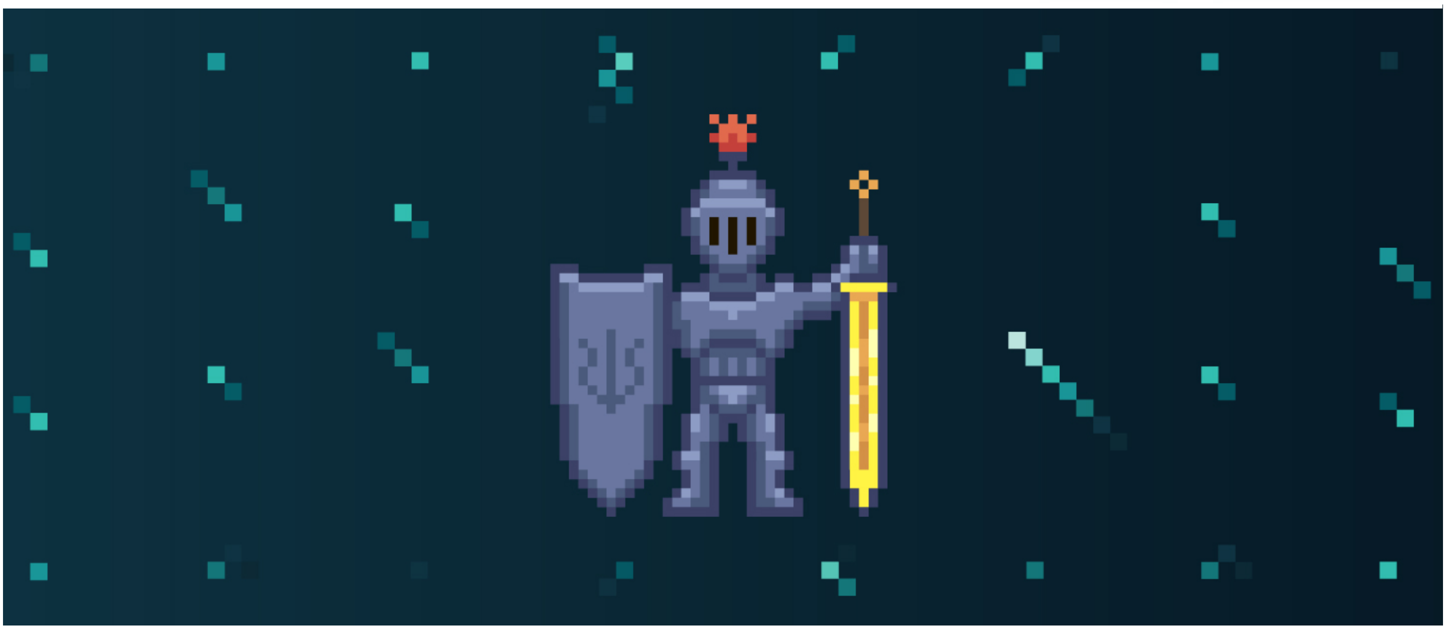


BACK TO BLOG

# How to build a resilient remote-working business

James Harrison

August 17, 2023

Whether business owners like it or not, remote working is here to stay. About 42% of workers already work a remote or hybrid schedule, according to a Gallup study. Some head into the office for team meetings and face-to-face collaboration, but many work from home all week – wherever that may be – allowing for a truly global and dispersed workforce. We all know the pros and cons by now, but here we're going to focus on one downside in particular: it's harder to manage, monitor and secure IT.

Laptops and smartphones blur the lines between work and organization's security. So let's look into the risks of remote working – and what you can do to reduce them.

## How does remote working impact cybersecurity?

The shift to remote work was well underway before the pandemic, but IT teams had to work round the clock to enable employees to stay connected, collaborate and productive when COVID hit – by whatever means possible.

The first priority was to maintain business continuity, and security often took a back seat – opening businesses to a host of potential security vulnerabilities. Many relied on tried and trusted remote access solutions like VPNs; some invested in virtualization and DaaS services; others ignored security altogether and fell back on old, unpatched legacy equipment. The result? Their attack surface expanded exponentially and left them dangerously exposed.

