A HEALTHCARE EXECUTIVE'S GUIDE TO

Ransomware Protection as a Service™

InterVision

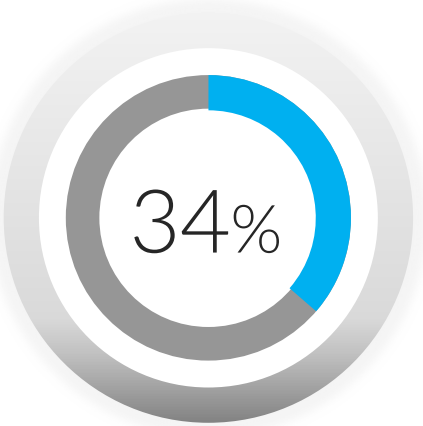
Cybercrime is one of the leading causes of downtime in healthcare

When a healthcare organization experiences a ransomware attack, the losses can be staggering in financial and human terms. Detecting and preventing ransomware attacks are vital IT responsibilities, but most security experts agree: Even with the best protection schemes, businesses will continue to fall victim.

Your role as a business leader is to mitigate the risks of cybercrime, including ransomware, and decrease the toll it takes on the organization and your bottom line. In this eBook, we'll touch on several focal points essential to your position, whether you're in IT leadership, sitting in the C-Suite – or both!

To help you find the information and insights you're looking for, we've divided this eBook into three sections:

1. The current state of the ransomware threat and its impact on businesses.
2. Why most ransomware strategies miss the mark and leave businesses vulnerable.
3. How Ransomware Protection as a Service™ (RPaaS™) can help you close the gaps.



of healthcare organizations worldwide were hit by ransomware in 2020.

- HHS Cybersecurity Program, Ransomware Trends 2021

INTRO:

The Ransomware Threat Landscape

InterVision

A HEALTHCARE EXECUTIVE'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

WHAT YOU DON'T KNOW, WILL HURT YOU

...the ransomware threat is growing

The data looks bad.

For a sector that relies on data, the statistics should send some red flags for those responsible for their organization's compliance and security measures.

50%

increase in ransomware attacks against healthcare organizations.

72%

of incidents reported had PII data leaked in the first half of 2021.

69%

of healthcare organizations that retrieved their data could restore it.

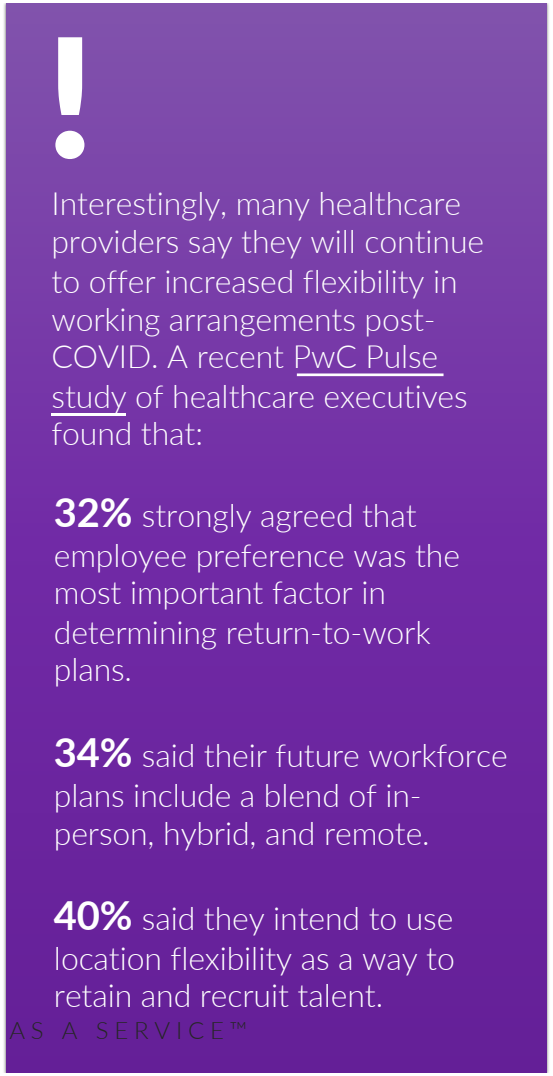
Work-from-anywhere strains healthcare systems

Healthcare businesses rely on direct interactions between patients and providers, but even this sector was impacted by COVID-19. Non-essential workers were sent home and given access to systems remotely. Patient triage was increasingly done via telehealth, with continued care offered through video sessions whenever feasible.

