splunk> turn data into doing

CASE STUDY

# GoTo Accelerates Detection Use Case and Reduces Manual Analyst Workflow With Splunk Intelligence Management

## Key Challenges

Without an intelligence management platform, GoTo was manually conducting correlation and analysis across multiple intelligence sources — a time-intensive process because each intelligence feed needed to be viewed individually.

## Key Results

GoTo now uses Splunk Intelligence Management to automatically ingest, normalize and correlate multiple intelligence sources, leading to significant time savings and easier collaboration across teams.

**Industry:** Online Services

**Solutions:** Platform

## To scale, organizations must embrace the power and potential of automation.

A pioneer in remote work technology and a driving force behind today's work-from-anywhere movement, GoTo (formerly LogMeIn) has become one of the world's largest SaaS companies with tens of millions of active users, more than 3,500 global employees, over $1.3 billion in annual revenue, and approximately two million customers worldwide who use its software as an essential part of their daily lives. They offer a wide range of products and services including Unified Communications & Collaboration, Identity & Access Management, and Customer Engagement & Support.

### Turning Data Into Outcomes

- 10s of hours saved each week
- Reduced manual cycles
- Easy cross-team collaboration

Prior to implementing Splunk Intelligence Management, GoTo lacked an intelligence management platform. They were submitting intel feeds directly into Splunk Enterprise Security but could not visually manipulate or correlate the data from multiple data feeds. Each investigation meant that they needed to access intelligence feeds separately and then attempt to manually correlate and analyze the data, which was very time intensive.

Splunk Intelligence Management has given GoTo a single source of truth for multiple data sources. The time saved has allowed GoTo to scale to meet customer demand.

### Don't mind the gap — fix it

Before Splunk Intelligence Management, the team at GoTo lacked a centralized intelligence management platform and struggled with the gap in point-to-point intel. Now team members can easily combine their threat intel feeds into one centralized, cloud-native platform. Internal and external data sources are automatically ingested, normalized and correlated to help prioritize investigations — and accelerate triage. By using a bi-directional data flow and a uniform tagging system, GoTo is able to have a wider view of information enriching opportunities and improved visibility across diverse intelligence sources.

And by cutting out manual, point-to-point investigations, GoTo now has a central place to coordinate their response efforts. This eliminates redundant analyst workflows across multiple tools — saving GoTo tens of hours each week by cutting down on redundant workflows.

It was also easy for the GoTo team to get started. "Splunk Intelligence Management allowed me to play out my use cases for free," says Mike Rennie, threat and vulnerability manager at GoTo. "Seeing the value that even the free version provided as an IT-ISAC member, and then seeing what the paid version could do with allowing us to bring in indicators from other sources was a no-brainer for our organization."

Splunk Intelligence Management allowed me to play out my use cases for free. Seeing the value that even the free version provided as an IT-ISAC member, and then seeing what the paid version could do with allowing us to bring in indicators from other sources was a no-brainer for our organization."

**Mike Rennie,** Threat & Vulnerability Manager at GoTo

## Informed, actionable automation

With Splunk Intelligence Management, it's now easier for GoTo to manage a diverse set of tools. GoTo uses the platform to manage premium intel and open-source feeds to populate Splunk Enterprise Security for alerting and then enrichment in ServiceNow.

They can also manipulate indicators, add notes and tags and correlate data. Splunk Intelligence Management uses dynamic, cloud-based intelligence repositories known as Enclaves to manage user permissions and control proprietary flows of intelligence to tools and teams. This allows GoTo team members to maintain data that they may not want to alert on, such as firewall events, email events, endpoint protection events, endpoint protection events, IP addresses, or domain names to use for correlation against other intel in Splunk Intelligence Management.

## Next up: scalability and success

With Splunk Intelligence Management automating tasks that previously took as much as 40 hours per week, GoTo was able to scale to meet customer demand. The organization will continue to rely on Splunk Intelligence Management as it continues to help companies and individuals do their best work.



22-19521-Splunk-GoTo-CS-101