses.



Rich metadata

Dataminr alerts include 100+ fields to drive precision and automation



Automation

Trigger SOAR playbooks automatically based on early warning signals



CIM integration

Use external Dataminr alerts for both built-in and custom dashboards



IoC correlation

Map alerts to internal telemetry to improve threat hunting



Pre-built dashboards

Visualize alerts and events in Splunk with out-of-the-box dashboards

High-Value Gains You Can Measure

With Dataminr + Splunk, you can enhance security, resilience, and operational efficiency by proactively identifying, analyzing, and responding to emerging, cyber, physical, operational, and reputational risks.



Operational efficiency

Cut through noise and focus on the most important threats



Faster response times

Accelerate detection, prioritization, and remediation



Proactive defense

Identify threats early and act before they escalate



Continuous visibility

Reduce risk with real-time threat exposure management



Stronger ROI

Maximize the value of your existing Splunk investment

Turning Data Into Action



MITIGATE THIRD-PARTY RISK

Financial services organization

A global bank receives an alert just minutes after a vendor is hit with ransomware. The security team takes action to prevent downstream impact while an automated workflow notifies internal stakeholders, all before they receive word from the vendor.



CONVERGE CYBER AND PHYSICAL SECURITY

Government agency

A federal agency receives real-time alerts about suspicious activity near a secure facility. At the same time, login anomalies appear in Splunk. With unified visibility across domains, the agency escalates response and prevents further compromise.



ADOPT CONTINUOUS THREAT EXPOSURE

National energy provider

A power company is alerted to a zero-day exploit targeting its operational technology (OT) infrastructure. Flagged by Dataminr and correlated in Splunk, the team links it to internal assets and triggers automated patching—avoiding costly disruption.

Let's Make an Impact Together

Make the most of your Splunk investment with real-time, AI-powered alerting. Join the organizations transforming security with the Dataminr + Splunk joint solution to expand visibility, accelerate threat detection, automate response—and keep your organization ahead of emerging threats.

Talk to our team today and let's build smarter cyber defense—together.

[Click here](#) to request a demo of real-time external context with Dataminr and Splunk.

Sources

1. Gartner, *Third-Party Risk Management Best Practices*, Oct 2024.
2. SANS Institute, *SANS 2024 Threat Hunting Survey: Hunting for Normal Within Chaos*, Mar 2024.
3. Statista, *Number of Internet of Things (IoT) Connections Worldwide from 2022 to 2023*, June 2024.