How companies are leveraging Zero Trust to secure devices

Modern enterprises have an incredible diversity of devices accessing their data. This creates a massive attack surface, and as a result, devices can easily become the weakest link in an organization's security strategy.

Enterprises need more visibility and control into the devices accessing their networks and corporate resources. IT leaders are increasingly utilizing Zero Trust approaches to ensure device health and compliance are verified before granting access to the network and corporate resources. Whether a personally owned BYOD device or a corporate-owned and fully managed device, a Zero Trust approach helps enterprises improve visibility and minimize their attack surface area.

We surveyed IT leaders from across the globe to discover how they're using Zero Trust practices to secure devices and enable safe access to resources.

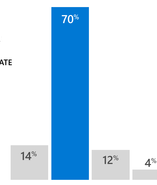
1 THE NUMBER OF PERSONAL DEVICES ACCESSING CORPORATE NETWORKS IS SPIKING

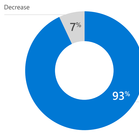
1/4

Due to the pandemic, **86%** of IT leaders say at least a **quarter of their staff** are connecting to corporate networks through personal and shared devices right now.

WHAT PERCENTAGE OF YOUR EMPLOYEES USE PERSONAL DEVICES TO ACCESS CORPORATE RESOURCES AND DATA?

This trend isn't expected to slow down anytime soon. **93%** of companies expect the number of employees using personal devices to increase in the next year.



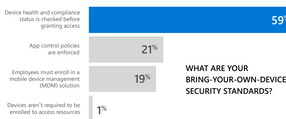


HOW WILL THE NUMBER OF EMPLOYEES BRINGING THEIR OWN DEVICES CHANGE IN THE NEXT YEAR?

Many companies are implementing a Zero Trust security model where devices are monitored for health and compliance before granting access to corporate resources. Gaining visibility into the threat landscape is a vital step on this journey.

On a positive note, **99%** of IT leaders are at least monitoring personal devices for security threats.

However, only **19%** are using a mobile device management (MDM) solution—which is required to enforce critical Zero Trust controls and protections such as preventing users from sharing sensitive corporate data.



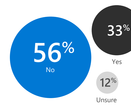
WHAT ARE YOUR BRING-YOUR-OWN-DEVICE SECURITY STANDARDS?

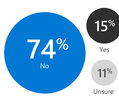
2 DEVICES ARE MONITORED, BUT NOT ALWAYS USED IN ACCESS DECISIONS

87% of respondents say they have visibility into **all user devices** accessing the corporate network.

CAN YOU MONITOR THE HEALTH AND COMPLIANCE STATUS OF PERSONAL DEVICES BEFORE GRANTING ACCESS TO COMPANY RESOURCES?

However only **74%** of companies are monitoring health and compliance statuses **before** granting access.

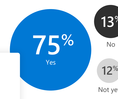




DOES YOUR CURRENT POLICY ALLOW YOU TO MONITOR HEALTH AND COMPLIANCE STATUSES OF EACH PERSONAL DEVICE BEFORE GRANTING IT ACCESS TO COMPANY RESOURCES?

In an effort to protect company resources, most IT teams currently use data loss prevention software to monitor devices accessing the network.

DO YOU USE A DATA LOSS PREVENTION TOOL TO PROTECT COMPANY RESOURCES?



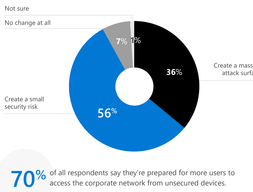
While data loss prevention can protect resources from insider threats, it's a reactive approach—and not enough for a mature Zero Trust model. Adding least privileged access means that data is proactively protected from non-sanctioned use.

3 MOST IT LEADERS AGREE THAT PERSONAL DEVICES ARE INCREASING RISK EXPOSURE

As the use of personal devices increases, IT leaders are concerned with the increase in their attack surface area. Many have proactively prepared for the increase in personal devices or have started altering their strategies.

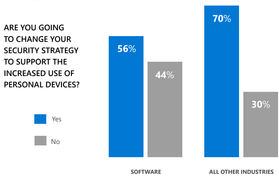
92% of companies agree the proliferation of personal devices will increase their attack surface area

HOW DO YOU THINK THE PROLIFERATION OF PERSONAL DEVICES WILL AFFECT THE SECURITY OF YOUR COMPANY?



70% of all respondents say they're prepared for more users to access the corporate network from unsecured devices.

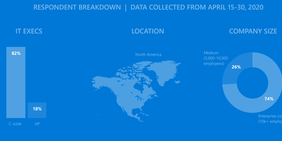
ARE YOU GOING TO CHANGE YOUR SECURITY STRATEGY TO SUPPORT THE INCREASED USE OF PERSONAL DEVICES?



To prevent devices from being the weakest link in your security strategy, you need visibility into the devices accessing your network, and ensure you're only allowing those that are healthy and compliant to access corporate resources.

Learn how Microsoft Endpoint Manager provides a comprehensive suite of tools to help you manage and monitor mobile devices, desktop computers, virtual machines, embedded devices, servers, and more.

RESPONDENT BREAKDOWN | DATA COLLECTED FROM APRIL 15-30, 2020



Insights powered by PULSE

Microsoft