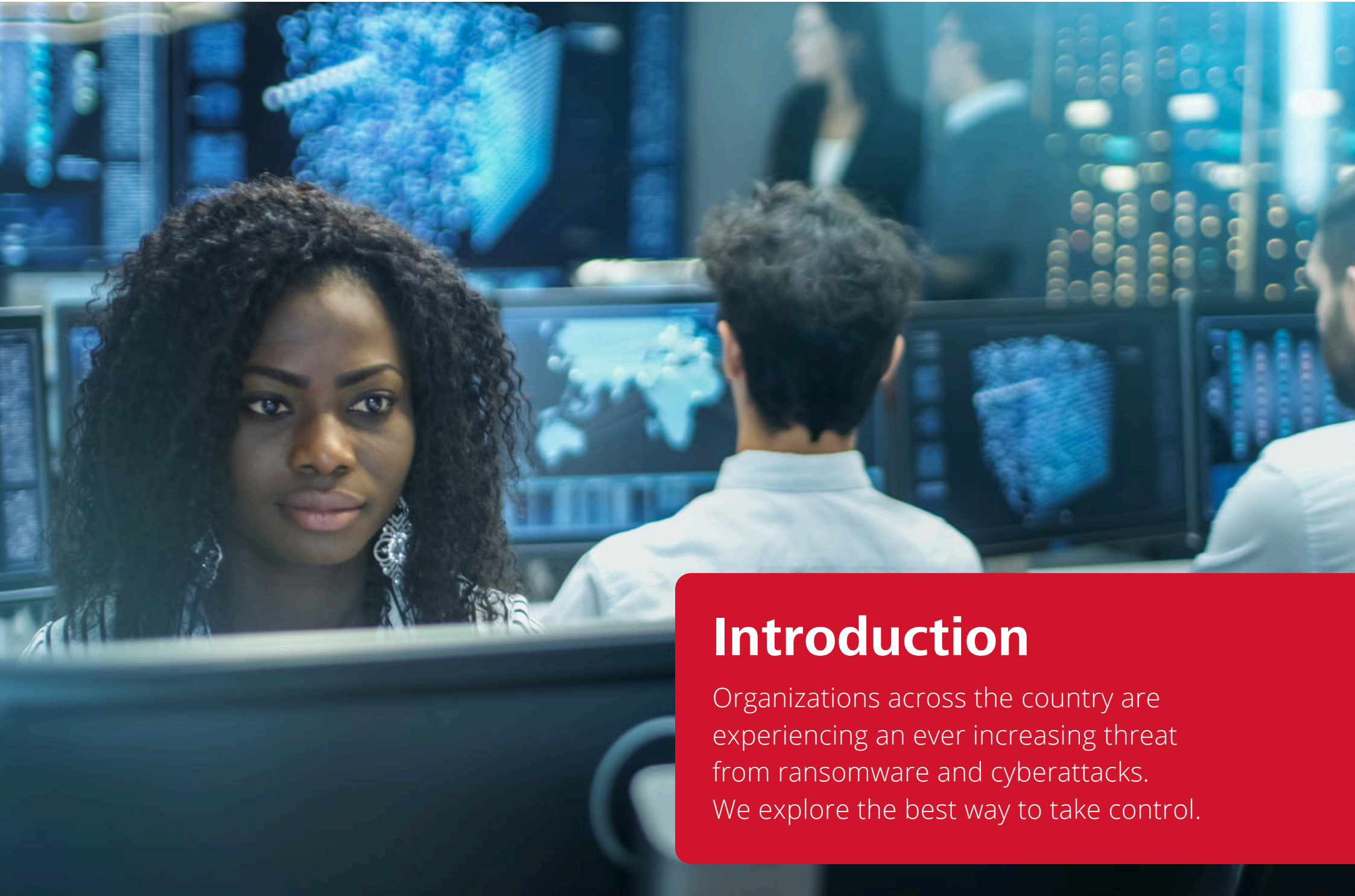
RICOH
imagine. change.