While a work-from-anywhere strategy helped providers offer quality care during the crisis, it put an increasing strain on systems.

According to John Gray, InterVision CTO, **"The challenge was that many businesses were not prepared for the speed at which they needed to implement their work-from-anywhere strategy. One of the primary reasons we developed our ransomware-as-a-service solution was to help these businesses bring their defenses up to the level they need to be at to support the business' growth plan."**

Businesses, across all sectors, simply were not ready for the ransomware threat and the impact it can have on their business.



PART ONE:

Ransomware's Impact on Business

InterVision

A HEALTHCARE EXECUTIVE'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

How reliant on technology are you?

Many healthcare organizations are so reliant on technology and connectivity they can't go back to doing business "on paper," even if they wanted to. This reliance makes the threat of unplanned downtime due to ransomware particularly worrying.

+ INTERCONNECTED EQUIPMENT
+ ELECTRONIC HEALTH RECORDS (EHR)
+ PATIENT/PROVIDER PORTALS
+ PATIENT WEARABLES
+ CONNECTIVITY BETWEEN LOCATIONS
+ DATA SHARING BETWEEN PROVIDERS
+ TELEHEALTH SERVICES
+ HOMECARE PROVIDER ACCESS

The high cost of ransomware in healthcare

The HHS Cybersecurity reports that the average ransomware payment in 2020 was a mere $131,000 – a drop in the bucket compared to other ransomware-related costs for the healthcare sector.

The average bill for rectifying a ransomware attack in 2020.

LOST BUSINESS & REVENUES

Loss of access to systems and data can lead to reduced revenues and lost confidence in the provider.

STOLEN OR CORRUPTED DATA

Encrypted data may be sold on the dark web, whether the organization pays the ransom or not.

DECREASED ACCESS TO CARE

Systems outages can impact the quality and availability of care, even to the point of endangering lives.

POTENTIAL HIPAA VIOLATIONS

Both decreased access to care and stolen PII data can lead to potential HIPAA violations.

WHAT YOU DON'T KNOW, WILL HURT YOU

...a quick ransomware self-check

Self-check

Here's a quick self-check that will help you spot the gaps in your ransomware protection and recovery strategy. No need to tally up the responses.

Simply circling yes, no, or not sure will tell you what you need to know.

We have a Chief Information Security Officer (CISO) who oversees and is accountable for both cybersecurity and disaster recovery strategy.	YES	NO	UNSURE
We have a documented ransomware protection and recovery strategy that we review at least once a year.	YES	NO	UNSURE
All of our business and IT leaders understand our approach to ransomware and why adherence to the plan is vital to business continuity.	YES	NO	UNSURE
We've decided ahead of time how to handle ransom demands, and we're confident we can stick to the plan.	YES	NO	UNSURE
We have ransomware insurance, and our executive team understands exactly what it does and does not cover.	YES	NO	UNSURE
Our entire staff knows exactly what to do if they suspect a ransomware attempt has been made or an attack has been successful.	YES	NO	UNSURE
We have dedicated IT security specialists and tools with a focus on ransomware detection, protection, and mitigation.	YES	NO	UNSURE
Our IT staff is confident our current systems can detect any threats lying dormant in our systems or gathering data in advance of an attack.	YES	NO	UNSURE
Our disaster recovery plan includes ransomware contingencies.	YES	NO	UNSURE
We revisit our disaster recovery strategy, especially for new and critical workloads, at least once a year and test it regularly.	YES	NO	UNSURE

PART TWO:

Crafting a Comprehensive Ransomware Strategy

InterVision

A HEALTHCARE EXECUTIVE'S GUIDE TO RANSOMWARE PROTECTION AS A SERVICE™

RANSOMWARE STRATEGY

Does your ransomware strategy miss the mark?

NOT IF, BUT WHEN.

