RE-INVENTING NETWORK SECURITY FOR A CONNECTED FUTURE

Anti-virus and firewalls are no more the sole saviours of complex networks. Today, this term has undergone a dramatic shift. Organizations that used anti-malware are re-inventing security with the use of sensors for multi layered, centralized security systems. Businesses are also developing security technology that can understand artificial intelligence (AI) and machine learning (ML).

■ BY: DIVSHA BHAT <DIVSHA@GECMEDIAGROUP.COM> ■ PHOTO: SHUTTERSTOCK

The network security market flourished 2016 with a worldwide revenue of $2.2 billion. According to MarketsandMarkets, the Wireless Network Security Market is expected to grow from $8.47 billion in 2014 to $15.55 billion by 2019, at a Compound Annual Growth Rate (CAGR) of 12.94% during the forecast period. The increase in the usage of mobile devices and the increase in demand for integrated security solutions are few of the aspects that lead to the growth of the network security market in the coming years. The growth of SaaS (Software-as-a-Service) based network security solution is considered as the main factor in the growth of overall market.

TAKING ARMS AGAINST

NETWORK THREATS

With an increasing amount of people getting connected to networks, the security threats are also rising. The CIO's or the IT leaders are naturally cautious about their network safety. The organizations should look into mitigating risk by patching vulnerabilities. An unexpected connection could be an important sign of a possible breach which may pass unnoticed.

"The organization should look at deploying tools that provide the essential visibility and network context that allows security operations teams to detect and respond to breaches. There is no static network deployment which will mitigate all threats so organizations need to supplement the preventative security measures with rapid detection and response to minimize the impacts of breaches when they occur" said Peter Goodwin, Sales Engineering Director EMEA, Infoblox.

"Organizations should monitor the health and activity of their network in real time, immediately patch security updates and fixes, and harden their systems via secure communication protocols. They should also routinely keep security and activity logs to help them prevent threats and provide much-needed support for forensic analysis and government compliance. Lastly, users should be fully aware of security challenges and where threats can come from" commented Biju Bhaskaran, Pre-Sales Manager, Alpha Data.

"In order to be agile and provide required protection, security solutions need total network visibility, including physical and virtual hosts, operating systems, applications, services, protocols, users, content, network behavior as well as network attacks and malware. We can of course deploy technology to fix the issue on visibility – In fact that is what we are doing for many organizations, but it is really also about understanding the attack vectors which spread these threats and then ensuring that those vectors are eliminated or the risk mitigated" said Nicolai Solling, CTO at Help AG.

WHAT DOES RE-INVENTION MEAN?

To avoid breaches, organizationsare making sure they stay ahead of hackers. Businesses are protecting customers data with higher standards of security.In such a threat landscape, organizations are have taken several measures to combat the threats. "In keeping up with Global and regional trends, we have a very focused approach towards Cyber Security. We have recently launched our world class Cyber Defense Centre (CDC) in the UAE. This plays a very critical role in deploying advanced security intelligence and automation tools to identify threats quicker and with greater accuracy and precision. The way we do this is by scrutinizing threats with a combination of Threat Intelligence and end point technologies which are capable of detecting more complex threats and may be dormant in a customer's environment" said Sachin Bhardwaj, Director - Marketing and Business Development, eHDF.

"Alpha Data can integrate sophisticated security technologies sourced from its global partner network with Security Operation Center (SOC) and other standard global security processes"

-BIJU BHASKARAN,
PRE-SALES MANAGER, ALPHA DATA.

"We are actively involved in developing our cloud based capabilities, to provide the analytical ability to identify and contain data exfiltration, DNS tunnelling and other DNS related threats within the cloud"

-PETER GOODWIN,
SALES ENGINEERING DIRECTOR EMEA, INFOBLOX

NETWORK SECURITY TIPS TO MITIGATE RISKS

- Training & Awareness
- Establish a BYOD Policy
- Defense in Depth Network Security
- Unauthorized access
- Back-up the data
- Physically secure equipment and ports
- Set up a log management system
- Upgrade software with latest security patch
- Promote a security conscious environment
- Use two factor authentications

"Creating layers of protection or a "defense-in-depth" approach can help provide a sound strategy for network security"

-SACHIN BHARDWAJ,
DIRECTOR - MARKETING AND BUSINESS DEVELOPMENT, EHDF

"Be sure to establish safe practices when using and accessing cloud services; don't pass the responsibility of security to the cloud provider"

-OSAMA AL-ZOUBI,
CHIEF TECHNOLOGY OFFICER, CISCO MIDDLE EAST.

"We actually have developers who only focus on these API's and we believe that this elevates our services from just installing a box to building an end-to-end solution"

-NICOLAI SOLLING,
CTO AT HELP AG

Cisco says, in 2020, as many as 1 million connections will be included to the web every hour. "We're going to develop security deep into the network due to the fact that the network is going to be the platform throughout which all these connections enter your world and we need to begin preparing security the minute they hit the wire or we do not have a chance. So, security is deeply embedded to develop trust. All of this over time creates this adaptive system that comprehends your intent, has a level of trust built in, that then gets notified by context and continuously adapts and over time can really adjust itself based on exactly what it understands you're trying to do and the context it has seen flow through the network" said Osama Al-Zoubi, Chief Technology Officer, Cisco Middle East.

FINALLY

AI will play an important role in improving network security. But, the bottom line is, there is no perfect security. Hackers will also look into the emerging technologies to bypass network security. Cyber-attacks are triggered by humans, so countering them requires human logic and cannot be solely done by machines. The need to protect network security will go on for a long time and the mitigation techniques will change but the attacks are not going to go away.

CISCO

Cisco's approach creates an intuitive system that constantly learns, adapts, and protects, to optimize network operations and defend against today's evolving threat landscape.

eHDF

eHDF's Managed Security Services allows customers to avail of either tailormade solutions or they can combine several aspects of the available services to suit individual needs

INFOBLOX

InfobloxDNS records give excellent insight into what the compromised host is doing and right at the heart of the network and has a front row seat to what the adversary is trying to do.

Help AG

Help AG does proactive threat hunting for customers for malware and build automatically triggered use-cases when we see major malware outbreaks

ALPHA DATA

Alpha Data possesses exceptionally skilled personnel, processes, tools and technologies to identify threats at the earliest stages.