Five Ways

to master remote access security

A New Reality

No matter what industry you're in, your company has likely been affected by the coronavirus outbreak. In fact, you're probably reading this from home as we speak. Remote work is the new reality. While many of us will return to the office when it's deemed safe, many companies have seen first-hand the value and ability of employees to work from home, and will look to enhance and expand their remote workforces when things return to normal.

For network security teams, this poses a host of new challenges, particularly given the loss of physical control over those newly at-home corporate devices. But have no fear…we're here to share the important and often over-looked things to consider as you elevate your remote access visibility and security.

I. A Bridge Too Far

No,we're not talking about the 1977 WWII film starring Michael Caine and Sean Connery (albeit a great movie). Today, companies use VPN gateways and/or virtual remote desktops to provide their remote employees with access to the corporate network and other internal resources. The problem, however, is that some of the most popular VPN vendors have admitted to significant vulnerabilities that would allow any person from the internet with no credentials to use the VPN gateway as the bridge to your corporate network and crown jewels.

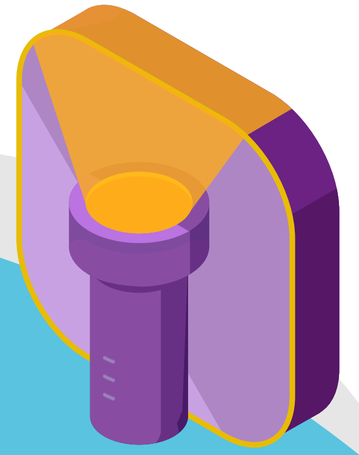
14,000

Pulse Secure VPN endpoints were still vulnerable more than three months after the vendor patch for a reported vulnerability.*

**Source:*
Security Boulevard

II. Are You Afraid of the Dark?

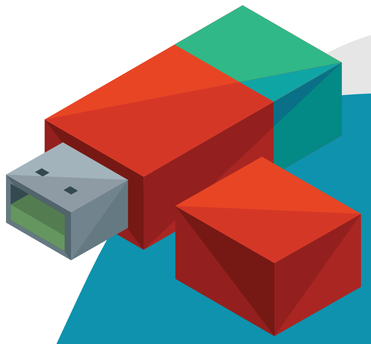
90s kids will get this Nickelodeon reference, although it’s not the show we’re focused on today. We’re all afraid of the dark, and rightly so…scary stuff happens in the dark. That’s why you need to be continuously aware of the risk posture of every remote device connecting to the network continuously – all the time, every time, no matter location or device type. This will allow you to react in real-time to potential threats before $#!% really hits the fan.



57%

of IT leaders believe remote workers will explore their organization to the risk of a data breach

**Source:*
Continuity Central



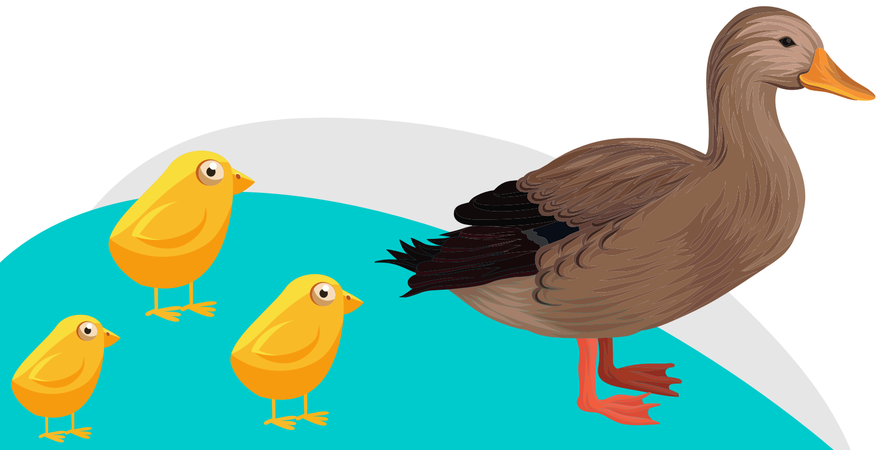
6/10

employees use non-encrypted USB drives on work devices.*

**Source:*
HelpNet Security

III. If You Play with Fire...

…you'll get burnt. If you want to play it safe, you need to be able to automatically remediate non-compliant devices being used by remote employees. This means being able to control whether non-encrypted USBs can be used on laptops, blocking or quarantining devices in which anti-virus and firewall is not up-to-date and beyond.



99.9%

of Microsoft enterprise accounts that get hacked don't use MFA.*

*Source:
We Live Security

IV. Walks Like a Duck, Talks like a Duck...

User credentials get stolen all of the time. Protect against the use of remote access credentials being used to connect non-company or non-compliant devices by using multi-factor authentication that only authenticates an endpoint based on the user's credentials AND the current risk posture of the device being used to connect.

V. I Am the [Road] Warrior!

The 90s got their shout out, now let's hear it for Patty Smyth and 80s. Anyway, companies with large teams of field representatives and road warriors already know this, but devices outside of the office are much harder to keep track of and can easily go missing. To protect against these devices being compromised if lost or stolen, it's best practice to employ full disk encryption, which applies encryption to the entire hard drive including data, files, the operating system and software programs.

45%

of healthcare breaches occurred due to stolen laptops.

**Source:*
CSO

Portnox

Portnox provides simple-to-deploy, operate and maintain network access control, secure wifi and visibility solutions. Portnox software can be deployed on-premises, as a cloud-delivered service, or in hybrid mode. It is agentless and vendor-agnostic, allowing organizations to maximize their existing network and cybersecurity investments. Hundreds of enterprises around the world rely on Portnox for network visibility, cybersecurity policy enforcement and regulatory compliance.

The company has been recognized for its innovations by Info Security Products Guide, Cyber Security Excellence Awards, IoT Innovator Awards, Computing Security Awards, Best of Interop ITX and Cyber Defense Magazine. Portnox has offices in the U.S., Europe and Asia.