ARMS CYBER

ARMS CYBER · WHITEPAPER

SELLING WHAT ATTACKERS CAN'T REACH

THE MSSP CASE FOR STEALTH-DRIVEN SECURITY

INSIDE THIS PAPER

– Abstract
01 The shift clients already feel
02 The gap EDR leaves
03 A preemptive model: Conceal, Adapt, Restore
04 The MSSP opportunity
05 Operational fit
06 What good looks like
07 Getting started

© Arms Cyber 2026. All Rights Reserved.

ABSTRACT

THE DETECTION-FIRST STACK HAS HIT ITS CEILING.

Clients are fully equipped with EDR and still losing data to ransomware, exfiltration, and insider loss. The damage lands after the alert.

MSSPS CARRY THE RISK WITHOUT A TOOL TO CLOSE THE GAP.

When a client gets hit, the provider owns the fallout but the prevailing stack has no answer for the data damage itself.

A PREEMPTIVE, STEALTH-DRIVEN MODEL CHANGES THE MATH.

Making critical data invisible to attackers, then containing and recovering through one strategy (Conceal, Adapt, Restore), removes the outcome clients fear instead of racing it.

FOR THE MSSP, IT'S A NEW SERVICE LINE, NOT ANOTHER VENDOR BOX.

High margin you own, a differentiator no competitor can claim, stickier accounts, and near-zero operational lift over the stack you already run.

© Arms Cyber 2026. All Rights Reserved.

SECTION 01

THE SHIFT CLIENTS ALREADY FEEL

The security market has spent a decade perfecting detection. Endpoint detection and response is mature, widely deployed, and genuinely good at what it does: watching for malicious behavior and responding to it. Most of your clients already own it. Many of them own more than one layer of it.

AND YET THE LOSSES KEEP COMING.

- **RANSOMWARE STILL ENCRYPTS.**
- **SENSITIVE DATA STILL WALKS OUT THE DOOR.**
- **INSIDERS STILL TAKE WHAT THEY SHOULDN'T.**

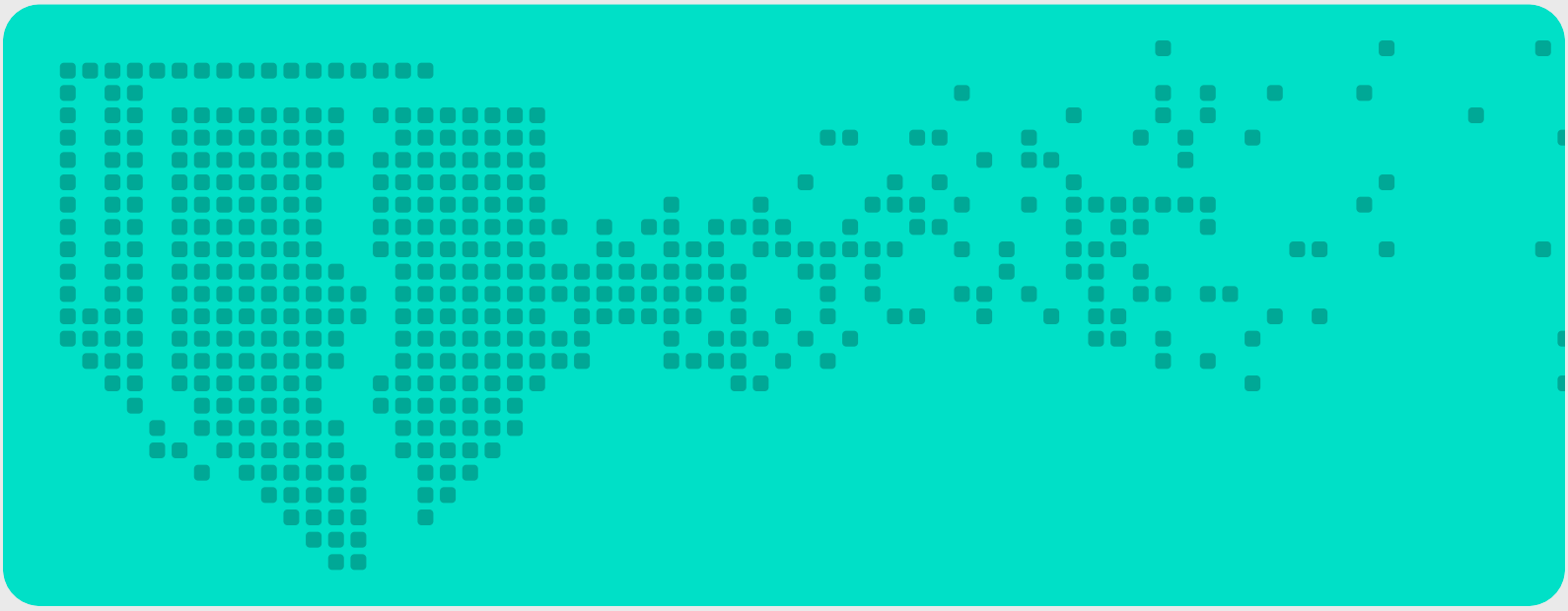
The tooling is better than it has ever been, and the outcomes clients actually care about (downtime, ransom demands, breach notifications) haven't gone away.

