Splunk Solutions for COVID-19 Response

Navigating the Pandemic in Higher Education

March 2020
# Table of Contents

Introduction ........................................................................................................................................... 3  
Splunk COVID-19 Dashboard ...................................................................................................... 4  
Remote Work ......................................................................................................................................... 5  
Remote Monitoring and Collaboration .................................................................................. 7  
Distance Learning ............................................................................................................................... 8  
Cybersecurity ........................................................................................................................................ 8  
Orchestration, Automation and Response ......................................................................... 9  
Cloud Migration .................................................................................................................................... 9
Introduction

The global COVID-19 pandemic poses unprecedented public health challenges for the individual and organizations ranging from, but not limited to, schools and universities to local hospitals to government agencies. Academic medical centers, like other hospitals are getting overwhelmed and many are starting to spill into university dorms to house patients. At a time when urgent action is critical, Splunk stands in solidarity with all of our customers, particularly those on the front lines of care and response. Empowering these personnel to operationalize their data with tools and solutions, so they can make confident decisions and take decisive action at speeds the crisis warrants, is our primary mission.

While the world is working together to stop the spread, improve test and treatment outcomes and protect the most vulnerable populations, data serves as an invaluable resource. It will help implement measures to slow the virus’ spread, help maintain and provide essential infrastructure and services, all while encouraging us not to give in to panic and fear. This is why Splunk is helping organizations leverage their data during this crisis so they can respond in ways that can help them thwart the pandemic’s ill effects. In the past, Splunk has worked with various partners to lend a hand in times of disaster and our response to the COVID-19 situation builds upon that foundation.

The Splunk Data-to-Everything Platform enables educational institutions to gain real-time insights from their data. We aim to leverage our suite of tools in service of campus-critical applications in this challenging time. As a trusted provider of security, IT monitoring and learning and campus analytics, our solutions are ideally suited to aggregate disparate data from any source, regardless of structure, in real-time and at scale. Our solutions can help facilitate secure data access, protect privacy, maximize uptime of critical IT resources and promote sharing on a needs-only basis with full audit capabilities.

Splunk has already developed an interactive Splunk COVID-19 Dashboard with the express goal of helping to monitor and understand the pandemic as it evolves, while responding the best way possible to ensure public safety. We've also seen community-driven work from the likes of Leidos, Prudential, Herc Rentals, and Accenture. Beginning with these public resources, our partners and customers can develop additional interactive dashboards customized to particular needs and situations. Their focus will be to analyze the data, correlate it with subject matter expertise on infectious diseases, and serve as a catalyst for additional interesting research, ideas, and suggestions.

Beyond this analysis and visualization of COVID-19 data, Splunk stands ready to continue our partnership with government agencies and assist them directly with relevant use cases -- telework (remote work), distance learning, cloud migration, orchestration & automation, cybersecurity, troubleshooting and collaboration. Large teams of teleworkers can add tremendous pressure to both IT and Security teams, and not to mention the infrastructure they support. Splunk has curated a list of solutions that can help facilitate this essential shift to telework (remote work) we are witnessing. These packages are easy to install and many are free to run for existing Splunk customers.

Technology plays a critical role in keeping essential services functioning and delivering assistance where and when needed, and Splunk is committed to helping in this effort. Splunk has curated some short term solutions to help organizations overcome current challenges while offering its traditional suite of solutions to ensure strategic advantage.
Splunk COVID-19 Dashboard

Splunk launched a new dashboard which utilizes publicly available data from Johns Hopkins University to track the global spread of COVID-19. In parallel, we released an app to engage our customer and user community so they can add their own data, and use it to help get a better understanding of the data behind the pandemic. Consistent and reliable data need not be elusive but can be difficult to identify and harness. However, given our decades of experience in delivering data-driven solutions to customers worldwide, we can help identify, ingest and correlate the relevant data quickly and deliver compelling visualizations through customizable dashboards.

Provided below are examples of dashboards developed by the Leidos Healthcare team using Splunk. These dashboards have been created with Johns Hopkins University data. All dashboards can be customized or augmented to ingest agency specific data sources.

