Mastering remote insights with Splunk: A bitsIO guide

Table of Contents

Introduction

Considering the contemporary workforce landscape, remote working is ubiquitous. Ensuring a secure work-from-home infrastructure is paramount. Irrespective of the industry, most organizations are responsible for providing an optimum, robust infrastructure that safeguards data as well as operations. Splunk emerges as an integral and invaluable ally, ensuring enhanced security through multifaceted support.

Splunk's Remote Work Insights (RWI) application serves as an anchor when it comes to fortifying the security fabric of the remote work infrastructure. Data from various sources are monitored and analysed by Splunk, which enables the organizations to identify and respond to potential security threats promptly. These real-time insights enable organizations to proactively implement
measures, preventing the exploitation of vulnerabilities.

Additionally, Splunk enables the tracking of user activities, which ensures that access is only granted to the concerned authorized personnel. The reports and dashboard of the application provide a coherent overview of the network security highlighting anomalies and suspicious activities. These are the capabilities that enhance the defence system of the organization and inculcate confidence in employees working remotely, knowing that their digital workspace is safe.

Splunk has ability to integrate with various security solutions, which further amplifies its efficacy. It consolidates data from diverse security tools, providing a unified comprehensive analysis. This aids in streamlining security operations and increases the ability to detect potential threats and eradicate them promptly.

In addition to this, the user interface of Splunk is mobile friendly. This ensures that security monitoring is not hindered by location. The flexibility acts as an instrument in terms of upholding security standards irrespective of where the employees are working from.

Splunk is seminal when it comes to establishing and securing work-from-home infrastructures. Cutting-edge analytics and real-time monitoring of Splunk enable organizations to navigate through emerging threats with promptness and confidence, ensuring streamlined operations without compromising on security.

We shall further understand and evaluate Splunk based on its context and utility.

Is the Remote Work Infrastructure post Covid-19, really secured?

Is the remote work infrastructure post Covid-19, really secured?

Evaluating the context

Considering the pre-pandemic landscape, only 7.9% of the world's population worked from home. During the pandemic, over 50% of the population around the world was working remotely. This was a move that allowed the businesses to continue with their business operations during the most unusual times.

In the contemporary landscape, work-from-home and hybrid infrastructure has become the new normal. Around 16% of the companies across the globe are operating on a completely remote infrastructure.

Contemporary technologies allow companies to operate in a way that was not possible in the past. Modern technology allows instant transfer of files and conference calls over Zoom, but it also faces a host of security threats. They come in various forms and have the potential to rob your company's time, data, and money.

Security threats are on the rise: Here's why?

The ability to work-from-home creates a considerable number of opportunities as well as challenges. There is a plethora of evidence that suggests that malicious actors are, in disturbingly large numbers, using the shifting work environment to hack and breach systems.

Implementing a work from home policy requires that company leaders become aware of the increased risk for security breaches as well as the need for additional monitoring of the online environment. According to Security Magazine, that includes being aware of the danger of insider threats, in which "a malicious insider utilizes credentials to gain access to a given organization's critical assets. This is especially true with COVID-19 and employees who are currently working from home."

Employees who are upset about changes such as fewer hours, reduced compensation, lost promotions, and more could react maliciously in these new working arrangements. Such anger or resentment can lead them to leak information or steal intellectual property. And if security controls to monitor and detect such activity aren't as robust as in the more traditional on-site environment, it could make it easier for such threats to be successfully deployed.

Another growing concern has been the proliferation of COVID-19 phishing scams, which are rising at an alarming rate. During a single week in April 2020, Google reported more than 18 million daily malware and phishing emails related to COVID-19 scams. These scams would impersonate government organizations (such as the World Health Organization) and may try to trick users into downloading malware. Others may claim to have information about government stimulus payments, and, in some cases, the phishers pretend to be the remote worker's employers.

Although, we are currently in the post-pandemic landscape, phishing and scam has been an increasing phenomenon.

