KNOWLEDGE BRIEF

SnoopWall is Recognized as Technology Leader in Network Access Control (NAC) Market

KNOWLEDGE BRIEF

BY

SnoopWall is Recognized as Technology Leader in Network Access Control (NAC) Market

Quadrant Knowledge Solutions recent study analyzes global market dynamics of Network Access Control (NAC) market. As a part of this research, Quadrant analyzed leading vendors involved in providing NAC solutions including NAC appliances, virtual appliances, and NAC-as-a-Service. This study provides strategic market analysis of Network Access Control market including market forecast, market share, competitive positioning, market trends, and strategic insights for growth.

According to Quadrant Knowledge Solutions study "***Network Access Control (NAC) Market Outlook***" is expected to grow significantly with a CAGR of 31.5% from 2016 to 2020. The market growth is primarily driven by rise in Advanced Persistent Threats (APTs), zero-day malwares, and corporate espionage.

The research of Quadrant Solutions identifies SnoopWall as technology leader in Network Access Control (NAC) appliance market. SnoopWall is known for its innovative breach prevention technologies, such as agentless quarantine and malware pre-cognitive to protect against malicious insiders, rogue devices, and latest ransomware. In addition to large NAC appliances, the company also offers nano appliances which make them preferred amongst small and medium sized businesses (SMBs) to secure their corporate networks at affordable costs.

Founded in 2012, and headquartered in Nashua, New Hampshire, SnoopWall is amongst the most innovative providers of patented network access control (NAC) solutions to protect corporate network against the most advanced threats. Through their patent-pending WinSHIELD, MobileSHIELD and AppSHIELD SDK, it's the first company to provide Counterveillance security solutions that help users to make their web and mobile browsing nearly invisible to provide robust information security for the bring your own device (BYOD) dilemma. SnoopWall's suite of products offer advanced network security solution that detects and blocks all rogue network access, remote control, prying and spying.

SnoopWall NetSHIELD™ – Next Generation of Agentless NAC Appliance

A robust strategy for network security is increasingly becoming the top priority of most of the organizations. Many big organizations, such as Anthem, Sony pictures, and Ashley Madison have also proved to be vulnerable and have been subjected to data breaches. Hence, most of the enterprises have instituted teams with their IT departments to scale up their network security technology on the concurrent basis. According to industry estimates, over

90% of the security breaches occur inside the company's network. While almost every company has basic network security infrastructure in place, such as firewall and anti-virus (AV), modern threats have grown beyond the capabilities of these basic security solutions.

SnoopWall's NetSHIELD™ is the next generation agentless NAC appliance that protects corporate networks against internal intrusion and malicious insiders by effectively managing access of devices into corporate networks. NetSHIELD™ pre-cognition engine is designed to quarantine an endpoint prior to infection. A proprietary mechanism ensures quarantining with zero-false positives. NetSHIELD™ enables users to manage, block, quarantine internal security threats, identify network vulnerabilities, detect and block rogue and malicious devices on networks, manage connected devices, and such others to protect corporate network against the most advanced security threats. It also helps organizations to conduct security audits and enforce compliance to regulatory requirements.

Network Security in the Age of BYOD, WYOD, and Mobility Trends

Increasing trend of mobility and bring your own device (BYOD) trend has made the mobile security amongst the top security concern globally. Management and access control of wide variety of mobile devices with multiple versions of software have become the prime importance for securing the corporate network along with security policy formulation and implementation across corporate networks. In addition, the companies are facing challenges with increasing adoption of wearable technologies and are looking for extended security policies to include wear your own device (WYOD) trend.

While networks can't clean the devices regularly to avoid malware infections, it can guard their access to detect malwares from entering corporate network. Users are likely to disable certain security settings and download apps on to their devices that are potentially virulent. This compromises the security of the smart devices and so, organizations need to ensure that these affected devices do not pass on the breach onto the network.

SnoopWall's MobileSHIELD™ enables effective implementation of BYOD and WYOD policies. SnoopWall MobileSHIELD™ endpoint agent is managed by its NetSHIELD™ NAC appliance through the optional BYOD command center. It enables employees to use their personal devices (smartphones, tablets, laptops etc.) without restriction outside of corporate networks or geofense. However, when into the corporate network, MobileSHIELD™ endpoint agent receives and enforces policies to protect businesses against infected and rogue mobile devices. SnoopWall's MobileSHIELD™ is proven solution offering next generation of mobility and BYOD security with the convergence of consumer privacy and business data security.

SnoopWall APPSHIELD™ SDK for Mobile Application Security

With growing usage of smart phones in the workplace, companies are increasingly providing access to important enterprise applications on users' smartphones. This possesses significant challenges in securing endpoint and network security that requires support for multiple mobile devices from multiple vendors and multiple operating systems. Typically users have several applications installed on their mobile devices containing sensitive personal information, such as banking apps, credit card, airlines, hotels, and corporate applications. Most of these applications access is secured with traditional username and passwords. Driven by significant growth in smartphone adoption, mobile platform have become the most popular target by cyber criminals and mobile apps containing advanced malware are becoming popular attack vector. Hence companies are looking for advanced security technologies for protecting mobile applications without compromising on consumer experience on the apps.

SnoopWall APPSHIELD™ (SDK software development kit) helps in protecting mobile applications containing consumer personal identifiable information (PII) for enhanced consumer app experience. SnoopWall's advanced cloaking technology is designed to make the mobile app invisible to others apps on the mobile and to the most advanced hackers, cyber criminals and malware threats.

Last Word

Driven by digital transformation, BYOD trend, and emergence of WYOD trend, network security has taken the center stage. Organizations are looking for formulating and implementing robust security policies and investing in advanced security technologies to protect corporate networks against expanding threat landscape. As cyber-attacks are increasing in frequency and complexity, securing corporate networks is a top priority of organizations. Hence many companies are adopting network access control solutions to manage access and security of variety of devices within organizations corporate network.

Driven by comprehensive, advanced, and scalable technology, SnoopWall is recognized as technology leader in NAC appliance market. SnoopWall's latest NAC technology is well positioned to help users with real-time quarantine of zero-hour malware and phishing attack, mac-spoof detection, TLD blocking and compliance enforcement.

Therefore, for SnoopWall's proactive and most advanced approach to breach prevention and for their cost effective solution, we believe SnoopWall will continue to become a dominant, growing force, in the Network Access Control marketplace, most especially for small to medium size enterprises and for larger organizations with remote offices.