## What are the common risks of remote working?

- **Phishing:** where attackers send fraudulent emails or messages to trick users into revealing sensitive information or download malware
- **Unsecured networks:** when employees use public Wi-Fi networks without a VPN, it can open the door to cybercriminals to intercept sensitive information
- **Personal devices:** when employees use their own devices for work, they may not have the sanctioned apps or security measures in place to protect sensitive data
- **Video conferencing:** many of the platforms rolled out and adopted during the pandemic had significant software flaws

## What's wrong with relying on a VPN?

Many relied on tried and trusted VPNs to connect their teams

VPN’s themselves aren’t the problem, but they can only handle so much traffic. With the massive increase in traffic with everyone working from home, many fell back on the "split tunnel" configuration of their VPN clients.

This meant traffic went through the VPN to connect to the company network, but when they searched Google, checked LinkedIn or streamed YouTube, traffic would bypass the VPN and use the employee’s home network instead. This one single configuration change meant businesses no longer had control over what their employees could connect to, download or access. But what did this mean in practice?

## Experience: existing technology (mis)handles new requirements

**By Product Lead, Andy Hornegold**

When systems/workstations are contained within an internal network you can restrict what those systems can connect to – everything crosses your businesses internet boundary. For example, you can stop connections to the internet over the file share functionality embedded in Windows (SMB). Almost every organization will restrict access from their internal network to the internet using SMB – there are very few use cases where it’s a good idea to allow it.

When people started working from home, many used laptops with a VPN to connect to and sent traffic via the business's network. This meant that every time the laptop tried to connect to a business system, the traffic would go via the VPN to the business network; but every time they connected to a non-business system the traffic would connect over the user’s home network. With this one configuration change, the business now no longer controls what the laptops can connect to and security has become a little more porous.

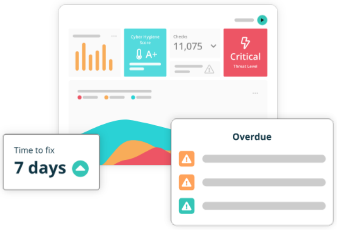
I was running red teams when this was happening. We phished a user and accessed a single laptop with endpoint security. It had a VPN into the company network which was locked down, but the VPN was running in split-tunnel mode so the laptop could connect to the internet. We couldn’t do much without being detected, but we could look through

We dropped a simple .url file in a directory on the company file share, and it was a directory used by all employees. When you browse your filesystem and come across a .url, Windows Explorer will try and show an icon for that file, and the location of the icon is specified within the .url file itself. We specified that the icon was stored on an internet server which we controlled.

Now, every time an employee browsed to that file share, their Windows OS would send a request to our server for the icon so that it can display in Explorer. When our server asked the victim's Windows OS to authenticate in order the retrieve the icon, it sent the hashed credentials of the victim user to us. We could crack those hashes and use them to access other internal systems and internet-facing systems with the same credentials.

The universal advice for this issue is to "block SMB connections to the internet at your firewall". But this doesn't work when people are working from home, because the connection doesn't come from the business network. We exploited this daily to hoover up credentials from users across the business.

This is a really simple technique, and it shows how businesses risk profiles have fundamentally changed because of the new ways of working.



This shows how a single configuration change can mean that IT teams no longer have control and visibility of what their people are using and connecting to. And if you can only get security updates when physically in the office, your team won't get them while working from home.

If your threat detection software is network-based, it's ineffective when no one is actually on the office network. This might be manageable when your team is hybrid and comes into the office once a week, but not when they're fully remote. And unpatched software is one of the most common breaches.

This is why zero-trust is so prevalent today. With zero trust, there are no boundaries and no perimeter. No one is inherently trusted. Everything is compartmentalized, and there is security in isolation. While it's more restrictive, the benefit is that it creates a far more secure environment that provides better protection against unauthorized access.

## So what makes a resilient business?

Ask yourself – what if? What if you're hacked and lose control of your systems and data? How will it impact your business? Would you lose your customers? Would you lose your reputation? Could you be hit with a fine? If the answer is yes to any of these, then it's time to take your cybersecurity more seriously.

It's natural that smaller businesses focus more on their bottom line than potential risks. But there are simple measures you can put in place now to safeguard your systems – whatever the size of your business. Vulnerability management, multi-factor authentication on every login, backing up your data, and using a password manager – these are just some of the basics that every business – however big or small – should put in place.