Ransomware, Containment and Isolation

Your Proactive Defense Against Ransomware



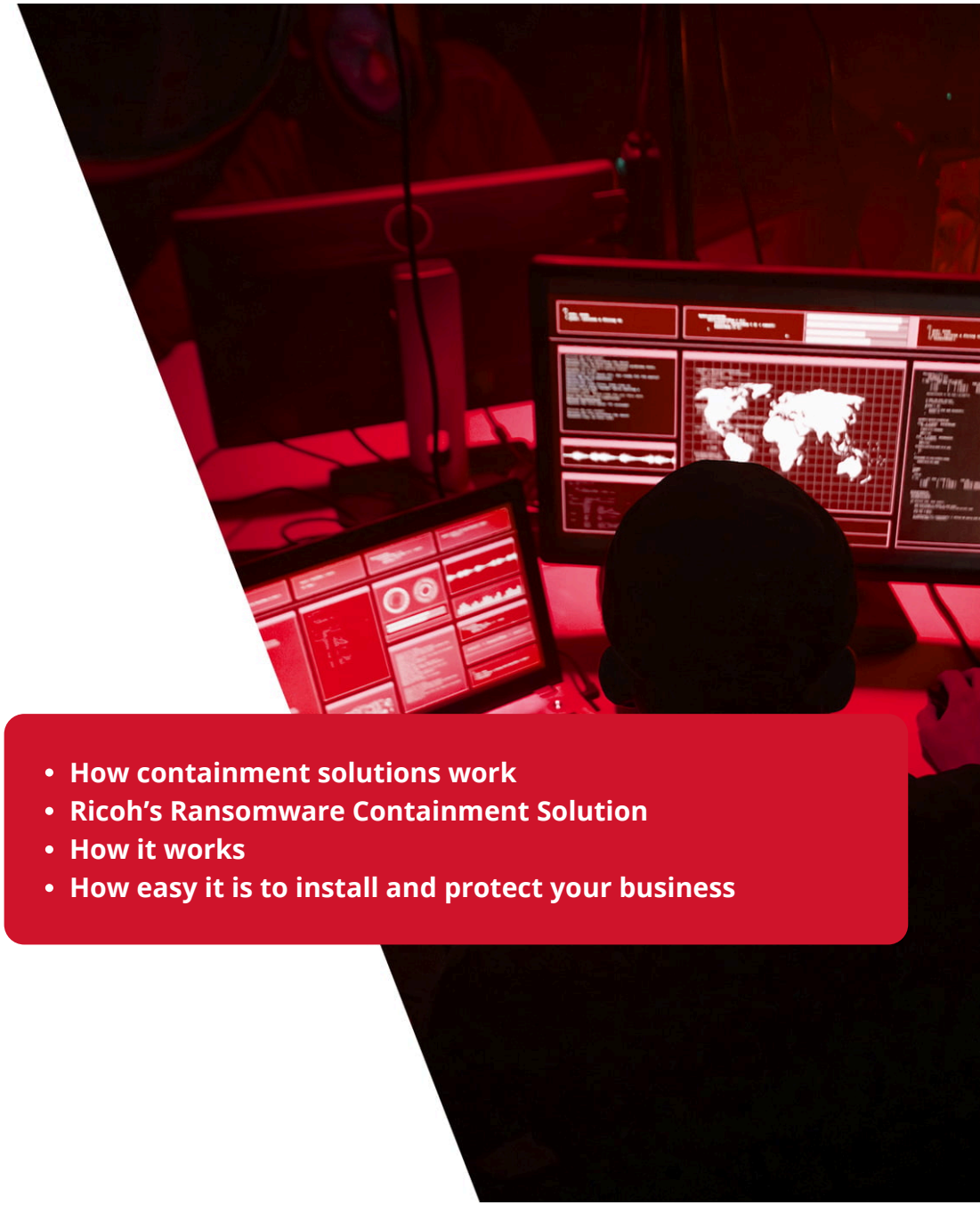
Introduction

Organizations across the country are experiencing an ever increasing threat from ransomware and cyberattacks. We explore the best way to take control.

Introduction

With ransomware attacks on organizations increasing 7-fold between the first and second half of 2020, it's getting ever more important for public and private organizations to prepare themselves for tomorrow, not for yesterday.