Ransomware attacks are not a matter of if, but when. Understanding that, many organizations have invested heavily in tools to strengthen their IT security position. That's good, but no detection and prevention scheme is 100% failsafe. Mitigating your risks requires a ransomware strategy that includes both protection and response.

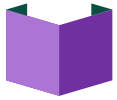
RANSOMWARE STRATEGY

Why businesses fall short

If your strategy includes hoping you won't get hit with ransomware, you're not alone. Several factors combined to make executing a comprehensive ransomware strategy more challenging than ever:

PEOPLE

Of the 75% of business leaders who said they had a specific plan or policy in place to effectively manage a ransomware attack, less than 60% felt they had the staff needed to execute that plan.



PROCESSES

Ideally, ransomware strategy would be included in disaster recovery and business continuity planning, but only about half of organizations have a disaster recovery plan, and few take the time to test their plan.

TECHNOLOGY

It would be great if there were a ransomware silver bullet, but there isn't. IT departments often deploy half a dozen or more technology "solutions" and still fail to fill all the gaps in their protection and recovery plan.

RANSOMWARE STRATEGY

Should paying the ransom be part of your response strategy?

As you craft your ransomware strategy, your organization's stance on paying ransom demands is one of the questions you'll need to discuss. Cybercriminals would like you to believe that if you fulfill their demands, you'll be able to go back to business as usual. That isn't always the case. Recent research underscores the need for a comprehensive ransomware response strategy that doesn't reward cyberthieves for their malicious actions.

61%
Said that they paid the ransom in 2021.

2%
of healthcare organizations that paid the ransom got all of their data back.

65%
Of the data was restored after payment.

80%
were hit with additional demands after they paid the initial ransom.

Is cyber insurance the answer?

As the ransomware threat and the impact of an attack on healthcare grows, experts predict cyber insurance will be more expensive and difficult to obtain. The data from the Sophos 2022 State of Ransomware in Healthcare report bears this out.

> **!** Cybersecurity insurance is rapidly becoming a "must-have" for many businesses, but it is not a replacement for a comprehensive ransomware protection and response strategy.

Of healthcare respondents said cyber insurance is getting harder to secure.

Reported the level of cybersecurity needed to qualify is now higher.

Said policies are now more complex.

Said fewer companies offer cyber insurance.

States that the application process takes longer.

Said the insurance is more expensive.

PART THREE:

InterVision's Ransomware Protection as a Service™ (RPaaS™)

InterVision

RPAAS DEFINED

What is ransomware protection as a service (RPaaS)?

"As a service" solutions are gaining traction as a way to ensure coverage of critical aspects of IT operations while freeing up internal staff to focus on business-building initiatives. Two of the most common solutions are Security Operations Center as a Service (SOCaaS) and Disaster Recovery as a Service (DRaaS). Both of these elements are vital components of ransomware protection and recovery, but few solution providers have connected the dots between the two.

