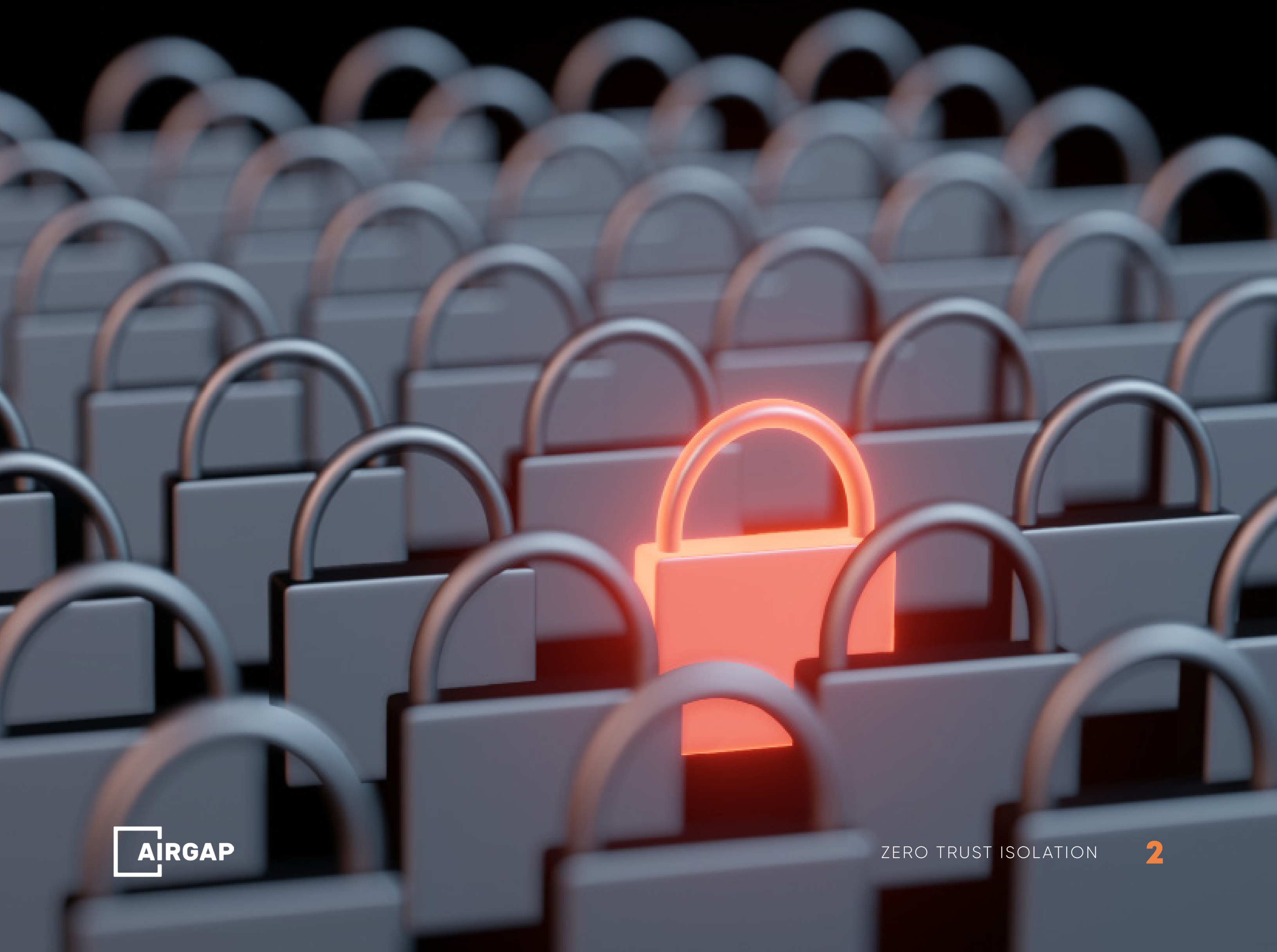