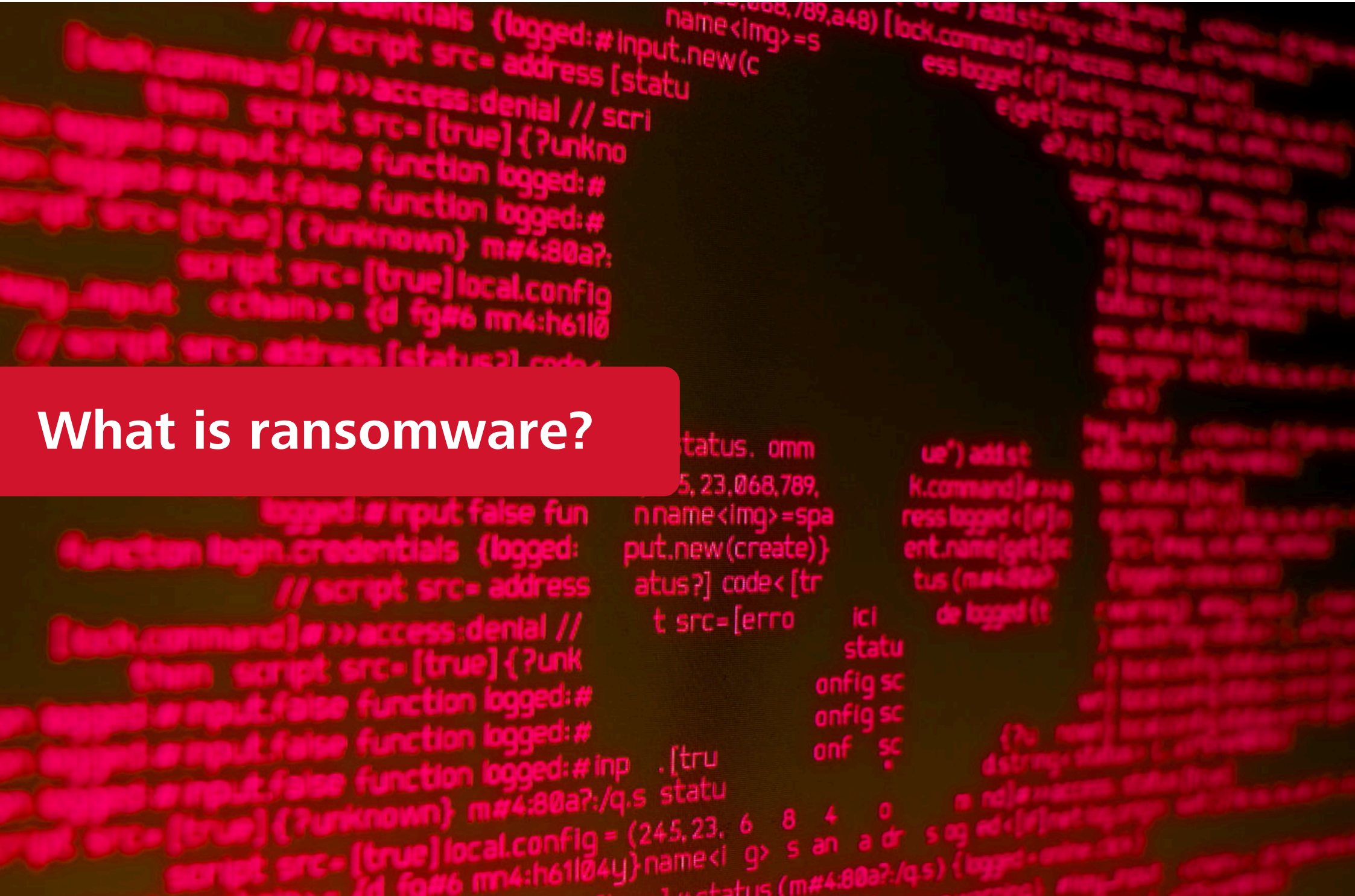
Ransomware attacks are getting smarter. As technology evolves and our work environments become more agile and complex, the current perimeter-based defenses we have to protect our digital infrastructure are quickly falling behind. In this guide we'll discuss what we're up against, and the best way to fight back.



What you'll learn in this guide

- **What is ransomware?**
- **How would an attack affect your business?**
- **Real-world examples**
- **Perimeter-based defenses vs 'Detect & Contain'**
- **How containment solutions work**
- **Ricoh's Ransomware Containment Solution**
- **How it works**
- **How easy it is to install and protect your business**

*Source : FortiGuard Labs Threat Report



What is ransomware?

What is ransomware?

Ransomware is a malicious software, which financially motivated criminals use to attack your data.

If they successfully infiltrate your system, the ransomware begins to encrypt files so you can no longer access them. This process doesn't alter the file names, so it is hard to see which files have been corrupted and which haven't. 4% of data lost in an attack is unrecoverable.*

They then hold this information hostage, demanding payment for its return. The average cost of a ransom in Q4 of 2020 was $154,108

Many leading antivirus software solutions are unable to detect new variants of ransomware for up to 4 weeks.