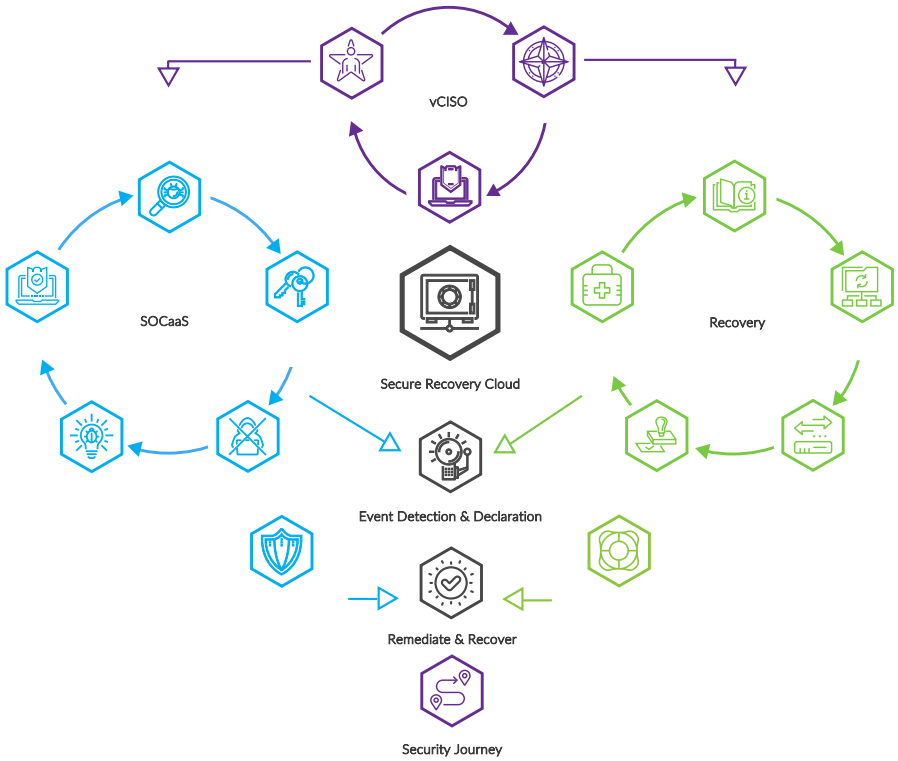
RPAAS DEFINED

InterVision's RPaaS Solution

InterVision combines its industry-leading DRaaS and security services into one comprehensive **Ransomware Protection as a Service (RPaaS)** solution that addresses an organization's broader IT security and disaster recovery requirements while closing the gaps in its ransomware detection & protection, respond and recover and advise & adapt strategies.

InterVision

Ransomware Protection as a Service (RPaaS)

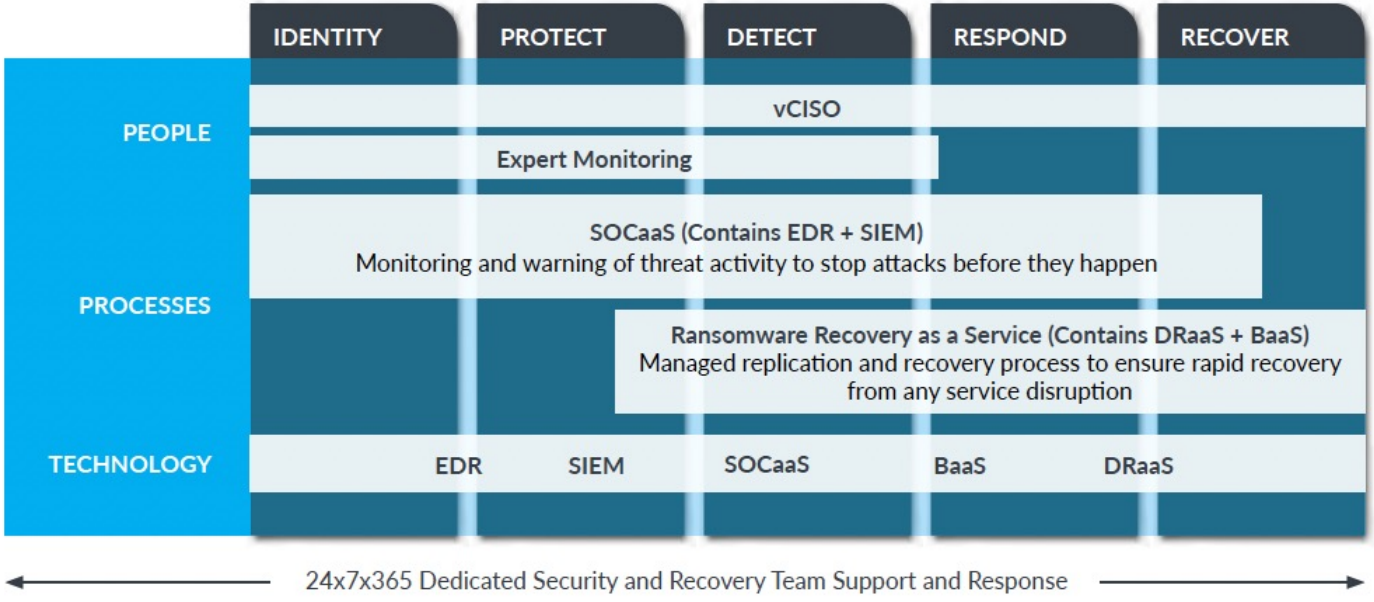


RPAAS DEFINED

InterVision

Comprehensive protection

To ensure end-to-end protection, the InterVision RPaaS solution follows the five steps of the NIST Cybersecurity Framework (CSF) for Critical Infrastructure: Identify, Protect, Detect, Respond, and Recover.