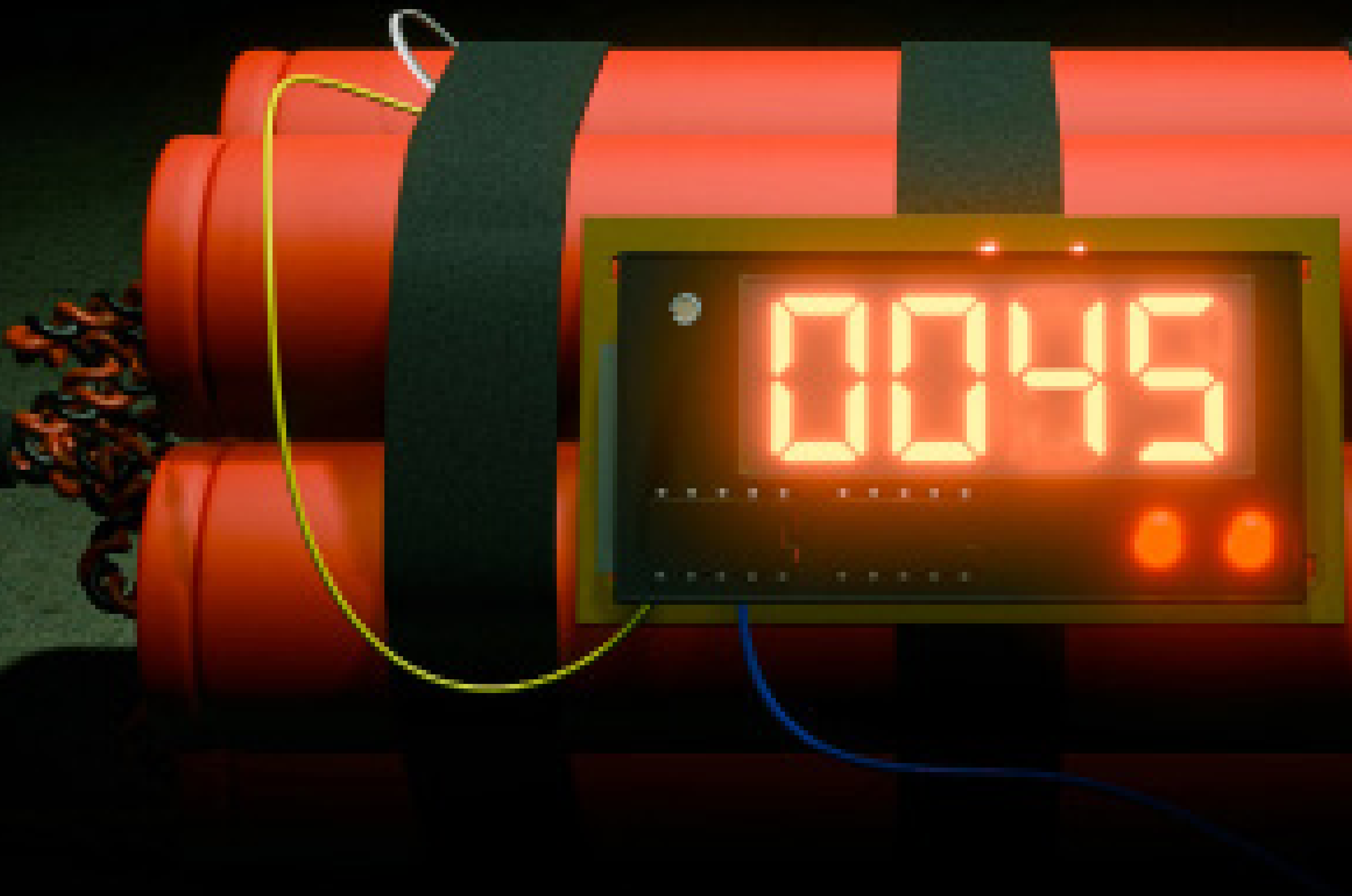
AIRGAP