And with attacks corrupting up to 10,000 files per minute, the consequences can be disastrous.

*Source: TechTarget

How does an attack affect your business?

If a ransomware attack takes hold of your data, they will demand money.

This leads to a very difficult problem – do you pay up? This might avoid reputational damage, but it will fund further attacks and in all likelihood the attackers won't relent.

Or do you refuse? This will mean spending a fortune on new equipment, disruption of your everyday activity and may affect how people see your business.

There is a third option. Take the fight to ransomware before you get attacked by installing a containment-based solution.

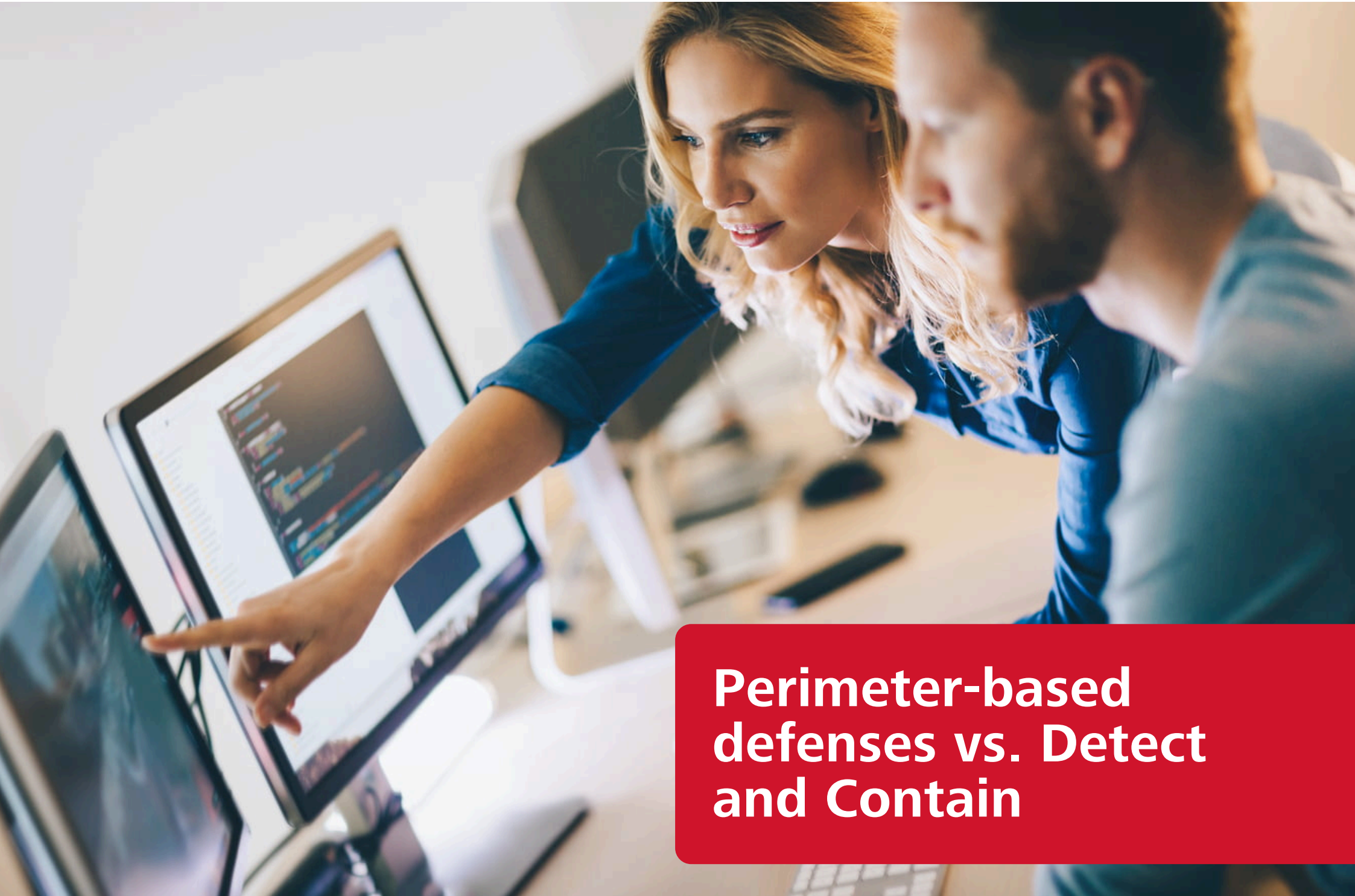
How have other businesses been affected?

