TANIUM | Cribl

SOLUTION BRIEF

Enhance Endpoint Management and Security with Tanium and Cribl LogStream™

SOLUTION BRIEF

Enhance Endpoint Management and Security with Tanium and Cribl LogStream™

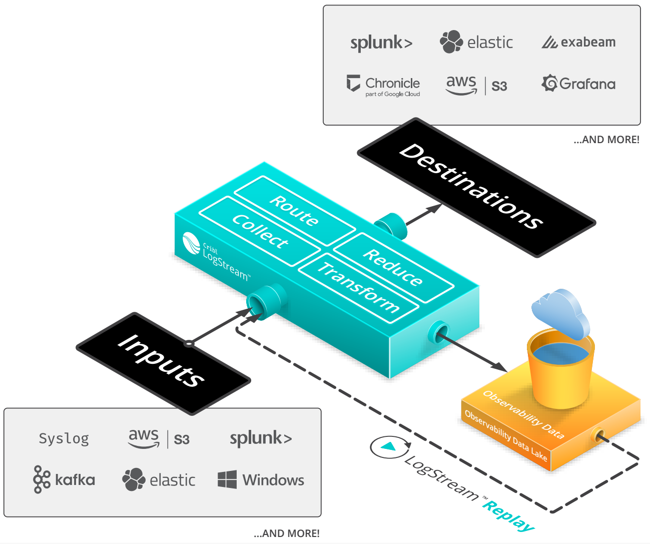
Together, the Tanium platform and Cribl LogStream provide a way for security and IT operations teams to better manage endpoint data and effectively integrate all their tools, reducing complexity and improving efficiency.

The Power of Tanium and Cribl

Need to use endpoint data to inform IT decisions on premises or in the cloud? No problem. Tanium provides high-fidelity endpoint data to enterprises with workflows spanning multiple domains in IT, including security operations, risk, and compliance. Tanium's endpoint and management security capabilities allow teams to query millions of endpoints in seconds using a single agent, a single console, and zero intermediate infrastructure. Teams can further integrate the rest of the Tanium platform with SIEM solutions, log analytics tools, threat feeds, or use it to send email notifications.

Those same organizations are turning to Cribl LogStream for similar reasons. They need an observability pipeline with the flexibility to get data into multiple tools from multiple sources without adding new infrastructure and agents. These companies also need a tool that can flex with them – deployable on premises or in the cloud. At the same time, they need an observability solution that gives them the ability to make new business decisions and test out new use cases at scale, regardless of the amount of data they have.

Together, Tanium Connect and Cribl LogStream provide a way for security and IT operations teams to better manage endpoint data and effectively integrate all their tools, reducing complexity and improving efficiency. When they further combine LogStream and the rest of the Tanium platform with Tanium Connect, these teams can easily integrate all their tools – reducing complexity, improving efficiency, and closing the gaps between operations and security.



THE CHALLENGE

Companies using the Tanium platform to manage endpoint data on premises or in the cloud need an observability pipeline to match – giving them the flexibility to test out new use cases at scale and inform critical IT decisions.

THE SOLUTION

When customers combine Cribl LogStream with the Tanium platform, security and ITOps can easily integrate all their tools – reducing complexity, improving efficiency, and closing the gaps between both teams.

THE BENEFITS

- Route Tanium endpoint data to the analytics tool or destination of your choice
- Reduce Connect data for faster incident response
- Enrich Tanium data in-flight for improved context and visibility
- Reduce workload on the Tanium platform – increasing data consistency and reducing overhead

CRIBL LOGSTREAM CAN SEND DATA TO AND FROM ANYWHERE, GIVING YOU THE FLEXIBILITY TO SEND TANIUM DATA TO KAFKA, AND ANY AWS, AZURE, OR GCP DESTINATION.

The Benefits of using Tanium with Cribl LogStream

ROUTE TANIUM ENDPOINT DATA TO THE ANALYTICS TOOL OR DESTINATION OF YOUR CHOICE

Cribl LogStream can send data to and from anywhere, giving you the flexibility to send Tanium endpoint data to the best tool for the job – or all the tools for the job – by translating and formatting the data into the appropriate tooling schema. Use LogStream to send Tanium data to Kafka, and any AWS, Azure, or GCP destination.

REDUCE CONNECT DATA FOR FASTER INCIDENT RESPONSE

With LogStream, you can easily eliminate duplicate fields, null values, and any elements from Connect data that provide little analytical value. In the same interface, you can filter and screen events for dynamic sampling, or aggregate log data into metrics to keep your downstream clean.

ENRICH TANIUM DATA IN FLIGHT FOR IMPROVED CONTEXT AND VISIBILITY

LogStream helps you process any observability data – like Tanium data – in real time. You can quickly add GeoIP information, DNS information, and more to your endpoint data in flight for improved context and visibility. When you use Cribl LogStream to enrich your Tanium endpoint data, your logs and events already have everything you need to start every investigation off on the right foot.

REDUCE WORKLOAD ON THE TANIUM PLATFORM – INCREASING DATA CONSISTENCY AND REDUCING OVERHEAD

Running multiple Tanium Connect jobs can be taxing on your resources, and with each job you put into motion, you run the risk of inconsistencies in your endpoint data. Rather than running multiple Connect jobs, you can run one Connect job and use Cribl LogStream to send the data everywhere it needs to go, increasing data consistency and reducing overhead.

CRIBL LOGSTREAM IS AN OBSERVABILITY PIPELINE THAT PROVIDES THE SIMPLICITY, FLEXIBILITY, AND CONTROL TO WORK WITH ANY TOOLING AND PERFORM WELL WITH EVEN THE LARGEST AMOUNTS OF DATA – MAKING IT THE PERFECT COMPLEMENT TO TANIUM.

Summary

Many enterprises are turning to the Tanium platform to manage and secure their endpoint data, while reducing complexity, improving efficiency, and closing the gaps between operations and security. These same enterprises now need an observability tool to match: flexible, reliable, and deployable anywhere. Cribl LogStream is an observability pipeline that provides the simplicity, flexibility, and control to work with any tooling and perform well with even the largest amounts of data – making it the perfect complement to Tanium.

With Cribl LogStream, Tanium customers can:

- *Route Tanium endpoint data to the analytics tool or destination of your choice*
- *Reduce Connect data for faster incident response*
- *Enrich Tanium data in-flight for improved context and visibility*
- *Reduce workload on the Tanium platform – increasing data consistency and reducing overhead*

Together, the Tanium platform and Cribl LogStream provide a way for security and IT operations teams to better manage endpoint data and effectively integrate all their tools, reducing complexity and improving efficiency.

To get started with Tanium and Cribl LogStream today, click here to sign up for LogStream Cloud. The Cribl Slack Community is also a great place to connect with leaders from other teams leveraging both Tanium and Cribl.

ABOUT TANIUM

Tanium gives the world's largest enterprises and government organizations the unique power to secure, control, and manage millions of endpoints across the enterprise within seconds. Serving as the "central nervous system" for enterprises, Tanium empowers security and IT operations teams to ask questions about the state of every endpoint across the enterprise in plain English, retrieve data on their current and historical state, and execute change as necessary, all within seconds. With the unprecedented speed, scale, and simplicity of Tanium, organizations now have complete and accurate information on the state of endpoints at all times to more effectively protect against modern day threats and realize new levels of efficiency in IT operations. For more information, visit tanium.com.

ABOUT CRIBL

Cribl is a company built to solve customer data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route security and observability data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit www.cribl.io or our LinkedIn, Twitter, or Slack community.