COVID-19: Global Metrics w/ map; US & Worldwide Confirmed, Active, Recoveries, and Deaths

COVID-19: Location Specific Metrics w/ nearest point of interest, including heatmap and location maps depicting outbreak clusters
Remote Work

While the concept of remote work is certainly not new, the magnitude of demand for remote work has increased dramatically, due to the evolving pandemic. As organizations scale out and shift to remote work, there will likely be rapid increases in network, remote access and collaboration software. To help organizations navigate the current situation, Splunk has created actionable guidance and a curated list of purpose-built solutions for Splunk customers to assist with this new operational model. This information can be found on our COVID-19 Response website. With more and more endpoints accessing your network remotely, you should expect rapid increases in VPN connections and usage. Furthermore, social streaming, distance learning and other extracurricular activities can bog down your network and slow down responses.
Since VPN is a popular remote working capability, Splunk has partnered with industry leading VPN technologies (such as Cisco, Palo Alto, Fortinet and others) to enable deep endpoint visibility and operational monitoring. Most organizations want to know what their faculty, students, staff and their devices are doing when they are at work or connected through university networks, on the road or working from the coffee shop. Splunk’s strategic partners have created tools to analyze endpoint data and present it through a customized monitoring and alert console. This enables customers to quickly understand user experience, endpoint behaviors and answer critical security and operational questions using infrastructure and endpoint data when they are on or off the network.

The example VPN dashboard below highlights geolocation of connected devices, successful and failed logins, and enumerates users utilizing VPN over time.
Server and endpoint data ingested and analyzed in Splunk addresses VPN use cases such as:

**Client Session Status and Statistics**
- How many clients are connected and are their sessions efficient?
- Improved mean time to resolution of VPN service issues

**VPN Infrastructure Monitoring**
- Resource monitoring to analyze and monitor load on VPN infrastructure
- Understand impact to network by monitoring traffic

**Data loss detection**
- Data hoarding activity—download and upload behavior
- Exfiltration—upload to external domains and network shares

**Day-zero malware and threat hunting**
- Unusual app/process behavior—running at root or on nonstandard ports
- Command and Control detection—burst of connections to new, unusual, or bad domain
- Threat detection—application process to host domain correlation

**Zero-trust monitoring**
- Off-net device monitoring—user, device, traffic, app, and data behavior
- SaaS use behavior—track SaaS services are being used
- Untrusted connections—track who is connecting to untrusted networks

**Unapproved applications and SaaS visibility**
- SaaS domains accessed - connections and SaaS use behavior
- Application and process visibility—find apps and processes running on devices

**Security evasion and user attribution**
- Endpoint security applications—detect if disabled or not installed
- CESA—detect if disabled or not installed
- Attribute user to network access—user activity down to network interface controller level

**Asset inventory**
- Device-type and OS inventory—identify and report by type
- Data privacy compliance—confirm removal of personal data from devices

**Remote Monitoring and Collaboration**
As every individual and institution is faced with shifting to remote work and distance learning as the only options, networks face increased stress. As faculty and staff turn to teleworking and students log in to classes remotely, secure and highly available access is critical. For organizations that need immediate assistance, Splunk has introduced a customized version of our Splunk Cloud Autobahn program, called the Remote Work Insights (RWI) Autobahn, that can help universities onboard a set of key data sources for use with Splunk Cloud and gain quick, actionable insights. Using the RWI Autobahn, you can monitor key performance indicators, identify emerging issues, and perform deep root cause analysis, all in one platform. Additional information on the resources available with Remote Work Insights, including apps and add-ons for on-premises Splunk installations as well as how to get started, is available on our COVID-19 response website. This website will be updated as additional use cases and data sources are added in the future.
Another key question to address is what can institutions do to better facilitate personnel productivity and in a remote environment? Collaboration tools are essential for productivity at any time, and not just for the admissions officer or the professor, but also help desk and support personnel. When all infrastructure is geared towards delivery of institutional critical services, it is important to ensure that systems can be recovered quickly in the case of any outage, interruption or even a cyber-attack. While monitoring tools can alert personnel, efficient collaboration can accelerate decisive actions.