Some recent well documented examples:

Eurofins.
Eurofins Scientific – the UK's biggest forensic services provider – was also hit by an attack in 2019. This highly-sophisticated strain of malicious software-led British police to suspend work within the company, as a massive backlog of 20,000 samples was built up.

Travelex.
More recently was the cyber-attack on Travelex. The initial attack cost over $200 million and shut the entire network down for 14 days before they could get their systems back online. They further went on to lose over $47 million in revenue, took a huge hit to their reputation and in turn affected their global partners such as HSBC.

RICOH
imagine. change.



Perimeter-based defenses vs. Detect and Contain

Perimeter-based defenses vs. Detect and Contain

Businesses traditionally enclose all of their data and devices within a perimeter, comprised of a combination of firewall, email scanners and web filtering solutions.

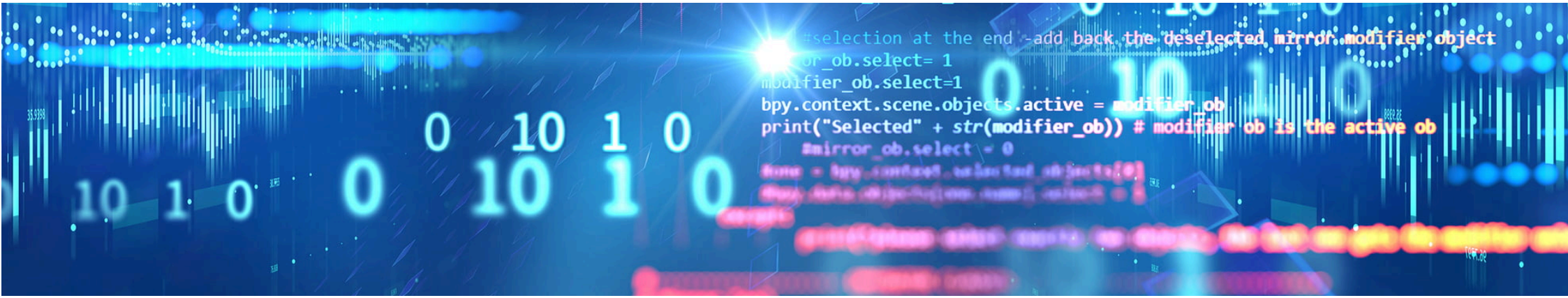
This screens everything that comes into the network, then blocks or removes anything that is flagged as malicious. The business should then be able to trust that it will keep out invaders and that all activity within it is safe. But this is no longer the case.

Today's business consists of multiple endpoints, often managed by public cloud providers, and employees accessing their organization off site. This means that malicious activity has more chances than ever to break in.

If your system is infiltrated, you need a proactive solution to defend it.

Our human immune system is a great metaphor for this: if we're unlucky enough to fall ill, our white blood cells rush to the rescue and fight off the infection.

This, broadly speaking, is how a containment-based defense system works for your business. It supplements your firewall by quickly identifying and containing ransomware attacks, stopping it from spreading and highlighting affected files for easy recovery.