Zero Trust Isolation

The best defense against Ransomware propagation

Once your perimeter is breached, what can happen?





You have 45 seconds!

Once inside, the bad actors can propagate laterally over shared networks (VLANs). There is no easy way to contain lateral threat propagation across all IPs & ports

What if you have unpatched business applications?

Bad actors already inside your organization can exploit vulnerable application stack

Traditional Firewalls have static access control policies. Devices on certain VLANs, Zones, or IP/Subnets have always ON access to corporate assets and any vulnerability in any of the application stack can be exploited.

What if there are legacy and insecure protocols running inside your organization?

Bad actors already inside your organization can **exploit insecure legacy protocols**

Github hosts ready made tools and tutorials on how to compromise insecure protocols

Click here to learn more

What if your enterprise depends on **IoTs for mission critical operations?**

A 2020 Business Insider Intelligence research report predicts there will be more than **41 billion Internet of Things (IoT) devices by 2027**, up from about 8 billion in 2019.

IoTs are the weakest link in the organization

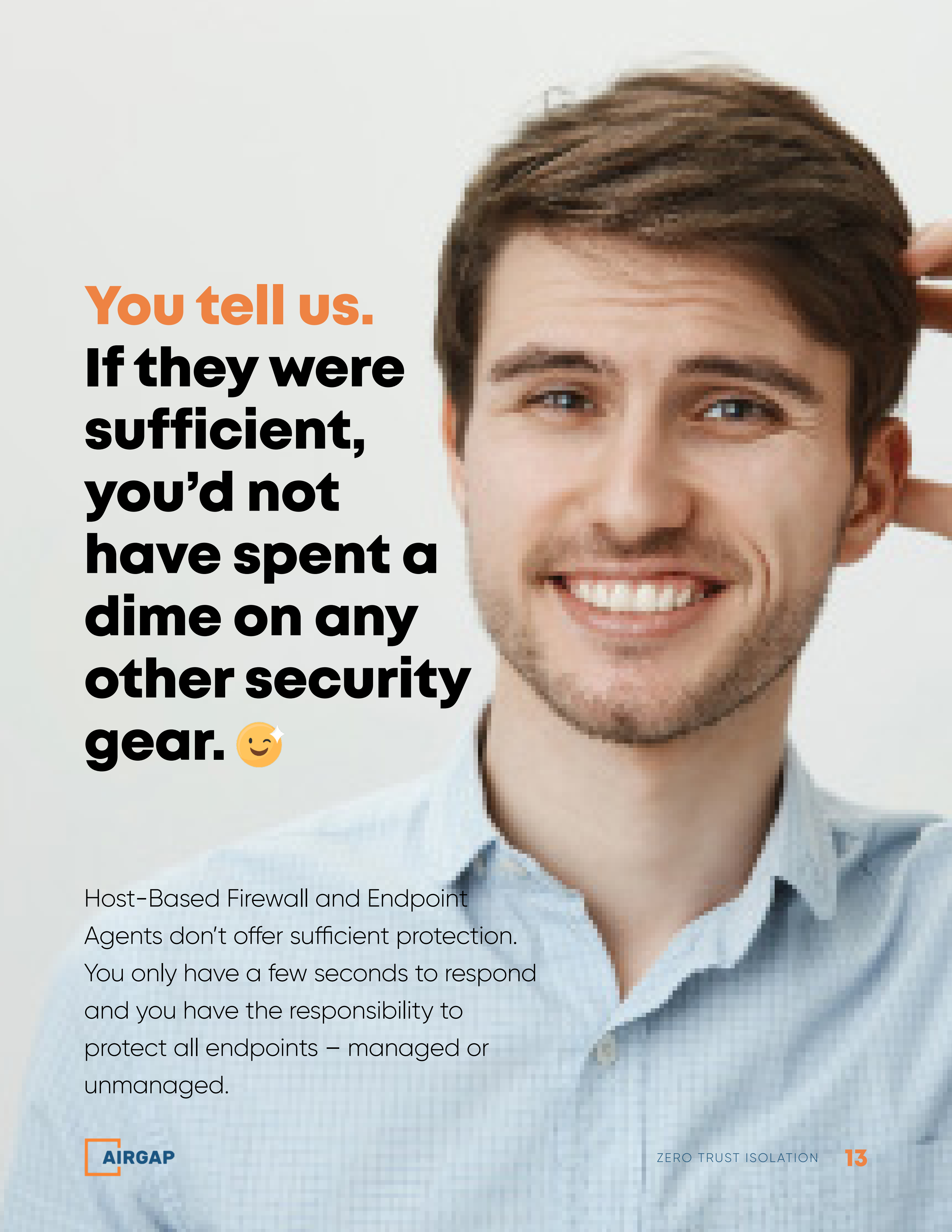
Vulnerable black-box OS, weak passwords, lack of strong encryption, and much more. Cyber-criminals often exploit these weaknesses to gain access to corporate crown jewels.

