OPTIMIZING ENTERPRISE SECURITY WITH SPLUNK ON PURE

AN IT DEPLOYMENT SUCCESS STORY

Here in IT, our strategic deployment of **Splunk** on Pure's **FlashArray //M20** has afforded us significant advantages over alternative deployment methods and enabled our Security team to get the most out of Splunk Enterprise Security (ES) as our security information and event monitoring (**SIEM**) tool. With external log sources from Okta, Box, G Suite, Slack, Workday, Salesforce, and many more, we gain real-time, actionable insight into the massive amounts of data generated by our most critical business applications, all on one consolidated, performance-enhancing storage solution.

ACCELERATING PERFORMANCE AND FORTIFYING SECURITY

The most impactful benefit we've gained by deploying Splunk on our own hardware is **fast and consistent indexing and search performance**, even during data volume spikes or when many users search simultaneously. Leveraging Splunk on Pure has also allowed us to **enable all correlation searches** in Enterprise Security, rather than just picking and choosing a select few. Since we're utilizing Splunk as our single pane of glass for monitoring all of our security operations, these features are critical to fortifying Pure's defenses against potential security threats.

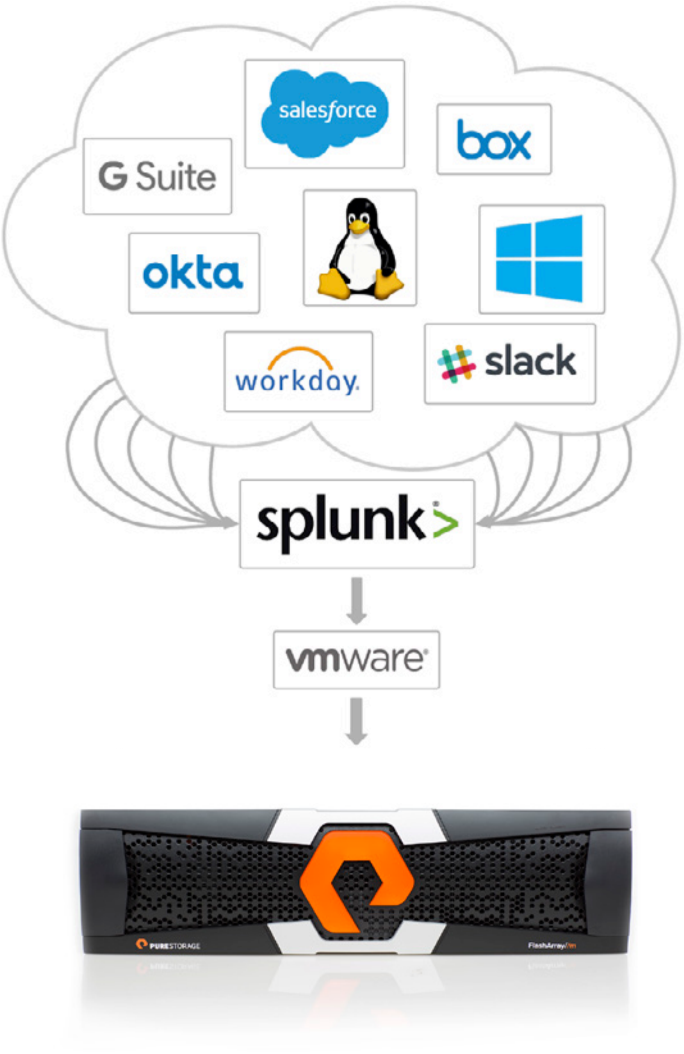
Splunk hammers storage with lots of random I/O, but Pure hardware provides reliable performance; our FlashArray maintains optimal performance even while handling **135 source types** including events from major cloud applications, performance metrics, vulnerability data, endpoint agent data, Windows and Linux servers, and firewall and network devices. With accelerated speed and enhanced performance, we've gained greater visibility into the security of our infrastructure without having to spend time logging into disparate systems. Moreover, the Splunk index cluster requires writing each piece of data twice to improve search performance and provide resiliency, but FlashArray handles the extra workload with ease. These enhanced correlated search capabilities provide our Security team with greater visibility across our enterprise and empower us to steadfastly defend our organization against security threats.

ENABLING UNMATCHED, SUSTAINABLE SCALE

Most importantly, our deployment of Splunk on Pure hardware is **scalable**. Unlike other storage arrays that suffer performance deficiencies when shared with other services, we currently have **Splunk**, **Tableau**, and **SQL services** all running on the same FlashArray with no negative impact to experience. Upgrading legacy storage arrays to meet the performance needs of Splunk can also require costly new hardware and system downtime, and the extra burden of performing data backups can cause potentially devastating failures. With Purity Assure, however, capacity and controller upgrades are non-disruptive so that the FlashArray always remains online. A one-size-fits-all storage solution, Pure hardware is capable of handling the large workloads that empower operational scalability.

We're currently indexing about 100 GB of data per day, but our array is fully capable of handling much more as Pure continues to scale. While Splunk on Pure has afforded our Security team enhanced visibility and monitoring capabilities, it's also enabling our Deployment team to onboard new hires more efficiently by processing data in Workday. Likewise, our System Administration team can leverage Splunk for application troubleshooting and resource monitoring in the near future, as will our Helpdesk team for performing root cause analysis (RCA). Beyond IT, other business units throughout Pure will eventually be able to leverage the power of Splunk on FlashArray to gather and analyze critical business metrics and experience the same impactful process improvements that we've gained in IT.

THE DATA FLOW


salesforce
G Suite
box
okta
workday.
slack
splunk>
vmware
PURESTORAGE
FlashArray//m