Unintended threats can be equally dangerous

A noteworthy aspect is that not all security issues come because of malicious intent. However, they can still have damaging consequences. With more employees operating remotely, it is likely that more apps will be downloaded and installed at their endpoints, which can activate malicious behaviour in the infrastructure without the knowledge of the concerned employee.

An employee may download sensitive information to a USB device in order to enable an easy access without any harmful intention, A vulnerable home network, which is significantly more prone to compromise and infection, can unknowingly introduce threats to the company infrastructure.

This creates concerns for all companies that have had to pivot to a work from home policy almost overnight. Even for companies that already allowed a certain amount of remote work, the sudden increase in the number of employees accessing the company network remotely could be placing their infrastructure at risk. That's particularly true if the organization has been unable to vet all devices being used.

Two of the most effective ways we can help safeguard your company immediately are:

Splunk Security Essentials:
This free app makes security simple. It provides you with the useful information you need, when you need it, with detections that include line-by-line SPL documentation. Each detection also includes context such as security impact, how to implement it, how to respond when it fires, and known false positives.

Splunk Enterprise Security:
This powerful, analytics-driven solution allows you to detect and respond to threats quickly. It's ideal for the financial services, public sector, and healthcare industry and allows you to gather all the context needed in one view to facilitate rapid investigations.

Even in the best of situations, having a large number of remote workers can create challenges for the IT department, your security team, and your entire infrastructure. With Splunk, bitsIO can help you:

- Manage your infrastructure as it adapts to the changing needs of your remote environment.
- Secure your endpoints and monitor your VPN's security by tracking connections, identifying abnormal behaviour, and improving the mean time to resolve service issues.
- Prevent data loss and leakage by monitoring data hoarding, exfiltration, and unauthorized USB device activity.
- Identify and respond to potential phishing content.

The primary endeavour of our venture is to ensure that networks and endpoints stay secured from the increasing number of threats. Educating remote employees to implement safe practices and identify threats is not enough. Understanding where the threats come from, obtaining actionable insights, will allow prevention and action.

With the due progression of time and advancement in technology, the threats will increase. Therefore, this is high time when this factor is taken into consideration. Companies bear two major responsibilities, one is to establish a secure work-from-home infrastructure, and second, is to instil confidence in the employees.

The entire effort is to create a digital landscape that is safe which enhances both trust and productivity.

Monitoring Employees Working from Home

Monitoring Employees Working from Home

Previously, we evaluated the requirement of a secured work-from-home infrastructure. In this section, we are going to evaluate the aspects of operation and supervision.

While the traditional office setup provides easy ways to supervise employees, ensuring productivity while respecting privacy in a work-from-home environment presents unique obstacles. Statistics shared by The Home Office in the year 2020 showed there had been an increase of 47% in productivity when the employees are working from home. Whereas the preferred option for employees has been working from home constituting 82% of them.

As stated earlier, this infrastructure had opened up several new horizons and introduced several challenges.

Why is tracking remote employees important?

Let us reflect on some of the crucial factors that highlight the importance of monitoring remote employees.

1. Productivity Tracking

Monitoring employees working from home is essential to track their productivity levels and ensure that work is being completed efficiently and within deadlines.

By implementing productivity tracking tools, employers can gain insights into the amount of time spent on tasks, identify potential bottlenecks, and optimize workflow processes.

This monitoring helps maintain overall team performance and ensures organizational goals are met.

2. Data Security and Confidentiality

With employees accessing sensitive company information from remote locations, monitoring becomes crucial to address data security and confidentiality concerns.

Employers need to implement measures to safeguard data and prevent unauthorized access or breaches.

Monitoring allows organizations to detect any suspicious activities, ensure compliance with data protection regulations, and take timely action to mitigate risks.

3. Workforce Coordination and Collaboration

Effective monitoring promotes coordination and collaboration within remote teams.

By having visibility into employees' work activities, employers can identify potential bottlenecks, allocate resources accordingly, and provide timely support.

