ADVANCED TECHNOLOGY GROUP (ATG)

Integrating IBM Defender and IBM FlashSystems with Splunk

Dan Thompson
Data Protect Architect
IBM Advanced Technology Group
danthomp@us.ibm.com

Matt Key
Principal Storage Technical Specialist
IBM Advanced Technology Group – FlashSystem
IBM Technology
mkey@us.ibm.com

Byron Grossnickle
Principal Storage Technical Specialist
IBM Advanced Technology Group – IBM Storage Virtualize/FlashSystem SME
byrongro@us.ibm.com

Accelerate with ATG Technical Webinar Series

Advanced Technology Group subject matter experts cover a variety of technical topics.

Audience: Clients who have or are considering acquiring IBM Storage solutions. Business Partners & IBMers are welcomed, too.

To automatically receive announcements of upcoming Accelerate with IBM Storage webinars, Clients, Business Partners & IBMers are welcome to send an email request to **accelerate-join@hursley.ibm.com**.

Integrating IBM Defender Data Protect and FlashSystems disk with Splunk - Tuesday, August 18th, 2026

IBM Gen 8 FICON Essentials: Securing and Optimizing the z17 and DS8000 Data Path - Thursday, August 20th, 2026

ATG Accelerate Site ← Click here to access the Accelerate with ATG webinar schedule for 2026, view presentation materials, and watch past replays.

ATG MediaCenter Channel ← This channel offers a wealth of additional videos covering a wide range of storage topics, including IBM Flash, DS8, Tape, Ceph, Fusion, Cyber Resiliency, Cloud Object Storage, and more . . .

ATG Offerings

Client Technical Workshops

- Cyber Resilience with IBM Storage Defender
- IBM Fusion & Ceph
- IBM DS8000 G10 Advanced Functions

TechZone Test Drive / Demo's

- IBM Cloud Object Storage Test Drive - (VMware based)
- IBM DS8900F Safeguarded Copy (SGC) Test Drive
- IBM DS8900F Storage Management Test Drive
- IBM Fusion Test Drive – Backup and Restore with OpenShift Virtualization
- Managing Copy Services on the DS8000 Using IBM Copy Services Manager Test Drive
- IBM Storage Ceph Test Drive
- IBM Storage Ceph Test Drive - (VMware based)
- IBM Storage Protect Live Test Drive
- IBM Storage Scale and Storage Scale System GUI
- IBM Storage Virtualize Test Drive

Please reach out to your IBM Representative or Business Partner for more information.

***IMPORTANT* The ATG team serves clients and Business Partners in the Americas, concentrating on North America.**

Please take our survey!

Please take a moment to share your feedback with our team!

You can access this 6-question survey via this direct link: **https://ibm.biz/Bdpcj3**

Or you can use this QR Code:

What is Splunk?

You probably already think you know what Splunk is; but:

Google-Fu:

- Splunk is a software platform that collects, stores, searches, and analyzes machine-generated data from websites, applications, and devices. It turns raw log files and metrics into real-time dashboards, alerts, and reports to help companies monitor systems and find security threats.

From Splunk web site:

- Though Splunk can refer to the company or its broader technology suite, it's anchored by a unified core: the **Splunk platform**, delivered as Splunk Enterprise for on-premises environments and Splunk Cloud Platform for SaaS. Regardless of deployment, this powerful data platform helps organizations collect, analyze, and act on machine-generated data in real time, powering solutions across observability, security, IT operations, and business analytics.
- Built on the unified Splunk platform, Splunk's solutions — including Enterprise Security (SIEM), Observability Cloud, and SOAR — extend its core capabilities to meet specific security and IT needs. These aren't standalone tools, but powerful use-case layers built directly on the platform.

Why Do I want to Integrate With Splunk?

- Generally, every production component in an enterprise should send alerts and/or logs to the corporate data aggregation/SIEM/SOAR infrastructure.
- Depending upon the platform, this will allow multiple integration points, reporting, monitoring, etc. You might feed problem management, change management, etc. from this central point.
- Integrating with SIEM/SOAR allows you to bring security violations and alerts into the security operations toolset.
- Should I integrate non-production systems with Splunk? Ideally you would test Splunk integration along with core functionality of your important componentry.

