Splunk Enterprise Security Add-On

The iboss Splunk Enterprise Security Add-On revolutionizes the way enterprises gather and process security log data. This advanced capability allows organizations to obtain enriched, context-specific security logs from every corner of their network. From remote workers and diverse device ecosystems to disparate geographic locations, every transaction, every user, every device, and every resource is tracked and logged, regardless of where it happens. Traditional methods of collecting data logs are labor-intensive, complex, and often lead to data insufficiency and incomplete Splunk dashboards. Furthermore, accessing and inspecting encrypted data is a significant challenge. The Splunk Enterprise Security Add-On from iboss circumvents these issues. It decrypts and inspects HTTPS data, ensuring the automatic collection of detailed logs from all network traffic, regardless of location. Crucial endpoint data, like MAC addresses, are automatically captured and associated with logs by iboss, leading to a more comprehensive understanding of security incidents.

The add-on significantly enhances the efficiency of your Splunk Enterprise Security by automatically populating your dashboards with valuable data. This rapid population process saves precious time, enhances threat detection and response capabilities, and unlocks the full potential of your Splunk system.

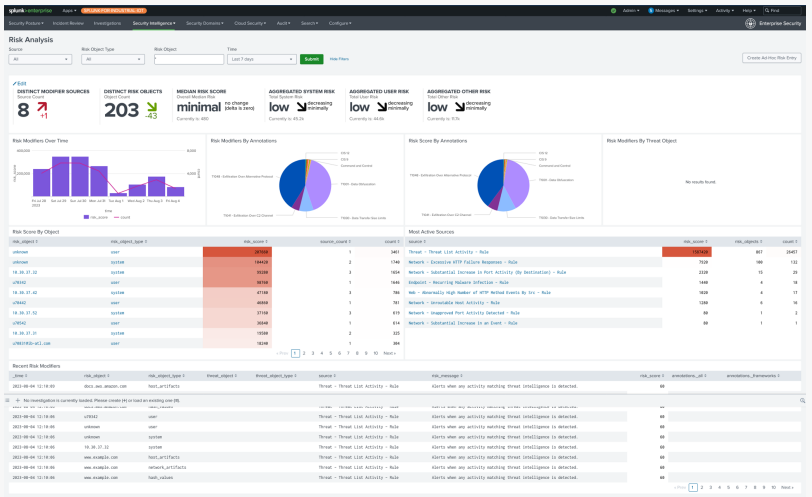
The complexity associated with setting up log forwarding is another hurdle that this add-on effortlessly eliminates. Unlike traditional setups requiring intricate network configurations and cooperation across teams, iboss facilitates automatic log forwarding to Splunk, reducing implementation time from weeks or months to mere seconds.

BENEFITS

- Automatic, comprehensive log data collection of all traffic, irrespective of location
- Populates Splunk Enterprise Security dashboards with valuable data, enhancing your ability to respond to cybersecurity threats
- Facilitates automatic log forwarding to Splunk without the need for complex network configurations
- Automatically captures and associates endpoint data with logs
- Eliminates VPN backhaul which substantially reduces costs and improves connection speeds
- Eliminates the need to configure multiple point products to get Splunk Enterprise Security Dashboards up and running

Splunk Enterprise Security Add-On

In the rapidly evolving world of cybersecurity, the true potential of your existing Splunk Enterprise Security system lies in its seamless integration with iboss. With iboss, your Splunk implementation can reach its full capacity, providing enhanced security, better operational efficiency, and detailed log information. By combining iboss' Zero Trust SSE with your Splunk Enterprise Security, you can quickly achieve unprecedented cybersecurity resilience. Harnessing iboss' robust capabilities, you can unlock value from your Splunk system in less than 60 seconds.



Ordering Information

SKU: Splunk Enterprise Security Add-On

Required Package: All Packages Advanced or Higher

HOW IT WORKS

- iboss Cloud Connectors are installed onto devices which connects them to the iboss Zero Trust SSE for access, security, and logging. Assets, OT and infrastructure data is connected to iboss using agentless methods such as proxy or transparent routing
- The Splunk Enterprise Security Add-On is enabled and connected to Splunk
- With all connections running through iboss for security, inspection and logging, the iboss Zero Trust SSE sends CIM-compliant events to Splunk from all users, assets, and resources automatically, each with over 800 security attributes
- The Splunk Enterprise Security dashboards are automatically populated instantaneously, including visibility into infected devices, malware, and other high-risk data
- There is no need to backhaul data through a VPN for remote users to get security rich data which reduces costs and improves productivity
- The need to configure various network and other systems to get rich data is reduced or eliminated saving valuable time and effort for network and security teams