Monitoring tools enable real-time communication, task management, and progress tracking, enhancing collaboration and facilitating seamless teamwork.

4. Performance Evaluation and Feedback

Monitoring employees working from home provides a basis for performance evaluation and feedback.

By tracking and measuring individual and team performance, employers can assess productivity levels, identify areas for improvement, and provide constructive feedback.

Regular performance evaluations can help align individual goals with organizational objectives and foster continuous growth and development.

5. Compliance and Regulatory Requirements

Monitoring remote employees is crucial to ensure compliance with regulatory requirements and company policies.

Certain industries have specific regulations that mandate monitoring practices to protect sensitive information and prevent fraudulent activities.

By implementing appropriate monitoring measures, organizations can demonstrate compliance, mitigate legal risks, and maintain the trust of clients and stakeholders.

6. Employee Engagement and Well-being

Monitoring can also contribute to employee engagement and well-being in a remote work environment.

Regular check-ins and communication foster a sense of belonging and support among remote employees.

Monitoring tools can help identify signs of burnout or excessive workload, allowing employers to address these issues and promote a healthy work-life balance.

Risks of a WFH Workforce

As employees turned kitchen tables into workspaces at an unprecedented pace, they began using home equipment to complete tasks that had previously been done in the office environment.

That means that unmanaged routers and printers on home ISPs began replacing the secure office network, creating an environment that seemed ready-made for security breaches.

The increased use of virtual private networks, or VPNs, saw encrypted networks being extended to employees' homes. While the VPN may have been safe, many home networks are already infected with malware that could be used to stage an attack.

The security of the hardware being used may be compromised, which then allows hackers to gain access to the VPN. Businesses that have had to quickly adapt to a remote workforce have many endpoint challenges to address because so many vulnerabilities have been introduced.

In addition to VPN challenges, mobile options present a significant vulnerability. Many workers now find themselves completing certain tasks via mobile, and it's no surprise that it didn't take long for hackers to recognize the opportunity and access workers' phones.

For example, hackers created a malicious mobile app that looked like a legitimate app developed by the World Health Organization. Once downloaded, however, the application was designed to steal sensitive data, including personal, financial, and business information.

How do we monitor employees working from home?

Monitoring remote employees is seminal for enhancing productivity and ensuring a collaborative environment. The current landscape is highly dynamic, and work-from-home infrastructure will remain prevalent. Organizations that support remote infrastructure are entrusted with the task of tracking progress, ensuring task completion, and fostering communication.

Therefore, the monitoring of remote employees should be done with enhanced efficacy. Let's look at three tools bitsIO can employ to monitor critical services and help keep your network and all your employees' information safer.

1. Multifactor Authentication

Multifactor authentication, or MFA, requires two or more pieces of information to authenticate the user's identity before granting them access.

It plays a key role in maintaining safety, particularly in a remote environment where an unauthorized user may have access to equipment. Having MFA in place is a critical way to keep your IT environment safe, and bitsIO has two Splunk features to accomplish this.

Splunk Add-on for RSA Multifactor Authentication. With this add-on, a Splunk software administrator can collect data from the RSA SecurID Authentication Manager server. Once the platform has indexed all the events, simply use the pre-built dashboard panels to review the data.

Duo Splunk Connector. Administrators can import all the critical logs to view and monitor activity. This includes authentication logs, administrator logs, telephony logs, and endpoint logs. New dashboards can also be created and modified to support necessary data.

2. Remote Access VPN

With more users connecting simultaneously to the corporate internet, it's critical to be able to monitor activity and troubleshoot instances where users cannot connect.

Three Splunk options for doing that are:

Palo Alto Add-on. This add-on pulls data from the user's firewall and provides advanced endpoint security. It also allows reporting on key links and has a GlobalProtect VPN feature to help with troubleshooting remote access situations.

Zscaler App. This application is designed to provide visibility and dashboards into remote access on all Zscaler products, regardless of the user's location. It has focused dashboards for insights such as threat intelligence, web usage, remote access usage, and more.