Are there increased risks associated with employees “working-from-home”?

Glad you asked.

Corporate laptops can be breached in insecure settings such as home or public hotspots and subsequently used as a launchpad to gain access into corporate network via VPN. Once the bad actors are inside your network, you know what happens next.

Isn’t end point protection solution sufficient?



You tell us. If they were sufficient, you'd not have spent a dime on any other security gear. 😉

Host-Based Firewall and Endpoint Agents don't offer sufficient protection. You only have a few seconds to respond and you have the responsibility to protect all endpoints – managed or unmanaged.

We add new security gear every year. We must have sufficient protection, no?

Traditional security solutions aren’t sufficient

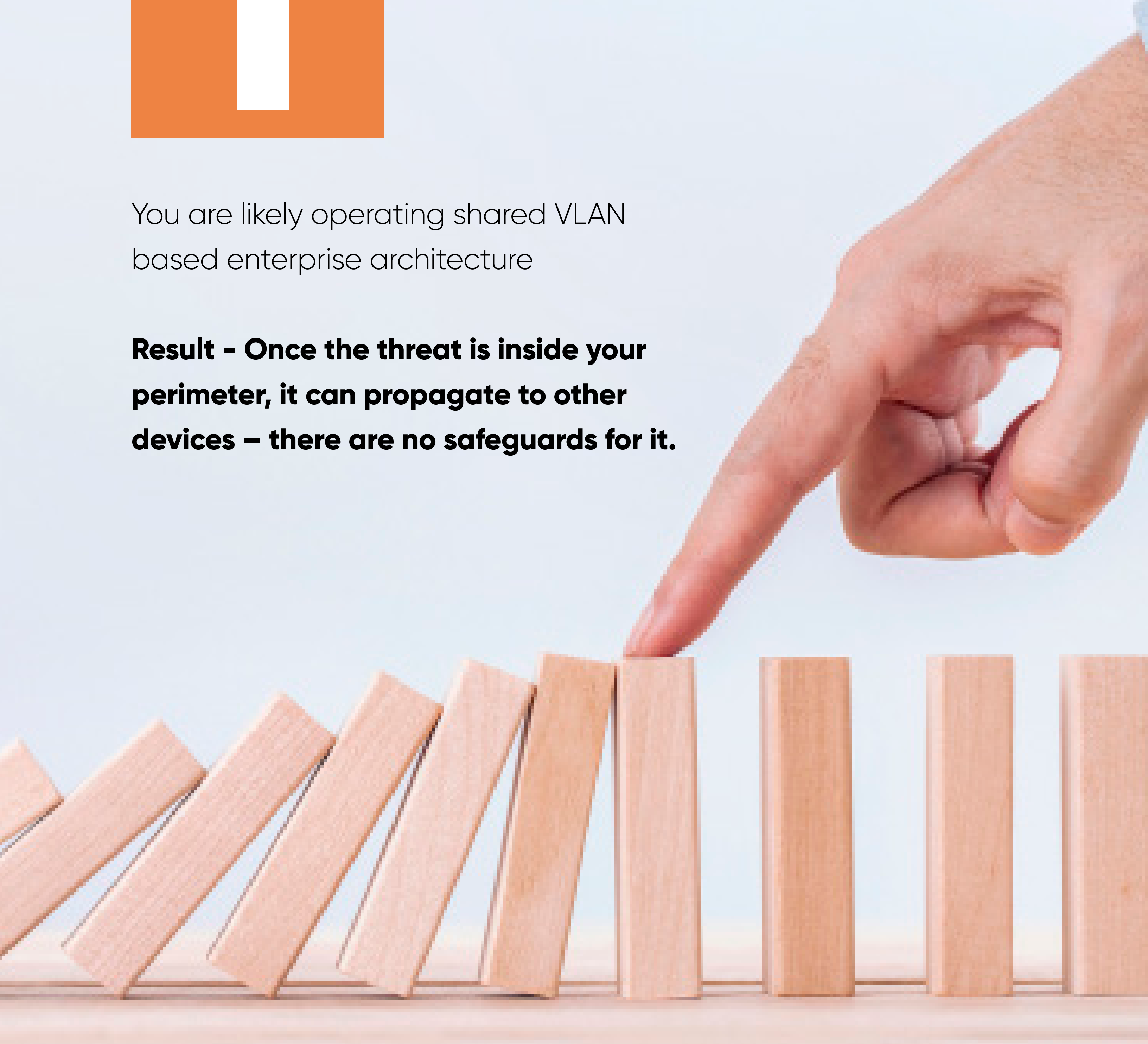
According to Forbes, **51% of the organizations** have been a **victim of Ransomware attack** in the last 12 months

Why aren't current security solutions sufficient?

1

You are likely operating shared VLAN based enterprise architecture

Result - Once the threat is inside your perimeter, it can propagate to other devices – there are no safeguards for it.



2

Your bank doesn’t offer you network access for using their application. So, why does your network firewall & VPN provide your employees, contractors, and partners network level access to your business application?

Result - Once the threat is inside your perimeter, it can propagate to your business applications – there are no safeguards for it.

3

You have some legacy insecure protocols such as Kerberos or Windows File Share operational inside your organization

Result - Once the threat is inside your perimeter, it can exploit legacy protocols – there are no safeguards for it.

Time to think different.

“**Insanity:** Doing the same thing over and over again and expecting different results.”

- Albert Einstein

Zero Trust Isolation

The best defense against Ransomware propagation

1

Eliminate lateral threat propagation

Don’t let one infected device bring down the enterprise. Continue to operate Shared VLAN infrastructure without the risks.

2 Prevent application & data breaches

Eliminate network level access to prevent ransomware from propagating to your business applications. For additional security, seamlessly enable 2FA across the enterprise

