

Containment Changes *The Recovery Equation*

AI made ransomware faster. Recovery-first strategies cannot keep up. Active Containment® stops encryption at roughly 9 files, so the business never goes down.

EXECUTIVE SUMMARY

Containment ends the recovery problem instead of shortening it.

The math of an unchecked attack is simple. Ransomware is built to encrypt everything it can reach. Recovery is then a race to restore it all. Only 16% of organizations hit by ransomware fully recover in less than a day, according to Sophos. The rest measure recovery in days, weeks, or months.

Active Containment® changes the math. It stops encryption after a few files, then isolates the threat. There is no mass encryption to restore. There is no dependency on a clean backup. Employees keep working.

Resilience and operational continuity both deny leverage to the attacker. With containment, recovery becomes a smaller, quieter, and controlled task.

16%

of ransomware victims fully recover in less than a day

Sophos, State of Ransomware 2026

~9 files

is where Active Containment® stops encryption and isolates the threat

QuellSecure

LEGACY STRATEGY

Restore after the damage. The attacker sets the scope.

CURRENT RECOVERY

Shorter downtime. The business is still down.

NEW & 100% CONTAINED

Stop the damage at 9 files. The business keeps running.

A COMPANION PAPER



AI Is Changing the Ransomware Landscape showed the problem: AI has compressed attack timelines from days to hours and minutes. This paper shows the answer.

THE PROBLEM, RECAPPED

AI has compressed the ransomware timeline.

3.4 hrs

median time to reach
Active Directory, down 70%
year over year

*Sophos, Active Adversary
Report 2026*

39%

of breaches now involve
ransomware, up from 34%

*IBM, Cost of a Data Breach
2026*

79%

of ransomware incidents
begin with compromised
identities

*Sophos, State of Ransomware
2026*

FOUR SIGNALS FROM THE FIELD

AI-assisted extortion **2025**

One low-skill operator used an AI coding agent to hit 17 organizations with data extortion in a single month.

Anthropic threat intelligence

PromptLock **Aug 2025**

The first known AI-powered ransomware calls a local LLM at runtime to generate its malicious scripts on the fly.

ESET Research

PROMPTFLUX **Nov 2025**

Malware that uses an AI model to rewrite its own code, defeating signature-based detection.

Google Threat Intelligence Group

HexStrike-AI **Sept 2025**

Attackers used an AI offensive framework to weaponize Citrix NetScaler flaws in roughly 12 hours.

Check Point Research

AI shrinks the window between access and impact. Detection built on known threats falls behind. Response that waits on a human falls further behind. Many organizations answer with ever-improving backup and recovery tools. Resilience plans adapted to AI-enhanced threats will need to add proactive, efficient tools that ensure continuity.

THE RECOVERY GAP

Faster recovery is still recovery.

Recovery has improved. It is still slow. Sophos surveyed 2,158 organizations hit by ransomware for its State of Ransomware 2026 report. Even well-prepared teams stay down for days.

SHARE OF VICTIMS FULLY RECOVERED



84% are still recovering after day one. Nearly half are still recovering after a week.

Sophos, State of Ransomware 2026

3 weeks

average time to recover

\$1.7M

average recovery cost per incident, before any ransom

WHERE THE BEST-LAID RECOVERY PLANS BREAK

01

They start after the damage.

Recovery is reactive by design. The attacker sets the scope. The defender cleans up.

02

They depend on a clean backup.

Backups are a primary target. A tainted or incomplete one turns days of downtime into weeks.

03

They cannot plan for the unknown.

Real attackers will fight back. Runbooks and procedures are a starting point, not a blueprint for survival.

Can you shrink downtime risk to 0% with what you're doing, or do you need something new?

THE SOLUTION

Stop the one thing every attack must do.

Active Containment® does not wait to recognize the attacker. It watches the one action every ransomware attack must take: encrypting files.



ATTACKER CONTROLS THE ENTRY

The attack path does not matter.

A phished credential, an AI-weaponized exploit, or a simple misconfiguration all arrive at the same choke point. Active Containment® intercepts at the file system level, stops encryption after a small, fixed number of files, and isolates the threat.

YOU CONTROL THE OUTCOME

Variant-agnostic by design.

It does not need to know PromptLock, PROMPTFLUX, or whatever comes next by name. It does not need a signature. It does not need a human to notice in time.