Cisco App. Similar in functionality to the two above apps, this helps map Cisco ASA device access to the Splunk environment.

3. Access Management

Access management uses a variety of processes and technologies to control and monitor access to the network. Splunk offers these add-ons to help troubleshoot issues with services such as single sign-on (SSO) capabilities or redirects.

Okta Add-on. This allows an administrator to collect data related to event log information, user information, application and application assignment information, and group membership information.

SailPoint Add-on. Easily extract audit event data from Sailpoint's IdentityNow product.

Best Practices for Monitoring Remote Employees

To monitor remote employees effectively, it is important to establish practices that foster productivity, accountability, and employee well-being. Here are some practical tips and guidelines to consider:

Setting Clear Expectations and Goals:

- Clearly communicate expectations regarding work hours, availability, and deliverables.
- Set specific goals and objectives for individual employees and teams.
- Ensure that employees understand what is expected of them and how their performance will be evaluated.

Establishing Regular Check-Ins and Communication Channels:

- Schedule regular check-in meetings to discuss progress, challenges, and provide feedback.
- Utilize video conferencing, instant messaging, or project management platforms for effective communication.
- Encourage open dialogue and create a supportive environment where employees can share concerns or ask for help.

Encouraging Self-Reporting and Transparency:

- Encourage employees to proactively report their progress, complete tasks, and any obstacles they may be facing.
- Implement reporting mechanisms such as daily or weekly status updates to track work activities.
- Foster a culture of transparency, where employees feel comfortable sharing their achievements and challenges.

Balancing Trust and Accountability:

- Trust your employees to complete their work and meet expectations.
- Focus on outcomes and results rather than micromanaging their every move.
- However, ensure that employees are held accountable for their responsibilities and meet agreed-upon deadlines.

Respecting Privacy and Data Protection Laws:

- Respect employees' privacy while monitoring their work activities.
- Clearly communicate the extent and purpose of monitoring to employees. Comply with data protection laws and regulations to safeguard employee data and confidential information.

Promoting Employee Well-being and Work-Life Balance:

- Recognize the importance of work-life balance for remote employees.
- Encourage regular breaks and time for self-care.
- Promote employee well-being by providing resources for mental health support, promoting healthy work habits, and fostering a positive work culture.
- By implementing these best practices, you can establish a monitoring framework that promotes productivity, accountability, and employee satisfaction in remote work environments.

What is Splunk?

With the context of Spunk's requirement, we would now move on to scrutinize what Splunk actually is.

As more data is generated in every industry and organization, it creates a tremendous opportunity for businesses to understand their customers better and, in turn, provide better service to them. But this wealth of data also has a downside that most business leaders are painfully aware of: While amassing data has become easier, analysing and understanding it has become more complex.

All that data must be sorted and searched to find the right information, which has typically been a slow and painstaking process. When there is a considerable amount of data, sometimes it is hard to identify from where to exactly begin.

That is where Splunk comes in. To put it as simply as possible, Splunk is a software platform that was created to help make sense of machine-generated log data. It is primarily used for searching and monitoring machine-generated large data using a web-style interface. Once it discovers the requested data, Splunk uses its algorithms to assemble that information and provide companies with operational intelligence.

Operational intelligence zeroes in on recurring business processes and events and looks for ways to improve them. It could be considered the analytics side of business intelligence, and it is a key component for industries ranging from financial services to logistics and beyond. But operational intelligence relies on urgent, accurate, real-time intelligence that can be acted on immediately.

Such immediacy was not always possible in the past. However, Splunk provides users with that instant search and analysis that equips companies with an informed competitive edge. Being able to analyse the data and not just collect it is a critical step because the solution to different problems is hidden in machine data. The Splunk technology, which was developed in 2003 and launched a year later, is scalable and versatile, making it easy to capture, index, and correlate real-time data.