How does a component integrate with Splunk

- There are multiple integration points, depending upon the component.
- For example, Defender Data Protect can integrate in 4 ways:
- Syslog
- RESTful API
- Integration Application
- WebHooks

How does a component integrate with Splunk

- There are multiple integration points, depending upon the component.
- For example, Defender Data Protect can integrate in 4 ways:
- Syslog
- ~~RESTful API~~
- ~~Integration Application~~
- WebHooks

WebHooks is considered the replacement for older or more complicated methods for alert aggregation.

Typically, depending upon the application, WebHooks are used to send alerting.

Syslog allows system logs of different types to be forwarded to a central Syslog server.

So, it depends upon what you want to do with what data. Generally, alert forwarding allows the application to decide what to raise an alert for, which syslog allows you to dig into details but requires greater post-processing. It is entirely possible you will want both.

How do you achieve this integration?

For all data input types you may wish to create a custom INDEX where that data is stored. This allows you to isolate the information and avoid flooding the default index with data from every component. In either method below, you will define an input and then have it use the default or dedicated index.

SYSLOG:

Enable a syslog server (rsyslog on Linux) to receive and store logs from a component. If you want to isolate the data or format how logs are stored, you can have a rule with a unique port (TCP and or UDP). Have your component send syslog data to that target.

NOTE: In our demo, we are running the syslog server on the same host as Splunk Enterprise and defining an input type of File (identifying it as syslog data).

This is not recommended:

The most modern method is to deploy a Splunk Connect for Syslog container and have it forward events via webhooks. Another method is to deploy a traditional syslog server on a different host and install a Universal Forwarder to send data to the Splunk environment.

WebHooks:

Define an input type as HTTP Event Collector (which generates a unique token) the configure your component to send data to that collector.

Example Syslog Rule

Stored in /etc/rsyslog.d in unique file:

```
# Load UDP and TCP input modules to listen on standard port 514
module(load="imudp")
input(type="imudp" port="6514")

module(load="imtcp")
input(type="imtcp" port="6514")

# Define file permissions so the 'splunk' group can read the logs
$FileOwner root
$FileGroup splunk
$FileCreateMode 0640
$DirCreateMode 0750

# Create a dynamic folder template based on the sending device's hostname
template(name="SplunkDynamicPath" type="string" string="/var/log/splunk/%HOSTNAME%/%PROGRAMNAME%.log")

# Write all remote network messages to the dynamic path and stop processing
if ($fromhost-ip != '127.0.0.1') then {
    action(type="omfile" dynaFile="SplunkDynamicPath")
    stop
}
```

Documentation on integrating Storage Insights with Splunk SOAR via Webhooks

https://community.ibm.com/community/user/blogs/satyam-kaushik/2025/08/05/automating-ransomware-response-integrating-ibm-si

Automating Ransomware Response: Integrating IBM Storage Insights with Splunk and Splunk SOAR

As ransomware threats grow in sophistication and frequency, organizations must adopt proactive and automated defense mechanisms. IBM Storage Insights (SI), a cloud-native SaaS platform, provides real-time ransomware detection across IBM storage systems. When integrated with Splunk and Splunk SOAR, SI becomes a powerful component in a broader security operations strategy—enabling centralized monitoring, automated alert forwarding, and orchestrated incident response.

This blog outlines the end-to-end integration of IBM Storage Insights with Splunk and Splunk SOAR to streamline ransomware alert management and response.

Integrating Defender Data Protect with Splunk

Look for the Cohesity Solutions Guide for Integrating Cohesity with Splunk (covers webhooks), on MyCohesity partner/customer portal.

Title: Integrate Splunk with Cohesity

Demos

Demo:

- Splunk Indexes
- Splunk Data Input
- Pointing Defender Data Protect to Splunk via Webhooks
- Pointing Defender Data Protect to Splunk via Syslog
- Integrating IBM FlashSystems to Splunk via Syslog
- Review syslog folders.
- Review data in Splunk
- You are Free!!!

Please take our survey!

Please take a moment to share your feedback with our team!

You can access this 6-question survey via this direct link: **https://ibm.biz/Bdpcj3**

Or you can use this QR Code:

Thank You