portnox™

SOLUTION BRIEF

Ransomware Response and Control

Gain Visibility, Control and Response Capabilities to Combat Ransomware and Related Malware Attacks

The Challenge

Ransomware and malware, malicious cyber threats that request victims to pay a ransom to retrieve stolen and encrypted data, are now the most prevalent cybersecurity threats. Recently, such attacks have increased in frequency and severity, evidenced in the 2017 WannaCry/NotPetya attacks that affected over 200,000 computers globally.

Faced with the threat of ransomware attacks, many organizations are now actively engaged in updating their cybersecurity defenses and authentication procedures to avoid the attention of hackers. This can be a difficult process because many companies are unaware of the state of their network and which points of connection are vulnerable to threats – such as Internet of Things and Bring-Your-Own devices. With ransomware attacks becoming increasingly common and affecting more businesses than ever before, there has never been a better time to gain an advantage over the hackers by implementing a layered ransomware defense, response and remediation plan on the enterprise network.

An effective plan for defeating cyber extortion is based on ransomware defense tools, such as anti-virus and anti-ransomware software that provide: behavior-based detection, prevent file modifications, prevent access to files, recover files and vaccinate against the ransomware strain. However, these offerings are only part of a comprehensive ransomware response and remediation solution because, as any cybersecurity expert knows, security starts with the network. Therefore, a good ransomware defense, response and remediation plan integrates full visibility of the network with all connected, managed/unmanaged endpoints (even IoT and BYOD), control over access to files, resources and data, and remote remediation capabilities, including the possibility of quarantining or blocking infected devices to control for lateral attacks.

The Portnox Solution

Portnox's Rapid Ransomware Response and Control Solution addresses the reconnaissance, exploitation and remediation phases of the ransomware kill chain, and, together with its technology partners and integrations, can be used to make up a holistic ransomware solution:

Reconnaissance

During this phase, the attacker collects information on the target, be it through research of publicly available information or social engineering.

> **How Portnox Helps:** Portnox's solutions provide a real-time picture of all network elements, attaining information about their status including security posture assessment, granular information and context on endpoints, as well as their level of compliance. Organizations can assess endpoints based on company security policies to understand the level of risk and identify vulnerabilities early-on. Endpoints that fail to uphold the network security policies, are missing the latest anti-virus and OS patches, or have certain technical specifications that have been deemed vulnerable, will be blocked from accessing the network or quarantined until security updates are made. Portnox offers the ability to see into one of the weakest areas of the corporate network, i.e. Internet of Things (IoT) devices. CISOs, network administrators and IT teams can discover where IoT devices are located on the organizational network and detain them in a separate VLAN network with limited access.

Exploitation

In the delivery and exploitation phase, hackers use the information attained in reconnaissance to carry out attacks on vulnerable endpoints, users and areas of the network.

> **How Portnox Helps:** Portnox receives information from third-party security vendors to actively identify anomalies. Portnox has full communication with these vendors, so that their assessments are seamlessly integrated. Carry out on-going sandboxing of endpoints according to defined characteristics, including for IoT devices. Filter endpoints according to patch, anti-virus, operating system and active applications and quarantine them if one or more of these aspects has been deemed vulnerable. Portnox shares information when an endpoint's posture assessment changes, helping network administrators identify attempts at social engineering and the early stages of a breach. The admin can then bring that device into compliance with security policies, or quarantine access until remedial security measures are taken.

Remediation

Sometimes, despite having all the right solutions in place, ransomware still gets through. That's why having a rapid remediation plan in place is always a good idea because not only will it help prevent further damage or the lateral spread of the attack, it will fortify business continuity.

> **How Portnox Helps:**
>
> - **Automate Patch Updates Across the Network:** Enforces necessary patch, anti-virus, operating system and application updates across managed and unmanaged endpoints, located both on and off premise.
> - **Immediate Incident Response:** Contains ransomware events by remotely disconnecting endpoints from the network – no manual touch required. Drill down to the level of specification: device type, operating system, anti-virus software version, switch location, and more. Perform automated actions on every device, in all locations, instantly.
> - **Arm Incident Response Teams:** Portnox arms IT professionals and network admins with the ability to remotely take actions on employees' devices. In addition, IT professionals can create an effective incident response plan for each kind of device, employee and office location based on network specifications.

Relevant Technology Partners and Integrations

Portnox prides itself on being a fully integral solution with most major third-party security applications, appliances, software and hardware. Aside from mining data from other sources, Portnox is known for its seamless deployment, even across the most complex networks and security architectures.

Conclusion – Portnox Is Part of a Ransomware-Ready Organization

Ransomware is one of the top threats to individuals and businesses in recent history. Not only does it put sensitive, private information at risk, it has a noticeable impact on the pace and progress of businesses of all sizes. Yet while it's clear that it's not a problem that can be ignored organizations have yet to significantly increase their IT security budget to account for the preparation, response and remediation to such wide-reaching attacks.

Portnox offers network access control solutions that go beyond authentication and control so that organizations can get a hold on network security. Portnox's solutions bridge the gap between endpoint compliance (risk) and the need for network access control to serve a number of immediate cybersecurity needs.

Click here for more information on how to implement a ransomware response and remediation plan together with Portnox!

Contact Us

Americas: usinfo@portnox.com | 1.855.476.7866
Europe: dotell@portnox.com | (44) 1273.256325

www.portnox.com

portnox™