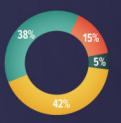
THE STATE OF NETWORK SECURITY

DO YOU FEEL YOUR ORGANIZATION'S NETWORK IS AT RISK FROM CYBERATTACKS AND/OR BREACHES?

80% ARE VERY/SOMEWHAT CONCERNED ABOUT NETWORK BREACHES

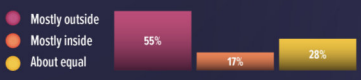


No company is immune to attack. No organization is too large or too small to fall victim to a data breach. [1]

DO YOU FEEL THIS RISK LARGELY ORIGINATES ON THE OUTSIDE OR THE INSIDE OF YOUR ORGANIZATION?

55% BELIEVE THE RISK OF BREACHES COMES MOSTLY FROM EXTERNAL SOURCES

34% of data breaches involve internal actors.[1] It is important that enterprises protect their networks from internal and external attacks. Consider a Zero Trust approach to network security.



ARE YOU TOTALLY CONFIDENT THAT YOU HAVE VISIBILITY INTO ALL THE DEVICES ON YOUR NETWORK?

72% BELIEVE THEY HAVE COMPLETE VISIBILITY INTO ALL DEVICES

Most IT departments do not have complete visibility and are surprised when network scans find large numbers of unknown endpoints. Indeed Gartner reports **61%** of networking professionals had low to no confidence that they knew every device connected to their network. Network security requires visibility.

IF YOU USE IoT, DO YOU TAKE MEASURES TO SECURE THEM?

98% TAKE MEASURES TO SECURE THEIR IoT DEVICES - WITH **49%** USING THE PRE-SET PASSWORDS THE IoT DEVICES COME WITH

Using the pre-set passwords that IoT devices come with is not adequate security. Lists of standard passwords are readily available to hackers. Gartner reports that it takes only 3 minutes to hack an IoT device. The best practice is to enforce strong IoT security, where you deny all traffic to and from the IoT device unless it is to an authorized host and using an authorized protocol or application.

IF YOU USE IoT, ARE YOU AWARE OF ATTEMPTS TO HACK THEM?

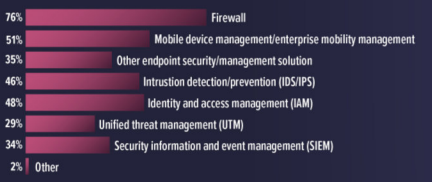
70% OF IoT USERS ARE AWARE OF SUCCESSFUL OR ATTEMPTED HACKS OF THEIR IoT

The rapidly growing population of IoT devices significantly increases the attack surface of networks. Many IoT are relatively easy to hack – simple OS/RTOS do not have strong security features, and often come with no or preset passwords. Many IoT devices are user-less, making it hard to enter network credentials, and stay unsecured.

WHICH OF THESE SECURITY SOLUTIONS DO YOU CURRENTLY HAVE DEPLOYED?

BUSINESS RELY ON A VARIETY OF SECURITY SOLUTIONS TO SECURE THEIR NETWORK

A layered approach to security is essential for hardening network security. Any business investing in network security should ensure that they can integrate seamlessly with their existing security solutions and work with the leading threat intelligence feeds.



WHAT IS/WOULD BE YOUR PREFERRED DEPLOYMENT MODEL FOR A NAC SOLUTION?

70% PREFER CLOUD-BASED NAC; ONLY 28% PREFER ON-PREM DEPLOYMENTS

Cloud-managed NAC has many advantages: it streamlines NAC deployments across sites by centralizing the configuration, management and troubleshooting, and results in unified policies that are consistent across sites. It also reduces the need for on-site intervention and for NAC administrators at each site.

INDUSTRIES

No industry vertical is immune to attack. Security risks are different for every industry: a health clinic bombarded with ransomware attacks has very different needs from a school protecting the online safety and data privacy of its students. Having a sound understanding of the threats your industry face can help prepare you to manage the risks more effectively and efficiently.

INDUSTRIES WHO ARE CONFIDENT THEY HAVE VISIBILITY INTO ALL DEVICES ON THE NETWORK

79% Finance
52% Education

INDUSTRIES WHO FEEL THEIR NETWORKS ARE MOST AT RISK

88% Finance
86% Professional services
84% Healthcare

Similar to security risks being different for every industry so too is the IoT risk. The type of IoT devices and the adoption rate varies per industry. Performing a risk assessment of your IT, OT and IoT environment is essential to level set where your business is at, and to determine your network security goals.

INDUSTRIES AWARE OF IoT HACKS

88% Finance
80% Government
73% Technology

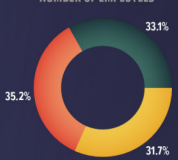
INDUSTRIES MOST LIKELY TO HAVE INCREMENTAL IoT SECURITY (beyond pre-set passwords)

56% Government
56% Manufacturing
55% Education

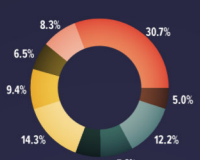
INDUSTRIES AWARE OF SUCCESSFUL IoT HACKS

34% Education
31% Professional services
28% Government

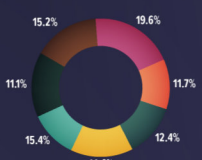
SIZE OF ORGANIZATIONS BY NUMBER OF EMPLOYEES



PARTICIPATING INDUSTRIES



PARTICIPATING COUNTRIES



[1](Verizon 2019 Data Breach Investigative Report)