As your teams scale up your systems to accommodate remote work and distance learning, Splunk is here to help. Our collaboration solution, VictorOps, seamlessly integrates with Splunk Enterprise or Splunk Cloud to automate incident management reducing alert fatigue and increasing uptime. It empowers teams by routing alerts to the right people for fast collaboration and issue resolution. It streamlines on-call schedules and escalation policies to ensure efficient routing and handling of issues. By providing contextual alert information and suggestions driven from machine learning it empowers collaboration to solve problems with speed and efficiency, all while capturing essential remediation data. With native iOS and Android apps, the right person can receive metadata-rich notifications directly to any device.

**Distance Learning**

As schools and universities take proactive action to ensure their students, faculty and staff stay healthy, they have required them to work from home and take/conduct classes from home. And this has significantly increased the need for online video conferencing tools like Zoom. This could pose a significant challenge to IT teams since they not only have to ensure the best student experience across multiple online class rooms and all the students, but also support those who are embarking on this online learning journey for the first time.

Layering Splunk IT Service Intelligence (ITSI) onto the solution stack enables monitoring, analytics and AI capabilities to provide insight across infrastructure, business services, and applications. Correlating logs, metrics, and change-management data between multiple silos enable institutions to comprehend complex interdependencies and display near real-time service health scores for critical solutions, such as remote worker VPN access. Using built-in machine learning features of ITSI to detect anomalies allows system administrators to predict outages before they occur and move to root-cause analysis before an outage affects system up-time.

**Cybersecurity**

Nefarious actors, ever looking for and who thrive on uncertain situations, are increasingly targeting and attacking agencies and our critical infrastructure. And remote work options only expand the attack surface and endpoint monitoring is even more critical now than ever.

The Cybersecurity and Infrastructure Security Agency (CISA), under the Department of Homeland Security (DHS), has published insights into Risk Management for the Novel Coronavirus for executives to think through physical, supply chain and cybersecurity issues that may arise during the pandemic. For organizations racing to manage and ensure secure connectivity via their VPNs, CISA has issued a set of VPN guidelines to help manage bottlenecks they might run into. Splunk can help quickly streamline your organization's security posture, mitigating risk and exposing hidden security and operational gaps that can make systems vulnerable to data breaches and regulatory noncompliance. It automates security monitoring, threat detection and anomaly detection using machine learning so scarce security resources can spend more time analyzing higher fidelity behavior-based alerts for quick resolution.

Account compromise, in particular, becomes more relevant as the risk for the exposure of your employees' endpoints increases due to factors outside your control — i.e. users connecting via a public Wi-Fi hotspot or have no security applied on their home router making them more vulnerable to attacks. Splunk Security Essentials (SSE) is a free app that aims at making security simpler and allows you to validate data sources, capabilities, test and implement detections mapped to cybersecurity frameworks like MITRE ATT&CK and many more.
While there are plenty of unknowns, it's also a great opportunity to focus on the basics; the must-do things for security maturity. To that end, there's no better place to start than with a strong cybersecurity policy. Splunk can help organizations improve their cybersecurity policies by maturing security operations across the entire event lifecycle. Our robust network of partners via the Adaptive Operations Framework integrates with leading cybersecurity players so that customers can drive advanced threat detection and mitigation. The best practices you apply today can extend and enhance your security posture into the future.

**Orchestration, Automation & Response**

People are an important part of delivering an institution's mission but most organization's, if not all, are short of them. **Phantom**, Splunk's orchestration and automation platform, is built to make automation easy, intuitive and effective, taking care of mundane and repetitive work, so scarce resources can spend their time on more important tasks.

Phantom is typically used in security or operational centers to overcome challenges of volume, response time, repeatability, and expertise. A significant challenge posed by COVID-19 is reduced staffing as employees may be unable to work from the office, dealing with additional childcare responsibilities, or unable to work at all. As alert volumes increase and staffing decreases, SOCs and NOCs face volume-related challenges, as well as expertise issues while critical staff are taken away from their desks. Automation provides technology teams the capability to eliminate significant workload backlogs, allowing them to get through more and focus on tasks truly requiring human attention.