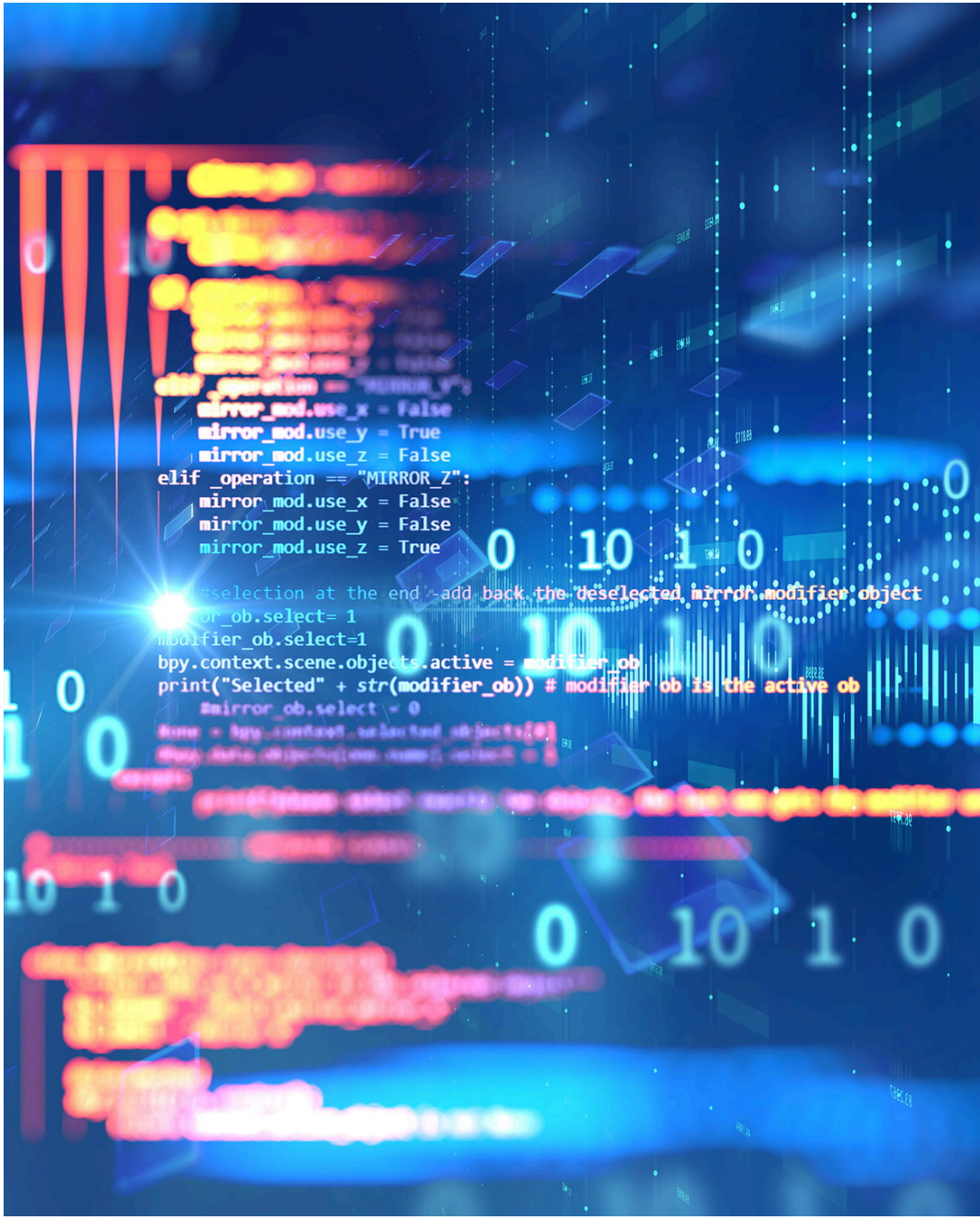
How containment works

Containment solutions are designed to put you on the front foot.