INDEPENDENTLY VALIDATED BY SECUREIQLAB

600

ransomware samples

195

unique families

100%

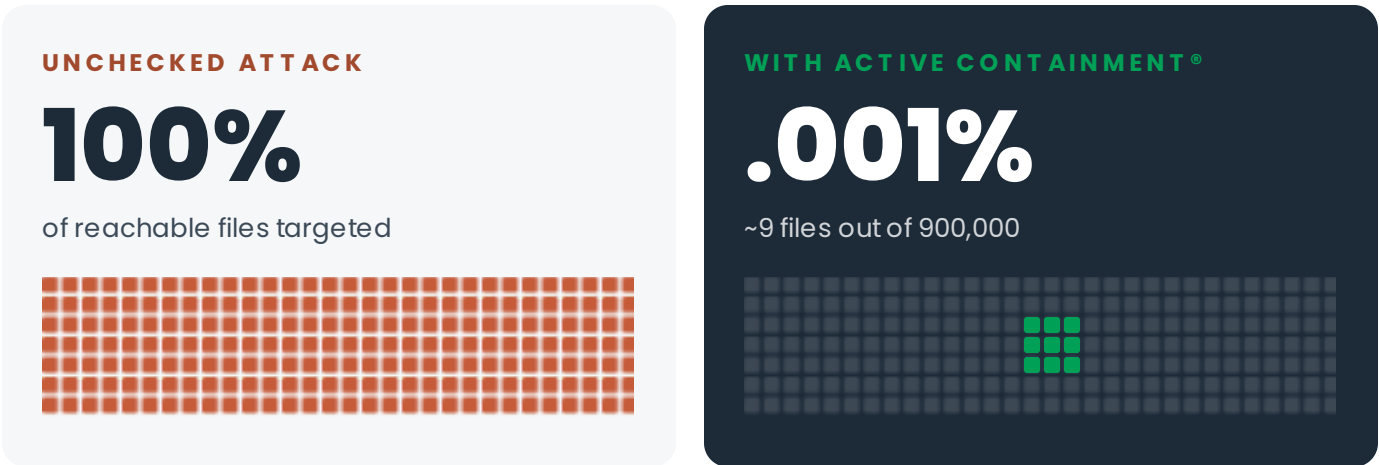
detection rate

Patent-pending technology.

THE NEW MATH

100% versus .001%.

An unchecked attack is built to encrypt every file it can reach. Active Containment® stops it at roughly 9. In a typical business environment of 900,000 files, that is .001%.



RECOVERY TASK	UNCHECKED ATTACK	WITH ACTIVE CONTAINMENT®
Systems affected	Endpoints, servers, shares	Contained and isolated at the point of encryption
Business status	Down, often company-wide	Running
Backup dependency	Full restore from a clean, untainted backup	None for operations; restore a handful of files
Forensics and rebuild	Tracing sources, testing remediation, and confirming restoration	Targeted review of a contained event
Risk to continuity	Only 16% recover in under a day	Isolated to a few files
Ransom leverage	High	Encryption leverage removed

Nine files is a help desk ticket. A fully encrypted file server is a crisis.

The 900,000-file environment is illustrative. Actual file counts vary by environment.

ZERO DOWNTIME

Everyone keeps working.

The real cost of ransomware is downtime. Not the files. The hours when no one can work.

RECOVERY-FIRST ATTACK

- ✗ Staff sent home or on paper
- ✗ Critical services interrupted
- ✗ Orders and billing stop
- ✗ Help desk becomes a war room

CONTAINED ATTACK

- ✓ Attack stops before the damage spreads
- ✓ Affected files are restored
- ✓ Everyone else keeps working
- ✓ Most employees never notice

The business stays open.

Revenue, services, and operations continue.

IT stays in control.

Review a contained event on your schedule, not an outage on the attacker's.

The client stays confident.

No outage call to make. No recovery timeline to defend.

This is the shift from reactive to in control. Recovery happens on your terms, at your pace, at a scale you choose.

Downtime from ransomware is not a risk you can take. We eliminated it.

BUILT FOR THE AI ERA

AI changes how attackers get in. It cannot change how it ends.

Every way AI makes ransomware worse is a way to beat detection or outrun response. None of them change what ransomware must do at the end. It will encrypt. That is where containment works.