A major benefit of leveraging automated responses, called Playbooks in Phantom, is that they can be built to follow the same process as expert users even when run by junior ones. This can greatly improve the effective skill level of a team while reducing pressure on overburdened senior staff. This frees up personnel, drastically reduces response time, improves consistency and ensures 24/7 responsiveness. When permissible, Phantom enables teams to respond through mobile devices, as well.

**Cloud Migration**

With most institutions still reliant on legacy applications, which were not built with remote access in mind, people have to be at their workstations hardwired by technologies to access them. For remote work, VPN technologies provide secure access to applications and work well under normal circumstances. But given the magnitude of telework in the current situation, where almost all students, faculty and staff need remote access, VPN access can be a bottleneck. Cloud solutions offer a distinct advantage to traditional on-premise architecture by allowing scalability on-demand.

The cloud environment, on the other hand, is purpose-built to endorse flexibility and deliver secure access. Security issues are inherently addressed when the cloud service is FedRAMP authorized. **Splunk Cloud** is FedRAMP authorized, satisfying most agencies’ risk management requirements.

As organizations migrate to cloud and hybrid locales, end-to-end operational visibility is essential before, during and after the transition to maintain insights into performance and address concerns related to infrastructure and application visibility. It also eliminates finger pointing when SLAs are missed and when IT’s reputation is on the line.

What does operational visibility look like in a cloud/hybrid environment? It's an end-to-end view of infrastructure and application performance across workloads and microservices, wherever they reside. It provides the intelligence needed to monitor and measure KPIs to ensure a compelling user/constituent experience when infrastructure spans public and private cloud and on-premises domains.
Additionally, by monitoring usage of various components that make up applications or systems, IT can have the confidence to rationalize applications and migrate only the components that are necessary, thus eliminating extraneous ones and saving costs.

- **BEFORE** a cloud migration, it’s important to measure the baseline user experience and performance, as well as define acceptable post-migration levels. Degradation in one performance area may be tolerated if it’s balanced or offset by gains in another. To accurately validate a migration’s success, the same monitoring tool should be used throughout the migration process.

- **DURING** a cloud migration, established performance metrics should be closely monitored. Variation from the baseline is an early indicator of trouble. A monitoring solution’s dashboard and alerts will quickly identify these issues well before production and save time and resources. A performance issue is better identified during a migration when it’s easier to pause and make corrections.

- **AFTER** a cloud migration, the same monitoring solution should be used to measure acceptable metrics and determine success. The continued use of monitoring solutions and dashboards, well after the switchover, is essential to ensure successful customer journeys, crossing on-premises and public cloud workloads.

Splunk can help educational institutions achieve objective, data-driven insights; for example, modeling and predicting how initiatives will play out in order to deliver on intended outcomes. In addition to helping monitor migrations during all phases to improve probability of success, granular, real-time monitoring capability can help avoid budget overruns caused by excess resource consumption, unexpected expenses, and inaccurate billing. Armed with data-driven insights, organizations can quickly make confident decisions and take action. For institutions that are involved in government-sponsored research or receive grants, Splunk Cloud meets FedRAMP risk management and security requirements, enabling proactive risk management from the start.

As COVID-19 continues to impact the global community, Splunk is focused on supporting our stakeholders and ecosystem — including you, our customers — through a time of great uncertainty. We have taken steps to help ensure our customers around the world can continue to rely on Splunk products and services to turn their data into meaningful outcomes. We know how critical our platform is to our customers’ operations and we are committed to ensuring you are able to fulfill your organization’s mission.

Thousands of public and private sector enterprises rely on Splunk to improve security, increase efficiencies, make data-driven decisions and gain tactical and strategic advantages. Whether cloud, on-premises or for large or small teams, Splunk has a deployment model that will fit your needs.

Learn more. Or [Contact a Splunk Expert](https://www.splunk.com) to discuss your environment and assess your requirements and how we can help you navigate these challenging times.