VISIBILITY

Visibility is a cornerstone of cyber defense and the reason it is recommended as a first control of most frameworks. You cannot protect what you cannot see. As organizations grow their footprint, expand use cases, extend into the cloud and beyond their perimeter, an accurate inventory is paramount to preventing cyber attacks. Organizations cannot prepare the appropriate defense and response strategies without a complete field of vision or truly understanding the status of the entire attack surface.

WHY FULL VISIBILITY IS CRITICAL FOR YOUR CYBERSECURITY STRATEGY

Get a Full View of Threats

You can only protect against what you know exists. Implementing a comprehensive strategy to gain visibility into your attack surface lets organizations proactively identify and mitigate potential security risks to safeguard critical assets and sensitive information.

Stop Lateral Movement of Attackers

Collect and correlate existing security tools alerts to shorten mean time to detection and response. Investing in proactive measures to stop lateral movement helps avoid potential financial losses, reputational damage and legal liabilities associated with a cyber attack.

Respond to Threats Quickly and Efficiently

Investing in visibility improves the overall cybersecurity posture and lets organizations stay ahead of potential threats through real-time insight into network traffic, application activity and user behavior. Potential threats can then be proactively identified and stopped before they cause an impact.

Device Visibility

Identify all managed and unmanaged devices with access to resources on premise, in the cloud or however they are available. Provide conditional access based on real time assessment of predetermined criteria.

Data Visibility

Properly discover, classify and monitor data wherever it exists; on local drives, in central file shares or in the cloud. Enable encryption and data loss prevention at each egress point.

Cloud Visibility

Proactively discover, scan and monitor all cloud resources. Continously assess the configuration, scan vulnerabilities and data connections to reduce the attack surface.

Application Visibility

Continuously scan and store software and application inventory in a central repository to ensure misconfigurations or vulnerablities are remedied.

East-West Traffic Visibility

Map the current application access and data flow between internal systems and internal/external systems. Continuously monitor for unauthorized or anomalous activity to detect a breach before a true impact is realized.

Network Traffic Visibility

Identify potential threats and malicious activities with thorough network inspection. Use traditional firewalls, IDS or purpose build deep packet capture and analyzers for true network forensics.

Alert Visibility & Correlation

Collect and correlate existing security tools alerts to shorten mean time to detection and response.

Brite

Brite.com
1.800.333.0498
SalesInfo@Brite.com