Splunk Solutions for COVID-19 Response

Navigating the Pandemic in Government

May 2020
Table of Contents

Introduction ............................................................................................................................................ 3

Increasing Situation Awareness ................................................................................................ 4
COVID-19 Dashboard .......................................................................................................................... 4
VPN Dashboard .................................................................................................................................. 6

Enabling Remote Working ............................................................................................................. 8
Remote Working Insights (RWI) ............................................................................................................. 8
ITSI ..................................................................................................................................................... 8
VictorOps .......................................................................................................................................... 8

Mitigating Cyber threats .................................................................................................................. 9
The threat .......................................................................................................................................... 9
Splunk Security Essentials (SSE) ..................................................................................................... 9
Phantom ........................................................................................................................................... 9

Scalability and Flexibility ................................................................................................................. 10
Splunk Cloud ................................................................................................................................... 10

Conclusion ...................................................................................................................................... 10
Introduction

The global COVID-19 pandemic poses unprecedented public health challenges for the individual and organisations ranging from, but not limited to, schools to local hospitals, local authorities, and central government. At a time when urgent action is critical, Splunk stands together with our customers, particularly those on the front lines of care and response. Empowering these personnel to operationalise 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 helps implement measures to slow the virus’ spread, 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 organisations leverage their data during this crisis so they can respond in ways that can help them thwart the pandemic’s 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.

To help organisations navigate the current situation easier, Splunk has created insights, 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. Some of these solutions are no cost or free to use on an existing Splunk platform. Others are commercial offerings.

In the following document we have shown how Splunk can support challenges you may be facing in the following areas:

- Increasing Situation Awareness
- Enabling Remote Working
- Mitigating Cyber threats
- Scalability and Flexibility

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

It is critical that government organisations keep ahead of developments with COVID-19 and are monitoring the global and local situation closely. Government entities need to provide critical information to their citizens and partners and also need to monitor internal service provision efficiently.

Splunk COVID-19 Dashboard

In March, Splunk launched a new dashboard which uses publicly available data to help track the global spread of COVID-19. In parallel, we released an app to engage our customer and user community so they can populate it with 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 plus experience in delivering data-driven solutions to customers worldwide, we can help identify, ingest, and correlate the relevant data quickly and deliver compelling visualisations through customisable dashboards.

Provided below are examples of dashboards developed by Splunk itself and the Leidos Healthcare team using Splunk. These dashboards have been created with Johns Hopkins University data or data from the UK Government. All dashboards can be customised or augmented to ingest specific data sources and correlate the relevant data quickly and deliver compelling visualizations through customizable dashboards.
COVID-19: Pandemic Specific Information to include critical drug supply, testing kit availability, co-morbidity risk factor counts, doctor attrition, rates, and available beds

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

COVID-19: Clinical Resource Management with percentage of increase in new cases by State and VISN
VPN Dashboard

While the concept of remote working is certainly not new, due to the evolving pandemic, the magnitude of demand for remote work has increased dramatically.

Most governments across Europe have now implemented remote working practices at all levels from local / state government to central government. The EU institutions have been fully utilising remote collaboration technologies and other political institutions like the Houses of Parliament are using teleconferencing facilities for committee hearings.

As organisations scale out and shift to remote work, there has been rapid increases in network, remote access, and collaboration software. With increased endpoints accessing your network remotely, you should expect rapid increases in VPN connections and usage. Furthermore, social streaming 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 organisations want to allow their employees to work effectively remotely and are being provided with the tools necessary to do their job. Splunk’s strategic partners have created tools to analyse endpoint data and present it through a customised monitoring and alert console. This enables customers to quickly understand user experience, endpoint behaviours 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 analysed 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 analyse and monitor load on VPN infrastructure
- Understand impact to network by monitoring traffic

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

**Day-zero malware and threat hunting**
- Unusual app/process behaviour—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 behaviour
- SaaS use behaviour—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 behaviour
- 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
Enabling Remote Working

As individuals and organisations shift to remote working, networks are facing increased congestion and demand. As public sector workers turn to remote working, access to secure collaboration tools is critical so government entities can continue to deliver citizen services.

Remote Working Insights (RWI)

For organisations that need immediate assistance, Splunk has introduced a customised version of our Splunk Cloud Autobahn program, called the Remote Work Insights (RWI) Autobahn, that can help agencies onboard a set of key data sources for use with Splunk Cloud and gain quick, actionable insights. This programme offers qualified customers a free Proof of Value that provides a prescriptive approach to delivering proactive visibility and reducing time to issue resolution within your organisation. With remote work monitoring from Splunk, 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 page. This page will be updated as additional use cases and data sources are added in the future.

ITSI

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 agencies 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.

VictorOps

Another key question to address is what can government entities do to better facilitate personnel productivity in a remote environment? Collaboration tools are essential for productivity at any time, and not just for the knowledge worker or the case manager, but also helpdesk and support personnel. When all infrastructure is geared towards delivery of mission-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, 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.
Mitigating Cyber threats

The threat
Malicious actors, who thrive on uncertain situations, are increasingly targeting and attacking government organisations and our critical infrastructure. Since the outbreak of the crisis, cyber-attacks have even targeted health organisations, such as Paris hospitals or the Dutch Institute for Public Health. Remote work options only expand the attack surface and endpoint monitoring is even more critical now than ever.

The UK National Cyber Security Centre (NCSC) has published advice for organisations to reduce the risk of cyber-attack on deployed devices including laptops, mobiles and tablets, and tips to help staff spot typical signs of phishing scams. The NCSC has outlined recommended steps for organisations in preparing for home working, setting up new accounts and accesses, controlling access to corporate systems, helping staff to look after devices and reducing the risk from removable media. The European Cybersecurity Agency (ENISA) published similar advice for companies switching to remote-working. In Germany, the Federal Office for Information Security (BSI) also produced guidance to manage cyber risks at times of coronavirus.

For all UK entities racing to manage and ensure secure remote working, the NCSC had issued a COVID-19 advisory. Splunk can help quickly streamline your organisation’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 analysing higher fidelity behaviour-based alerts for quick resolution.

Splunk Security Essentials (SSE)
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 have no security applied on their home router making them more vulnerable to attacks. Splunk Security Essentials (SSE) is a free application 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.

Splunk can also help organisations 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.

Phantom
Splunk 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 joint-operational command centres 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.
Scalability and Flexibility

Governments are providing critical services to citizens across Europe. In these challenging times they may be doing this with reduced resources and huge demands on their IT infrastructure.

Splunk Cloud

With most agencies still reliant on legacy, on-premise applications, which were not built with remote access in mind, government personnel 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 virtual working in the current situation, where almost all workers 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 and are purpose-built to endorse flexibility and deliver secure access.

As government bodies 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 the IT team’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, the IT team can have the confidence to rationalise applications and migrate only the components that are necessary, thus eliminating irrelevant ones and saving costs.

Splunk can help government entities achieve objective, data-driven insights; for example, modelling and predicting how initiatives will develop 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, agencies can quickly make confident decisions and take action.

small teams, Splunk has a deployment model that will fit your needs.

Conclusion

As COVID-19 continues to impact the global community, Splunk is focused on supporting our stakeholders and ecosystem through a time of prolonged 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 fulfil your organisation’s outcomes.

If you wish to discuss the content of this paper further please use the following contact:
Phone: +44 0.20.3204.4300   Email: Contact our EMEA Sales team

www.splunk.com