LogicFinder
Consulting, Development and Training

Network Fort

Ransomware Protection

Feb 2021

Introduction

Ransomware strikes every business either big or small but what's more important is to know how to respond to these attacks to minimize the associated costs. With the advancement in technology and techniques, ransomware detection has become more difficult as the attackers are more technology sound and they often deploy unrecognizable techniques to get into your network. To minimize the risks associated with ransomware, it's important to deploy such security system that can work ahead of attackers and prevent them from entering into your network.

Ransomware Propagates

Ransomware typically is a crypto malware commonly used for cyber extortion. Its most basic attack involves encryption malware, which at first encrypts data and applications and then hardware, and finally it extorts owner's encrypted assets to make a financial transaction. Ransomware can spread all over the company's network leading to tragic downtime. At times, the impacts are catastrophic and often lead to bankruptcy. Once a company's system is encrypted by ransomware, ransom hackers demand a huge amount to provide a decryption tool, this amount is generally 100 times more than the individual ransom amount demanded. Ransomware attacks are usually accompanied by phishing attacks. These attacks may include sending a malicious email attachment or a URL to an unauthentic website or an app containing a virus. At large, these target businesses and the encrypted network causes the company's operations to cease. In 2016, ransomware attacks have affected millions of end users and its cost victims were reported to be more than $1 billion.

Ransomware Impacts in Past Years

In the past years, most devastating impacts were observed for WannaCry and Pety, a outbreaks that affected thousands of end users .It locked down systems of large enterprises across the world and the hackers didn't even build a way to retrieve the lost data. It not only deprived the large enterprise from their important data but also damaged their processing ability. In most cases, ransomware is delivered through email that appears to be a legitimate one that entices one to follow a link or to download an attachment containing the malicious software. Some attackers also use social media messaging to deliver ransomware to crack your network security.

Ransomware Is Dangerous

Ransomware attacks can steal all your sensitive and confidential data including customer's login credentials, payment and transaction details, email addresses, contact numbers and much more. In just a single attempt, it can make your business lose its large number of loyal customers. Regardless of numerous practices often deployed by enterprises, Ransomware attackers are still able to crack your business's security. This is because the methods that companies employ to secure themselves from malware variants are not developing at the same pace as the malware authors.

Need of An Advanced Security System

NetworkFort understands that the security challenges for enterprises are continually increasing, as the attackers are more technology sound today, often use such techniques that appear to be legitimate, and hence, misguide any network person. In such cases, a dire need exists to deploy such an efficient security system that can detect any suspicious activity of attackers and block their access within a second before it may lead to any big crises. NetworkFort has realized that the traditional security systems desperately need evolution to cater the rapid growth of insecurities and attacks. We have evolved how cyber security is implemented and created a new mechanism to defend us against the rapid growing attacks.

NetworkFort, an Ultimate Cyber Tool

AI Platform

NetworkFort is a Cyber-Intrusion Detection System, which can cater enterprise level cyber-attacks using Artificial Intelligence. NetworkFort has raised the stakes of infiltrators by its design to protect the organizations by evolving itself to hunt out the advancing threats and attacks. NetworkFort serves as a security solution that secures connected devices across the network of both industrial and IT environments.

Constant Data Monitoring

NetworkFort passively monitors your network and scrutinizes it for any kind of crucial threat. It works with every device connected with your network including your airspace. NetworkFort provides immediate alerts upon noticing any anomalies in device's behavior that could be dangerous. It provides detailed history of each device and its connections enabling administrators to look out for connections made and protocols used, and data transmitted.

Threat Detection Technology

NetworkFort has an amazing threat detection technology that uses machine learning and artificial intelligence to identify when a device is operating outside of its traditional behaviour. Any deviation from normal behaviour or policy violation or device misconfiguration is thoroughly investigated. It detects any unrecognized device connection request or unusual operating software on a device and quickly gives off alerts to indicate that the device has been compromised.

NetworkFort, a Quick Solution

NetworkFort is an easy and a quick solution to deploy on any system. It efficiently minimizes operational downtime. NetworkFort is user friendly and can be deployed on any system. With integration of NetworkFort in your network, you will not need to worry about the minor details as NetworkFort itself does all the tasks for instance NetworkFort captures traffic and analyses it. NetworkFort has been designed by our team to root out highly threatening evolving attacks using Artificial Intelligence.

Scope of NetworkFort

NetworkFort provides AI-integrated cyber security solutions to a range of industries, from finance services, manufacturing & supply, education to telecommunications, e-commerce and health care. For organizations and businesses in need of reliable cyber, defence solutions, NetworkFort provides machine learning-powered product, NetworkFort that detects and protects against variant malware, ransomware, trojans and other cyber threats.