AI-ERA PROBLEM	WHY LEGACY DEFENSES STRUGGLE	WHY CONTAINMENT HOLDS
Compressed timelines	Machine-speed is the new standard, requires new balance for response to false positives	Reacts only when files are impacted.
Self-rewriting and runtime-generated malware	Threats evolve quickly. Prevention can't keep up.	If malicious encryption is the trigger, all ransomware looks the same.
Faster exploit weaponization	Patching cannot keep pace with hours from disclosure to exploit	The entry point does not matter; the impact is capped
Easier to steal identities	Valid credentials look like normal users	A legitimate login still cannot encrypt past the threshold
Scale from low-skill actors	More attacks against more targets, including SMBs	Every attack hits the same ceiling, no matter who launches it



The attack surface keeps shifting. The blast radius stays fixed at roughly 9 files.

RETHINKING THE STACK

The recovery landscape has changed.

Containment does not replace the security stack. It changes what the stack has to carry. When the worst case is 9 files instead of a whole network, every other layer is judged differently.

EDR and detection	Still find and investigate threats. No longer carry the full weight of stopping mass encryption in time.
Backup	Becomes a data-protection tool, not the last line between the business and a shutdown. A tainted backup is no longer an existential risk.
Incident response	Shifts from crisis recovery to a controlled response.
Cyber insurance	Less risk, cost, and complexity when downtime and encryption scope are capped.
Compliance	Data stays available and operations continue through an attempted attack.

WHAT IT MEANS FOR MSPS

Promise uptime, not faster cleanup.

MSPs carry the risk for every client they serve. One unchecked attack can take down many businesses at once and damage the MSP's own reputation. A recovery-first model forces the MSP to promise faster cleanup. A containment model lets the MSP promise something better: the business stays up.

That is a stronger story to sell and a lighter load to support. It turns ransomware protection into a differentiated, recurring service. The client conversation moves from how fast can you recover us to how you keep us running.

CONCLUSION

Containment is the new standard.

AI has changed the ransomware landscape. Attacks are faster, more adaptive, and easier to launch. Recovery-first strategies were built for a slower threat. They still leave most victims down for days or longer.

Containment resets the equation. Encryption stops at roughly 9 files. The threat is isolated. The business keeps running. Recovery becomes small, fast, and controlled.

The question is no longer how quickly you can recover. **It is whether you need to.**

NEXT STEPS FOR MSPS

01

See it stop live ransomware

Request a free containment demo and watch Active Containment® work in real time.

02

Model client exposure

Use the QuellSecure ransomware downtime risk calculator to size what downtime costs your clients.

03

Become Partner Ready

Join the Partner Ready Program and add zero-downtime ransomware protection to your stack.

Downtime from ransomware is not a risk you can take. We eliminated it.

quellsecure.com

SOURCES, IN ORDER OF APPEARANCE

References

1. **Sophos, The State of Ransomware 2026.** Survey of 2,158 IT and cybersecurity leaders across 17 countries, conducted by Vanson Bourne, Q1 2026. Recovery timelines, recovery cost, and identity-based initial access. sophos.com
2. **Sophos, 2026 Active Adversary Report.** Median time for attackers to reach Active Directory.
3. **IBM, 2026 Cost of a Data Breach Report.** Share of breaches involving ransomware.
4. **ESET Research,** "First known AI-powered ransomware uncovered by ESET Research," welivesecurity.com, Aug 27, 2025.
5. **Google Threat Intelligence Group,** PROMPTFLUX / PROMPTSTEAL disclosure, reported by The Hacker News, Nov 2025.
6. **Check Point Research,** HexStrike-AI / Citrix NetScaler weaponization, reported by The Register and Bank Info Security, Sept 2025.
7. **Anthropic,** threat intelligence report on AI-assisted data extortion, 2025.
8. **SecureQLab,** independent validation of QuellSecure Active Containment®: 600 ransomware samples, 195 unique families, 100% detection rate.

The 900,000-file environment used for the .001% figure is illustrative. Actual file counts vary by environment.

ABOUT QUELLSECURE

QuellSecure builds Active Containment®, patent-pending ransomware containment that stops encryption at roughly 9 files and isolates the threat. It is a zero-downtime alternative to backup-and-recovery, delivered exclusively through Managed Service Providers.

Read the companion paper, **AI Is Changing the Ransomware Landscape**, for the full evidence base behind the threat.