Joint Solution Brief

ATTIVO NETWORKS BOTSINK® DECEPTION SERVER INTEGRATION WITH THE QUANTEA QP AND PUREINSIGHT®

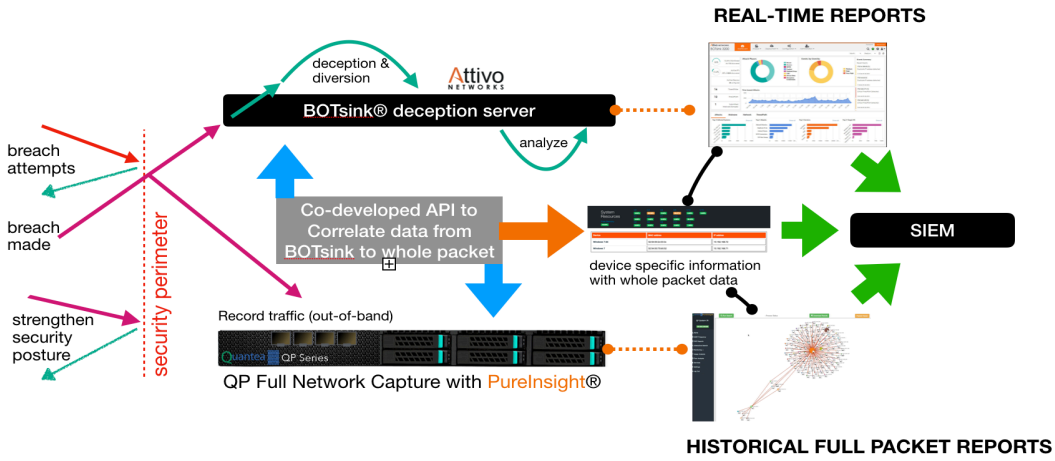
The Quantea QP and PureInsight® paired with Attivo's ThreatDefend® platform provides advanced, real-time, in-network threat detection and improved incident response. With the joint solution, customers receive improved threat intelligence to not only identify all affected nodes of compromised systems but also to uncover full network packet information and the propagation path of an attack. Organizations can reduce time and resources required to detect threats, analyze attacks, and to remediate infected endpoints, ultimately decreasing the organization's risk of breaches and minimizing data loss.

The Challenge

Cyber attackers have infiltrated and continue to break into the networks of even the most secure organizations. Whether the attacker finds their way in using stolen credentials, zero-day exploitation, ransomware attacks or simply starts as an insider, they will establish a foothold and move laterally throughout the network until they can complete their mission. Once attackers bypass the existing prevention mechanisms, they can easily move around the network undetected by the remaining security solutions. It can be difficult, costly, and time-consuming to identify and trace all endpoints affected by a network security breach or attack. Existing security measures have been proven inadequate when it comes to quickly detecting and shutting down these attacks.

Moreover, a longer response time means more data is compromised and more damage is made to network infrastructure. As attackers and botnets continue to increase in complexity, many conventional tools have difficulty adapting to new attack vectors and zero-day attacks. Surface data from alerts alone is insufficient for organizations to maintain their security posture, even in cases where attack vectors and compromised devices have been successfully identified. By correlating surface data from alerts and network traffic data, an organization can attain a highly accurate assessment of any security event. This set of challenges will require a holistic approach so that the organization can successfully identify an attack vector while gathering critical information only available through whole packet data.

The Holistic Approach of the Joint Solution



Attivo Networks offers the ThreatDefend® platform, providing early and accurate detection of in-network threats, regardless of attack method or surface, using deception and concealment technologies. It provides a detection fabric for cloud, network, endpoint, application, data/database, and Active Directory decoys and is highly effective in detecting threats from virtually all vectors such as APTs, stolen credentials, Man-in-the-Middle, Active Directory, ransomware, port knocking and more. The platform can deploy within all types of networks, including endpoints, user networks, server, data center, remote work sites, the cloud, and specialty environments such as IoT, SCADA, POS, SWIFT, infrastructure, and telecommunications. It not provides early detection but also adds automated intelligence collection, attack analysis, and third-party integrations to accelerate incident response.