3

Safeguard against legacy protocol vulnerabilities

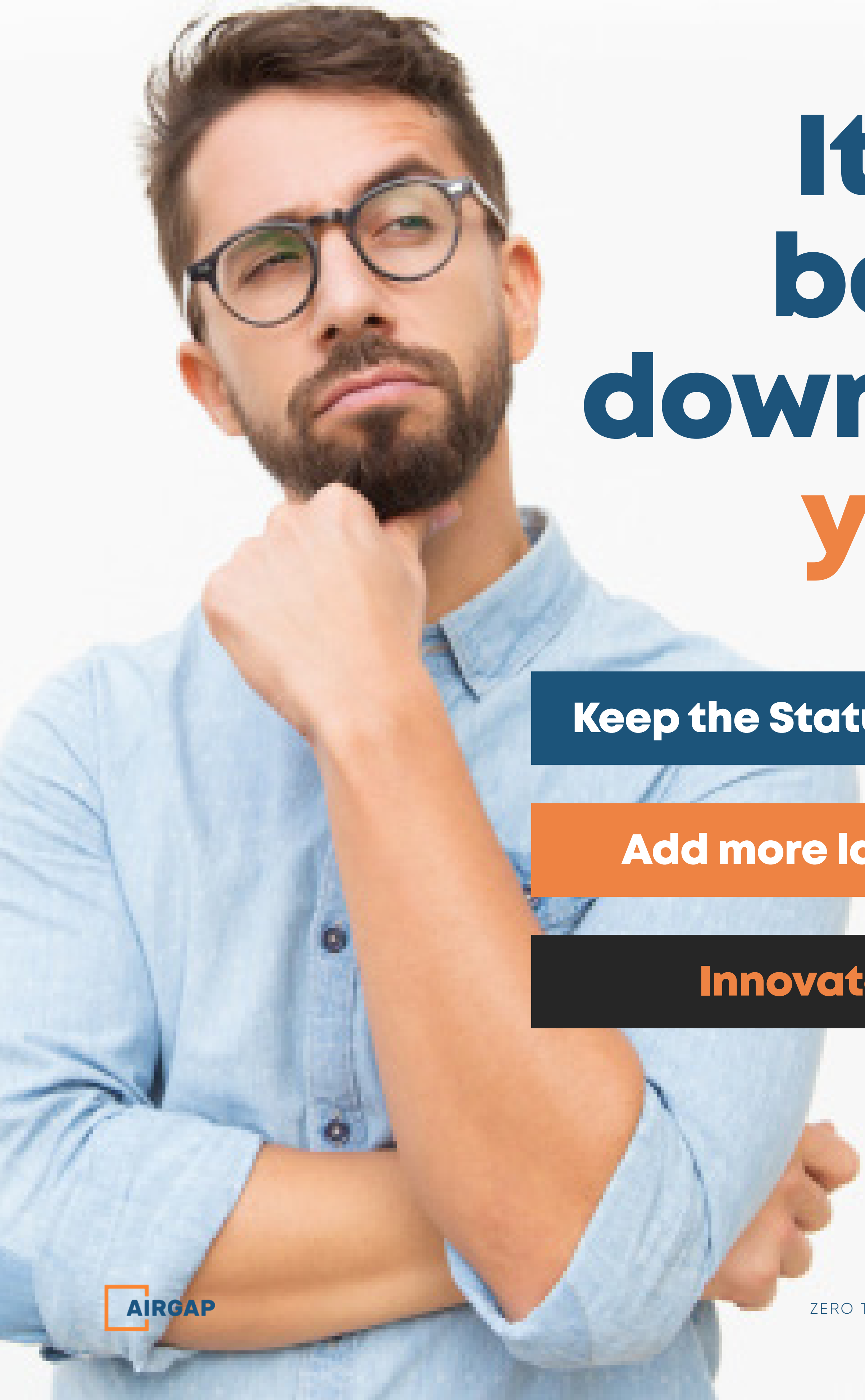
Continue to operate your infrastructure without design changes knowing that we have got your back.

4

Deploy in minutes. Not months.

No Agents, APIs, design changes
or forklift upgrades.

Your business is your business – migrate
to Airgap at your convenience – one user,
devices, network, or application at a time.



It all boils down to you!

Keep the Status-Quo!

Add more layers.

Innovate!

Zero Trust Isolation

Contain Ransomware to
a single device

What would you do if you are hit with ransomware?

Ransomware Kill Switch

RANSOMWARE PROPAGATION STOPS HERE.

The most potent ransomware response for any IT organization

AIRGAP

airgap.io

Aug 2020, v4