RICOH
imagine. change.

Ransomware, Containment and Isolation

Your Proactive Defence Against Ransomware

Introduction

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

Introduction

In the first half of 2021, the global number of ransomware attacks increased by 151%, and Canada often ranked among the top countries targeted.[1]

When organizations move to a hybrid work model, technology becomes more complex to manage and traditional, perimeter-based defences are no longer adequate. Breaches are happening, even with endpoint protection in place.

To stay ahead of ransomware, organizations must evolve their security strategy from prevention to include risk mitigation. Let's explore how ransomware isolation and containment can protect your business with minimal disruption, at just a fraction of you security budget.

- **Assessing the threat**
- **Perimeter-based defences vs 'Detect and Contain'**
- **How containment solutions work**

- **Ricoh's ransomware containment solution**
- **How it works**
- **Easy installation, instant protection**

[1] "Cyber Threat Bulletin: The Ransomware Threat in 2021" - Canadian Centre for Cyber Security

Assessing the threat

Malicious attackers are constantly innovating new and novel methods to defeat traditional, prevention-based detection methods.

Ransomware is insidious, quietly infiltrating networks for days or weeks before it strikes.

Many leading antivirus software solutions are unable to detect new variants of ransomware for up to **4 weeks.** In most cases, it goes undetected until files are encrypted and the ransom demand is made.

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

RICOH
imagine. change.

Perimeter-based defences vs. detect and contain

Perimeter-based defences 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 defence 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.

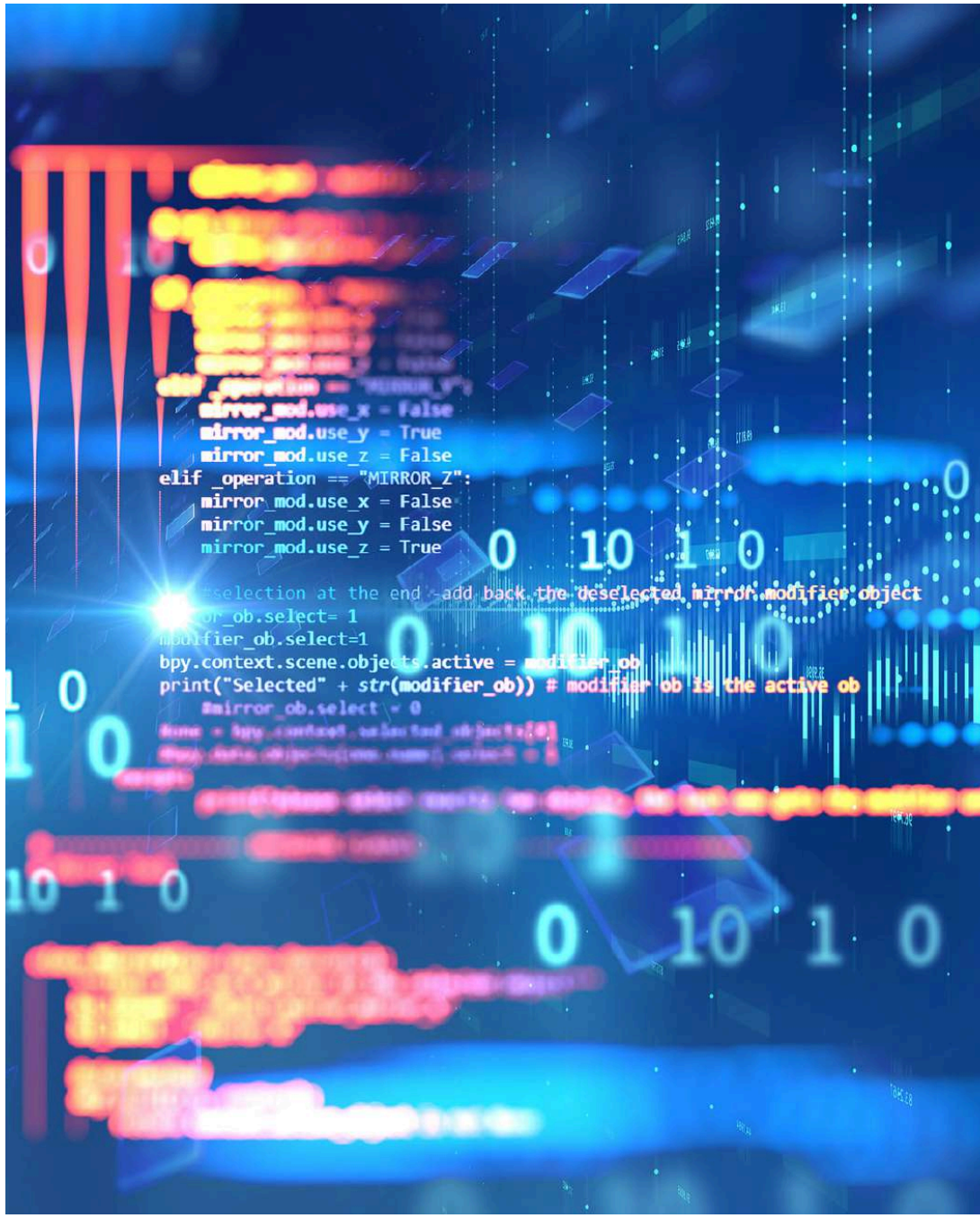
How containment works

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

By attacking any viruses that manage to break through your perimeter defence, 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 the user account and any files that have been infected.

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



RICOH
imagine. change.

Introducing Ricoh ransomware containment

Your built-in last line of defence for ransomware.

Introducing Ricoh ransomware containment

A military-grade 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.

Ricoh's Ransomware Containment Solution – a military-grade 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 simulated 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 of mind and a detailed overview of activity.

Simply get in touch with our team to book a free demo.

RICOH
imagine. change.

Thank you for reading this report on

Ricoh ransomware containment and isolation

Protect your organization with ransomware containment.

Book a free demo today!