With unparalleled storage capacity, the Quantea QP can store an organization's network traffic for weeks and months while maintaining high granularity. When Attivo's ThreatDefend platform identifies an attack and which devices within the network have been compromised, the security team will receive timely alerts and be able to access crucial information through the Attivo GUI. The QP API will extract the alerts and display them on Quantea's PureInsight® dashboard, from which security professionals can easily access whole-packet network information stored in the QP. This technology enables an organization not only to pinpoint all affected nodes and view a detailed history of the network traffic flowing through those devices but also to examine the web of interconnected devices surrounding infected areas so the security team and prioritize endpoints that are most at-risk and take action to halt the attack before any more devices can be compromised. More importantly, PureInsight® offers critical insight on what is being propagated through the network and the extent of the attack. In addition, this process can be easily automated. Overall, the setup highly reduces the response time and minimizes the risk, the extent, and the impact of a security breach, stopping an attack in the shortest amount of time possible if not completely preventing the breach to begin with.

The Attivo ThreatDefend®

The ThreatDefend Deception Platform creates an active defense against cyber threats and has many modular components. The Attivo BOTsink® deception servers provide decoys, the Informer dashboard for displaying gathered threat intelligence, and ThreatOps® incidence response orchestration playbooks. The Endpoint Detection Net suite includes the ThreatStrike® endpoint module, ThreatPath® for attack path visibility, ADSecure for Active Directory defense, the DataCloak function to hide and deny access to data, and the Deflect function to redirect malicious connection attempts to decoys for engagement. The ThreatDirect deception forwarders support remote and segmented networks, while the Attivo Central Manager (ACM) for BOTsink and the EDN Manager for standalone EDN deployments add enterprise-wide deception fabric management.

Quantea QP and PureInsight®

The Quantea QP is a high performance solution to network security issues which captures and filters network packets full-payload and provides accessibility with high speed search and analytics. With unparalleled storage capacity, it is able to duplicate network traffic in real time to store for up to weeks and months. The QP supports over 150 protocols and its API integrates seamlessly with PureInsight as well as third-party tools. Quantea's PureInsight® software has an intuitive interface that allows users to map and analyze the network at various levels of granularity to pinpoint and resolve network anomalies quickly and efficiently. PureInsight enables security professionals to analyze the topology of the entire network, focus in on details of specific nodes within the network, and investigate the web of interconnected devices surrounding infected devices.

About Attivo Networks

Attivo Networks® provides innovative reconnaissance, credential theft, privilege escalation, and attack lateral movement detection solutions for combating today's advanced threats and ransomware attacks. Delivering a superior defense for revealing and preventing insider and external threat activity, the Attivo ThreatDefend® Platform offers scalable protection, detection, and data concealment and access denial solutions for endpoints, Active Directory, and network devices. It provides comprehensive coverage and attack path visibility for user networks, data centers, clouds, remote worksites, and specialized attack surfaces. It streamlines incident response with forensics, automates attack analysis, and includes third-party native integrations. The company has 130+ awards for technology, innovation and leadership.

www.attivonetworks.com

About Quantea Inc.

As a pioneer in converging network analysis and data science, Quantea empowers enterprises to maximize operational potential, capture value, and drive growth like never before. Our technology provides organizations of all sizes with the capability of fully understanding their network. From a network's macroscopic topology to nanoseconds-worth of network traffic, the QP Series enables an unprecedented amount of data to be recorded with a high level of granularity and accessibility, and the PureInsight® software allows network analysis not possible in any other network-recording platform. Whether it is resolving user or network anomalies, protecting or detecting intrusion, or capturing network or business intelligence, insight begins with Quantea.

www.quantea.com