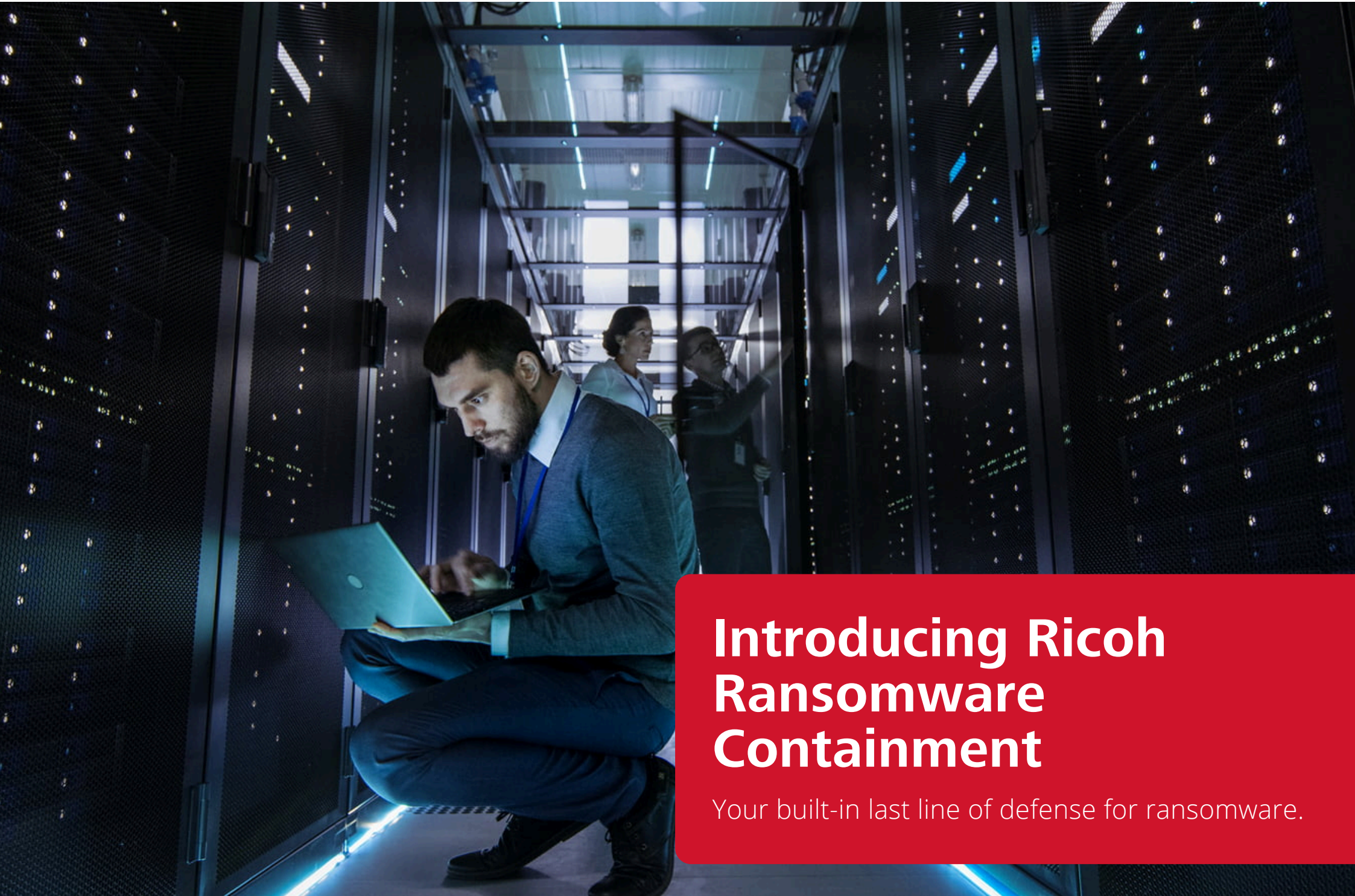
By attacking any viruses that manage to break through your perimeter defense, containment will ensure they don't take hold in your system.

They use built-in scripts to hunt down and contain any intrusion, locking down any files and devices that have been infected.

The most effective products currently on the market are military graded which offer both managers and IT teams the very highest level of confidence against ransomware and cybercrime.



RICOH
imagine. change.



Introducing Ricoh Ransomware Containment

Your built-in last line of defense for ransomware.

Introducing Ricoh Ransomware Containment

A military-graded containment solution.

Current responses by perimeter-based solutions systems are confused and limited. Victimized businesses can't trace the source of the damage, and infection is most often eventually identified by an employee, but far too late.

2020 Cyber Security Breach Survey

Ricoh's Ransomware Containment Solution – a military-graded containment solution – provides an automated technology that reacts in seconds, as soon as the virus infiltrates your system. So only a single device or file is affected.

How does Ricoh's Ransomware Containment Solution work?

Here are just some of the key features offered by Ricoh's Ransomware Containment Solution.

1. DETECT

Detailed live visibility with playback.

All activity is displayed on a dashboard in real time, and you can witness the near-immediate response to any attack as it happens.

2. REACT

Stop attacks within seconds.

Our solution will react within seconds of any unexpected file encryption taking place. It will also notify those who need to know.

3. RESPOND

Keep your business running smoothly.

The speed of response allows our containment solution to prevent the spread of the attack beyond a single user – keeping things business as usual.

4. RECOVER

Take the pressure off your operational teams.

An exact list is compiled of the few affected files before the single user's forced shutdown, making it easier to recover documents.