At InterVision, people make the difference.

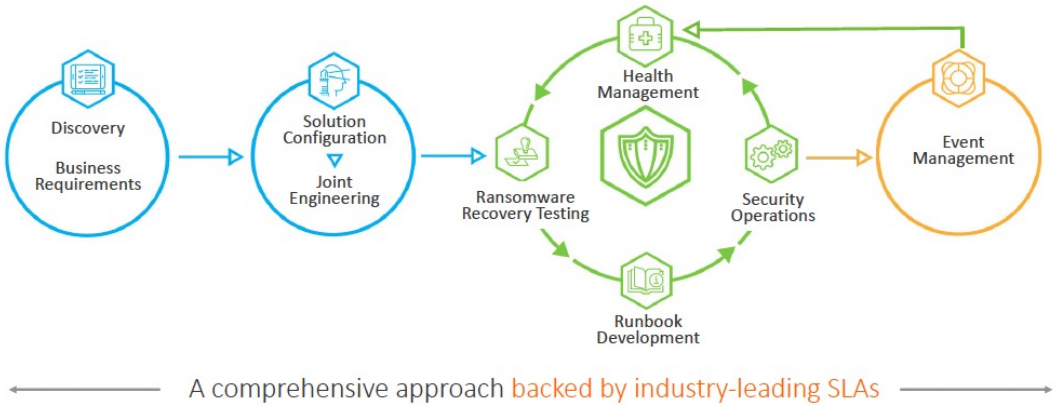
While lots of managed services companies could cobble together a plan for ransomware protection and recovery, what really ties the InterVision RPaaS solution together is the vCISO assigned to your account. These senior security advisors are “big picture” cybersecurity strategists who bring years of experience overseeing security across a vast array of disparate environments.

“When it comes to security and disaster recovery planning, every business needs to approach it differently. When I help clients map out their strategy, one of the key objectives I’m looking to achieve is to create a plan that meets their security and recovery objectives for their critical workloads but does not entail paying a ransom in the event of a ransomware attack.”

Allen Jenkins, InterVision Client vCISO

RANSOMWARE PROTECTION AS A SERVICE (RPaaS)

We're with you every step of the way.



From day one, your InterVision RPaaS team will work with you to create a ransomware protection and recovery strategy that uses the right tools for the job. Then they'll help you document, implement, and train your team on how to execute that plan, providing extra hands and expertise in areas where your current staffing may fall short. We'll also be with you every step of the way should a ransomware event require you to implement your recovery plan.

InterVision

The tech news makes it seem like only the high-profile companies that are being hit with ransomware. In reality, the data we shared in this paper includes ransomware attacks against companies of all sizes and all industries. In fact, smaller companies may be more at risk of ransomware because cybercriminals know they often lack the budget and resources to mount a proper defense.

Don’t let your organization be one of this year’s data points. The first step is to reach out to our RPaaS team for a complimentary consultation to discuss your business requirements and answer any questions you may have.

CONTACT US

InterVision

www.intervision.com/rpaas-health/

Sources

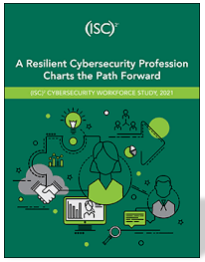
2021 CrowdStrike Global Security Attitude Survey

Howden, Cyber Insurance: A Hard Reset, 2021

Cybereason, Ransomware: The True Cost to Business, 2021

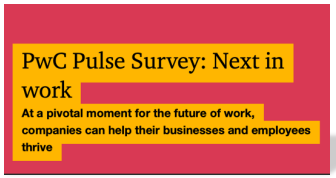
HHS Cybersecurity Program: Ransomware Trends 2021

Sophos State of Ransomware in Healthcare Report 2021



(ISC)2 Cybersecurity Workforce Study, 2021

Why is Office Occupancy only 31%? Korn Ferry, February 2022. 5 IBM Cost of a Data Breach Report 2021



HHS Cybersecurity Program: Ransomware Trends 2021