But it's also important to understand that even with these precautions and a zero trust approach, you can still fall victim to hackers. That's why you need to prepare for the worst and make sure you have a robust risk management and business continuity plan in place. Put simply, will your business survive if you're hacked? If not, how could you be more resilient?

There’s no single definition of what makes a resilient business. It depends on what type of organisation you are, how fast you’re growing and scaling, what industry you’re operating in, who you're trying to keep out, and what scenarios you want to resist. For example, healthcare and financial services providers need robust cyber security because they hold sensitive customer data and both industries are tightly regulated.

But even in these scenarios, ‘absolute resilience’ is almost impossible and probably not worth the time, effort and expense. A more realistic approach is to aim for what you are willing to accept as a business. Choose what resilience looks like to you, and you can reach this ‘relative resilience’ with a few simple tips.

## 9 top tips to become more resilient

1. Don’t work on personal devices
2. Don’t download unapproved software
3. Keep your software updated
4. Secure remote access with a VPN
5. Secure sensitive data stores and ensure they’re backed up frequently
6. Monitor your network to see what's exposed to the internet
7. Regularly check for vulnerabilities and fix them promptly
8. Implement Multi-Factor Authentication (MFA) everywhere
9. Train your team to follow cyber security best practices

## How Intruder can help boost your resilience

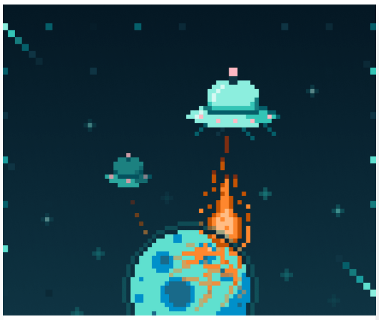
While these steps are easy to implement, keeping track of all activity on your network and changes to your cloud accounts isn't a walk in the park. But there are automated tools and solutions that can make it much easier.

Intruder continuously scans your network so you can see where you're vulnerable. It shows you what's exposed to the internet, and prioritizes issues so you can focus on fixing the most important ones first. Plus, any time it sees a change, such as an emerging threat, new cloud asset or an exposed service, it'll kick off a new scan for you.

This means you have visibility and control over your attack surface, you'll be notified of any changes to your IT environment such as open ports, and automatically synchronize hostnames or IPs. ***Put it through its paces with a free trial and make your organization as secure and resilient as it can be.***

Written by James Harrison

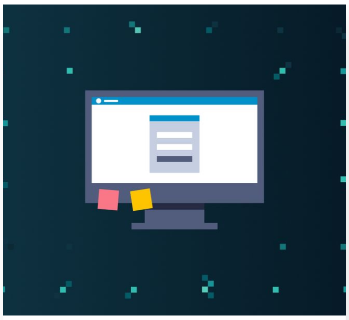
## Recommended articles



### Attack surface management: Find your assets before the hackers do

Find out how Daniel Thatcher demonstrated the importance of attack surface management to delegates at DTX Europe.

Daniel Thatcher October 18, 2023



### Single page applications: Why do you need to scan them?

Learn about single page applications, how they are different to mulit-page applications, why it's important to scan them for vulnerabilities, and how we scan them.

Charlie Fleetham January 24, 2024

### Gotta catch em all: Bug hunting explained

Eliminate visibility gaps and make issues actionable for your security and dev team.

James Harrison September 12, 2023

## Ready to get started with your 14-day trial?

TRY FOR FREE

intruder

SOLUTIONS

Developers

Start-ups and scale-ups

Enterprise

COMPARISONS

Intruder vs Acunetix

Intruder vs Qualys

Intruder vs Rapid7

Intruder vs Netsparker (Invicti)

Intruder vs Detectify

Intruder vs Pentest-Tools.com

USE CASES

Automated Penetration Testing

Cloud Vulnerability Scanner

Network Vulnerability Scanner

External Vulnerability Scanner

Internal Vulnerability Scanner

Website Security Scanner

COMPLIANCE

SOC 2

ISO 27001

PCI DSS

RESOURCES

Developer Hub

Help Centre

Blog

Guides

Glossary

Success Stories

Research

Webinars

COMPANY

About Us

Contact

Become a Partner

Careers (We're hiring!)

Protected by intruder

Contact us

Privacy Policy Terms of Service Status Security Sitemap

Registered in England, VAT Number GB228985360. Intruder is a trading name of Intruder Systems Ltd, Company Registration Number 09529593.