In addition to helping better understand how customers are behaving, the insights gathered by Splunk can show where businesses might be falling short and what areas they need to improve. This leads to the opportunity to provide better service, create happier customers, and ultimately boost your organization's bottom line.

How does Splunk function?

One way to understand Splunk is to think of it as 'Google for log files.' Today, data for companies is generated by a growing number of sources, including sensors, network devices, mobile phones, the Internet of Things (IoT), and more. But there are challenges to the massive influx of data, particularly:

1. It is complex to understand
2. It is not in a structured format.
3. It is difficult to analyze

Splunk was designed to resolve these three challenges by aggregating the data, analyzing it, and then storing it. One of its biggest advantages is that since it stores the data directly, it doesn't require a backend or database. Instead, it uses its indexes to store the data.

Within a designated searchable container, Splunk will capture, index, and correlate the data. Then, it presents the outcomes in an easily digestible format. This can include graphs, reports, alerts, dashboards, and visualizations. Splunk can use that machine-generated data to recognize data patterns, produce metrics, diagnose problems, and as previously mentioned, present intelligence that can instantly be applied to business operations. It also helps the user detect which configurations are being utilized within the log files, something that is typically a challenge for users.

Is Splunk right for your business model?

Around the world, more organizations are relying on Splunk; this includes finance and insurance, information technology, retail, trade, and more. Users have come to depend on it for their business needs, fraud prevention, service performance improvement, overall cost reduction, customer insight, and cybersecurity.

Splunk's popularity has grown because its instant access improves productivity and can be applied in several ways. It also has a rich developer environment that allows you to build Splunk apps quickly with help from approved web languages and frameworks.

If you are dealing with big data, Splunk can help navigate that information quickly and easily. And, as the landscape of Big Data continues evolving, so are Splunk's capabilities, meaning it can help you stay up to date and up to speed today as well as in the future.

Which Applications 'Ship with Splunk Enterprise'?

Splunk Enterprise is a powerful platform that allows organizations to gain insights from their machine-generated data.

It provides a range of applications that cater to different aspects of data management, analysis, and visualization.

That, in turn, allows for better insights into business operations and customer behaviour, enabling leaders to see where improvements could be made or where efforts are falling short.

In this section, we will explore the various applications that ship with Splunk Enterprise and how they contribute to the overall functionality of the platform.

Three Splunk apps ship with Splunk Enterprise

Splunk Enterprise ships with three applications that play a pivotal role in performing these vital search and analysis functions. They are central to the overall operation and navigation of the Splunk platform, so learning how they function can improve your user experience.

What is Splunk Enterprise, and How Do You Implement it?

If you find it challenging to collect and ingest data at a terabyte scale, search different data types of your business data, and derive data-driven insights to improve your decision-making, Splunk Enterprise is the platform for you.

It uses cutting-edge machine learning algorithms to help numerous organizations predict and prevent performance and security issues affecting their business operations.

Splunk Enterprise does this by clearly communicating complex stories from your business data and providing actionable insights to enhance your business operations and security.

In this section, we will explain what Splunk Enterprise is and how to implement it for your organization.

What is Splunk Enterprise?

Splunk Enterprise is a powerful software platform that helps organizations collect and index their machine data from various sources, including applications, servers, and network devices, allowing you to search, analyze, and visualize it in real time.

It provides valuable insights into your IT operations, security, and business processes.

In simple words, it is an advanced data analytics solution that numerous industries, including financial services, healthcare, retail, IT, and more, use to derive valuable and actionable insights from their business data.

Implementing Your Own Splunk Enterprise Environment

With that out of the way, let's begin planning your implementation strategy. For a successful implementation, you must follow a step-by-step installation plan starting with certain prerequisites.

Let's walk through this stepwise plan to implement your own Splunk enterprise environment.

Check Software and Hardware Requirements

First and foremost, ensure that your hardware and software meet the minimum requirements for your Splunk Enterprise environment.

