

# ScanPlus® Security Information and Event Management

## VELOX

### PRODUCT OVERVIEW

Version | Q2.2021

**VELOX**®  
Develops Opportunities For Enterprises...

INDIA | USA | DUBAI | NEPAL | ZIMBABWE | MEXICO | SRI LANKA



# About

Velox is a pioneer of the Indian IT Infra Monitoring and Cyber Security domain. We develop Information Technology Security Solutions and have been in the industry throughout the last decade. Velox has a range of world-class products that meet International Standards in terms of quality and delivery. We offer our solutions to many industries, such as the BFSI sector, Health Care, Manufacturing, and Industrial Automation Systems sector, just to name a few.

With Velox's subsidiary in the United States of America, presence in 7 countries and 3 continents and counting, and the inclusion of our adoption of international standards and regulation, with ISO 9001:2015, 20000 & 27000 and PA-DSS global certifications for our operations, Velox is set for global domination.

## Milestones

**2019-2020:** Asian-African Chambers of Commerce Award-Excellence in Innovation & Technology

**2018-2019:** CIO Tech - Top 20 Most Promising Cyber Security Solutions Provider

**2018-2019:** Business Connect Magazine - The Company of the Year

**2017-2018:** CTO Forum - Best Service Provider in India

**2016-2017:** Listed in CIO Magazine as India's Top 20 Most Promising Business Intelligence Solution Provider

Registered Members and Business Award Recipients of such fine Institutions:





# ScanPlus®

## SIEM | Overview

In the early days of Cyber Security, technological innovation centered around the development of preventive tools that could stop cyber-attacks as they happened. Tools such as host-based or network-based intrusion detection systems, firewalls, and anti-virus software are built to secure the network against attacks.

Today's cyber-attacks are often so sophisticated that without the proper tools, organizations may not even realize that an attack has taken place. This reality is why an increasing number of organizations are relying on their log files as a means of monitoring activity on the IT infrastructure and maintaining awareness of possible security threats. IT organizations must understand the features and capabilities of SIEM. ScanPlus SIEM is a real-time event data collection and correlation tool, which helps the organization with updated security and application-level information. It correlates, responds, and alerts the threat analyzed in the source of events.

ScanPlus SIEM is effective in security orchestration, automation, and response (SOAR) solution, it is possible to achieve more, in less time, while still allowing for human decision-making, at critical events.





# ScanPlus®

## SIEM | Overview

ScanPlus SIEM collects and aggregates log data generated throughout the organization's technology infrastructure, from host systems and applications to network and security devices such as firewalls and antivirus filters. ScanPlus SIEM then identifies and categorizes incidents and events, as well as analyzes them. The software delivers on two main objectives, which are as follows:

- To provide reports on security-related incidents and events, such as successful and failed logins, malware activity, and other possible malicious activities.
- To send alerts if analysis shows that an activity runs against predetermined rule sets and thus indicates a potential security issue.




# ScanPlus®

## SIEM | Functional Architecture

**Events Storing:** ScanPlus SIEM Stores the data for a longer period so that decisions can be made off of more complete data sets. Large networks produce massive volumes of data.

ScanPlus SIEM incorporates features that support efficient retention of high data volumes for required lengths of time. A historical report can be exported of the summarized analysis of the particular period.

**Customizable Dashboards:** Used to analyze (and visualize) data to recognize patterns or target activity or data that does not fit into a normal pattern. ScanPlus SIEM includes dashboarding features that enable real-time monitoring. ScanPlus SIEM Dashboards can often be customized to feature the most important or relevant data, increasing the overall visibility of the network and enabling live monitoring in real-time by a human operator.



# ScanPlus® SIEM | Functional Architecture

**Escalating via Alerts:** When data is gathered or identified that triggers certain responses - such as alerts or potential security problems - ScanPlus SIEM can activate certain protocols to alert users, like notifications sent to the dashboard, an automated email, or text message. ScanPlus SIEM can identify suspicious event log activity, such as repeated failed login attempts, excessive CPU usage, large data transfers, and immediate alert IT security analysts when a possible IoC is detected.

**Integration Feasibility:** Data can be gathered from any number of sites once ScanPlus SIEM is introduced, including servers, networks, databases, software, and email systems. The aggregator also serves as a consolidating resource before data is sent to be correlated or retained. ScanPlus SIEM aggregates event logs from all operating systems and applications within a given network.





# ScanPlus®

## SIEM | Functional Architecture

**Accurate Correlation:** Sorts data into packets that are meaningful, similar, and share common traits. The goal is to turn data into useful information. ScanPlus SIEM can use machine learning or rules-based algorithms to draw connections between events in different systems.

## FEATURES

- Real-Time **Event capture**
- Multi **Log Sources**
- User **Activity Monitoring**
- **File Integrity** Monitoring
- **Network Security** Monitoring
- **Firewall Security** Management
- **Network Security** Tools
- **Compliance** Report
- **USB Security** Analyzer
- **DDoS** Attacks and Botnet Detection
- **Import** Logs
- **Reports** and **Alerts**

# BRANDS WHO TRUST US



भारतीय प्रतिभूति और विनियम बोर्ड  
Securities and Exchange Board of India

**Perto**



**DCB BANK**

**HITACHI**  
Inspire the Next



Visit us at: [www.velox.co.in](http://www.velox.co.in) | <https://veloxtech.us/>  
email: [sales@velox.co.in](mailto:sales@velox.co.in)