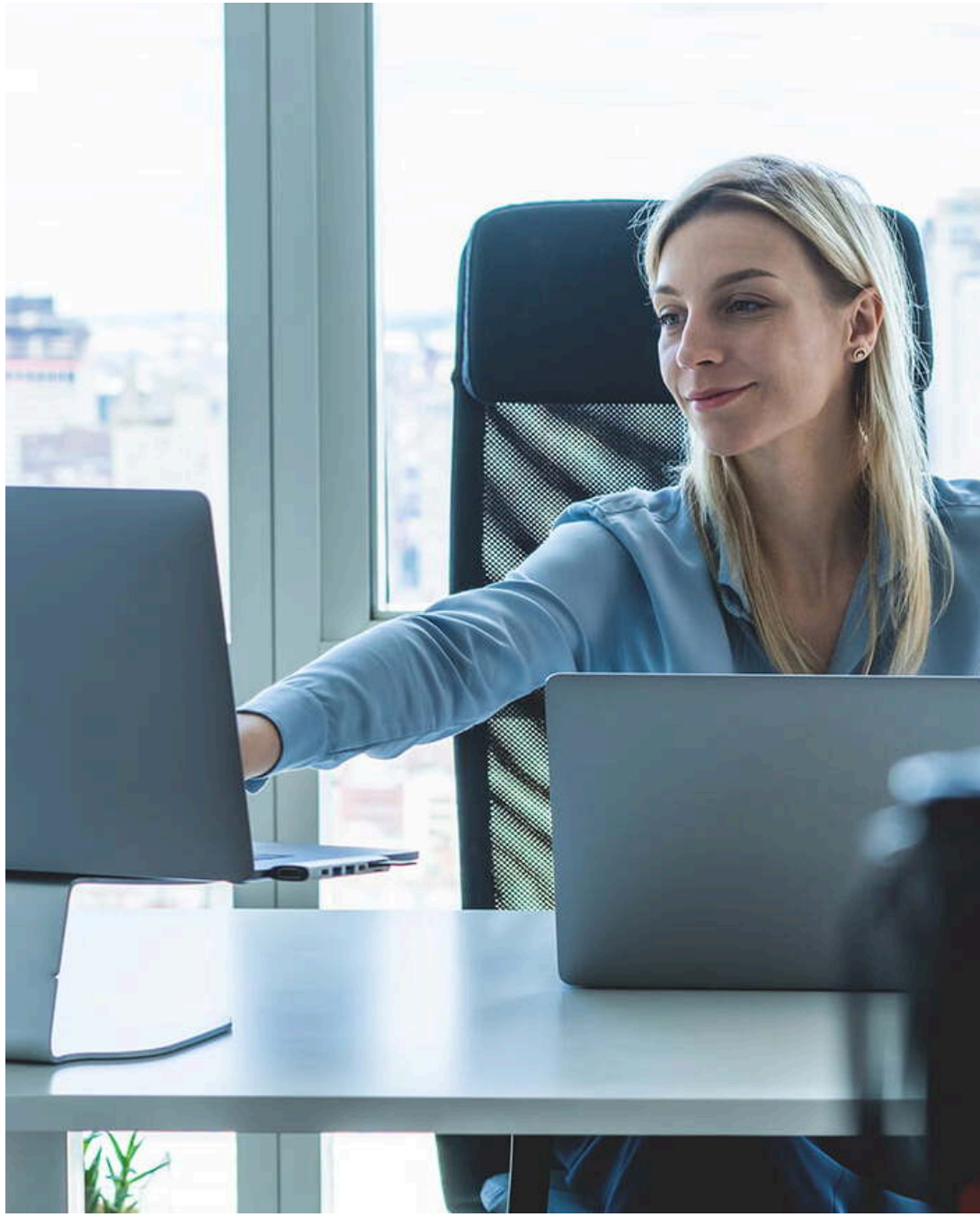
Installation made quick and easy

As little as four hours to be installed.

Not only is taking the proactive approach the best way to defend against ransomware attacks, it's easy to implement too.

Containment solutions can take as little as four hours to be installed, and it can usually be done remotely – meaning minimal disruption to your teams and business.

It isn't installed on any endpoints, or any of your existing files or servers. This means that there is no impact on your infrastructure or network performance. Meanwhile, settings are configured automatically using learning techniques that tailor to your business' activity.



Put Ricoh's Ransomware Containment Solution to the test

Try it for yourself

There's an easy way for us to demonstrate just how effective our technology is – we offer a free and detailed proof-of-value ransomware assessment.

Your IT and leadership teams will be able to test our technology safely through the introduction of an imitation ransomware attack.

Our software will see it as an attack and show you first-hand just how quickly and effectively your system will prevent it from spreading, as well as the series of protocols that follow afterwards for total peace and mind and a detailed overview of activity.

Simply get in touch with our team to arrange your free assessment.

RICOH
imagine. change.

Thank you for reading this report on

Ricoh Ransomware Containment and Isolation

If you have any questions,
please don't hesitate to get in touch.
Click here.

ricoh.ca/itservices