

BrightVue XDR

Photo by liv-bruce on Unsplash



360° Real-Time Security Management

In today's connected world, business performance depends on the uptime and performance of networks and applications. Traditional IT security strategies such as antivirus software and network firewall devices, are no longer effective in today's environments, as an increasing number of users now need to access enterprise applications remotely, from outside the physical enterprise locations. This exposes enterprises to new security risks and performance problems lurking everywhere—at the end-user device, on the network, or in the cloud.

Many network security solutions today continue to rely on manual procedures – log analysis and periodic testing - thus providing only limited insights into what is happening in the network. Often IT operations teams know there is a problem, but cannot get to the right level of analysis quickly or easily enough. IT teams need a new generation of solutions that provide a comprehensive understanding of threats affecting all the endpoints, as well as across the entire network infrastructure and the cloud. They need intelligence on a real-time basis across security threats and network performance, to quickly identify the root cause before the enterprises gets impacted.

BrightVue-XDR Extended Detection and Response Platform

BrightVue-XDR is a next generation SIEM platform that combines real-time network visibility with event data logs on the devices in the enterprise, to provide enhanced insights with superlative user and entity details and performance. Whereas the current generation of SIEM tools analyze event data but continue to leave blind spots, with BrightVue-XDR, IT security teams are no longer in the dark when analyzing events and responding them:

- Provides complete real-time visualization and understanding and control of users, assets and traffic flow.
- Inspects networks and issues alerts for threats and anomalies occurring in the enterprise network
- Scans computer systems and issues alerts on detecting security threats and vulnerabilities
- Tracks and analyses user activity to determine if any could lead to compromise and misuse

With full-scale, real-time monitoring and deep flow network analysis, BrightVue-XDR enhances IT teams' awareness about the network. BrightVue-XDR provides security and performance monitoring for cloud and on-premises environments in one fully-integrated platform.



Key Benefits

- **Business are becoming increasingly digital:** Gain tangible visualizations and understanding of your digital presence in cyberspace.
- **Business are churning out enormous data:** Data flow is like the blood flow of your business. Observe and understand conversationally the flow of your business data internally and externally from various end points.
- **Businesses rely more than ever on remote users and cloud:** Proactively detect your cyber risks at multiple levels and take action to protect and cover your business from business and financial damages.
- **Misuse and data thefts are on the increase:** Instantly understand users and entities digital behavior patterns and anomalies.
- **As your business grows, so do your IT assets:** Understand the utilization of your IT assets and optimize their use.
- **Expenditure on bandwidth and traffic are constantly increasing:** Monitor usage and performance of your communication links to optimize and lower costs.

BrightVue FA Probe

Minimum System Requirements

- Intel I7 Quad-core (3 GHz or above).
- 4 GB RAM or higher (recommended 8 GB).
- 500 GB HDD (7200 RPM) or SSD.
- 1 Gbps or 10 Gbps Intel Network Adapter with DPDK support.
- Cent OS Enterprise Linux 7.6.

About Veryx Technologies

Veryx is an innovative provider of visibility, security, monitoring and testing solutions for enterprises, cloud providers, data centers and telcos, to efficiently manage their networks and infrastructure. Veryx is constantly innovating to provide highly automated and flexible solutions, thereby customers can focus on what they do best – grow their business. Our unique product design and architecture, coupled with intuitive interfaces, provides highly efficient and capable platforms. Veryx has technology and marketing partnerships with global players in the communications networking industry.

Key Features

- **End-point Detection and Response** – Host Intrusion detection, File Integrity Monitoring, Network Intrusion detection and prevention.
- **Network Detection and Response** – for detection of threats and anomalies.
- **Real-time visibility of conversations** – across entire network with metrics on top users, conversations and bandwidth users.
- **User Entity and Behavioral Analytics (UEBA)** – profiling based on usage patterns of IT assets and threats faced.
- **Multi-log analysis** – for events and threats.
- **Network asset discovery** and inventory.
- **Vulnerability Assessment** –scan assets to identify vulnerabilities.
- **Application performance and user experience monitoring (APM)** – ensure business critical applications are functioning as per SLAs.
- **Software-based, supports on-premise and public cloud-based usage** – flexible and scalable to accommodate growing business needs.

BrightVue Controller

Minimum System Requirements (for on-premise deployment)

- Intel Xeon E5 - 1660 v4 (or equivalent).
- 32 GB RAM or higher (recommended 64GB).
- 2TB HDD (7200) RPM or SSD.

Veryx® and BrightVue™ are trademarks of Veryx Technologies. All other trademarks of respective owners are acknowledged.

Email : info@veryxtech.com

Web : www.veryxtech.com

USA: +1-267-440-0140

International: +44-203-371-8691