The hardware should be able to handle the load of the data indexing you plan to do. Splunk Enterprise can run on Mac OS, Windows, and Linux operating systems and requires a minimum of 4GB of RAM.

If your systems don't meet these requirements, you should purchase the right components and upgrades to prepare them for Splunk Enterprise installation.

Install Splunk Enterprise

Once your software and hardware meet all the prerequisite requirements, download and install the Splunk Enterprise software from the Splunk website and follow the installation wizard to complete the installation. It's pretty straightforward, so it should be a breeze.

Configure Server and Forwarders

Once you install the Splunk Enterprise software, you must configure its server and forwarders by editing the configuration files or using the Splunk Enterprise user interface.

The forwarders are critical components of the Splunk Enterprise environment that collect the data from your various sources and transmit it to the server. The server collects the data from the forwarder and is responsible for indexing and performing searches.

Create Apps for Inputs

Now, you must create your input apps or download prebuilt apps from over 2400 available in the Splunkbase app repository. These apps collect data from your various data sources into your Splunk Enterprise environment.

Once you have created or downloaded an app, install and configure the inputs to collect useful data, including log files, APIs, databases, and other important information.

Install Splunk-Based Ops

You will need Splunk-based IT ops to monitor and manage your IT infrastructure, including its network devices, servers, and applications. You can install the prebuilt Splunk Based Ops apps available for download on the Splunk base app repository.

The Splunk-based Ops makes system monitoring clearer and more user-friendly by enabling you to visualize the data using dashboards, charts, and other visualizations.

Ensure Data Is Coming into Splunk

The next stage of your Splunk Enterprise implementation plan involves checking the inputs where you ensure that the data is indeed coming into your Splunk environment.

Here, you use the search interface to check if the data is properly indexed and troubleshoot any problems if they arise.

Create Your Dashboard View

You can create custom dashboards in Splunk Enterprise to display the data you need. This includes charts, tables, maps, and more.

Share them with your team and set alerts for specific thresholds. Customize your dashboard view with all necessary aspects.

Check For Compliance for Enterprise Security

Enterprise security and compliance are vital for an organization to manage data securely. The Splunk Enterprise has prebuilt features that ensure enterprise security and compliance by enabling you to monitor and detect security threats, check compliance with regulatory requirements, investigate incidents, and provide insights for remediation.

Enable Data Models to Secure Data If Insecure

If your data is not secured, it can cause significant problems in the long run, such as financial losses, legal repercussions, and reputational damage. To avoid this, you can secure your Splunk Enterprise by enabling data models.

These data models allow you to classify the data and enforce access controls based on user permissions and roles. If you don't want to use the prebuilt Splunk Enterprise data models, take the time and create your own that suits your security requirements.

Check With Customers If They Have Data to Access Identities

To access identities in Splunk, identify the type of data you need and check if your customers have it.

Obtain necessary permissions and comply with data privacy regulations. Use Splunk Enterprise features to analyze data and gain insights.

Secure sensitive data with authentication and authorization mechanisms, including LDAP integration, which requires creating an LDAP strategy and mapping LDAP groups to Splunk Enterprise roles.

With all that said and done, there is one thing you should remember. Setting up Splunk Enterprise in your organization is a complex process involving numerous stages and configurations outlined in this article.

Ultimately, a Splunk Enterprise environment is only as good as the data you feed into it. You should consult with a professional Splunk Enterprise implementation partner that can walk you through every step of the process.

We recommend partnering with a Splunk-certified professional like BitsIO that can help you devise a solid data strategy before you start your Splunk Enterprise implementation.

Conclusion

In the contemporary workforce landscape hybrid and remote infrastructure will remain prevalent. According to the global research around 16% companies operate on a completely remote infrastructure. Therefore, evaluating and eradicating potential threats become increasingly integral.

bitsIO as a venture aims to establish secured work-from-home infrastructure enhancing the productivity of the companies and inculcating confidence within the employees.

The entire attempt is to create a smarter, secured workforce globally.