"WE HAVE THE TOOLS"

↓ GAP ↓

"WE STILL GOT HIT"

That gap between "we have the tools" and "we still got hit" is the experience your clients live with, even if they don't name it. It's also the gap you inherit. When an incident lands, the managed service provider is the one explaining what happened, managing the recovery, and defending the retainer. The stack did its job and the client still lost and that is an uncomfortable place to be selling more of the same.



© Arms Cyber 2026. All Rights Reserved.

SECTION 03

A PREEMPTIVE MODEL: CONCEAL, ADAPT, RESTORE

If the limit of detection is that it begins once the attacker is already acting, the way past it is to change what the attacker finds when they get there. That is the premise of preemptive, stealth-driven security: rather than racing to respond to damage in progress, remove the target entirely. If attackers can't locate the data, they can't encrypt it, exfiltrate it, or destroy it then there is nothing to act on.

This is the approach Arms Cyber's Raven platform takes, and it is built to sit on top of the security stack your clients already run, a complement to EDR and XDR, never a replacement. Raven works through a single strategy with three parts: Conceal, Adapt, and Restore.



IF ATTACKERS CAN'T FIND THE DATA ...

THEY CAN'T ACT ON IT.



CONCEAL

Raven hides critical files from attackers, keeping them invisible to both encryption and exfiltration attempts. Even when ransomware or AI-crafted malware runs on the endpoint, it cannot locate the protected data.



ADAPT

When an attacker does act, deceptive file structures draw them into false engagements, and behavioral signals expose the threat during execution, containing it before it spreads and keeping the real data untouched.



RESTORE

Clean copies are held in concealed, on-device enclaves an attacker cannot find or corrupt. If an attack is detected, recovery is immediate and data integrity stays intact, operations come back in minutes, without the downtime of traditional restoration. Raven also works with the client's existing backup ecosystem to identify clean restore points and prevent reinfection from compromised backups.

Underneath, the model draws on automated moving target defense (AMTD) to keep protected assets from sitting still long enough to be found. The result is coverage across the threats that matter most to your clients including AI-driven attacks, ransomware and other data threats, and human insider risk, each addressed by removing the attacker's ability to reach what counts.



AI-DRIVEN ATTACKS



RANSOMWARE AND OTHER DATA THREATS



HUMAN INSIDER RISK

© Arms Cyber 2026. All Rights Reserved.

SECTION 02

THE GAP EDR LEAVES

Detection and response is built on a simple premise: see the malicious behavior, then act on it. That premise has a structural limit. By the time there is behavior to detect, the attacker is already executing on the endpoint and for data-centric attacks, execution is the damage. Encryption, exfiltration, and destruction aren't precursors to the harm; they are the harm. A response that begins once those behaviors trigger is, by definition, racing damage that has already started.

SEE THE MALICIOUS BEHAVIOR, THEN ACT ON IT

ATTACKER EXECUTING	EXECUTION IS THE DAMAGE	RESPONSE BEGINS
On the endpoint	Encryption · Exfiltration · Destruction	Racing damage already started

THE QUESTION A DETECTION-FIRST STACK ANSWERS

"HOW FAST CAN WE RESPOND?"

This is why clients with excellent detection coverage still suffer real losses. The question a detection-first stack answers is "how fast can we respond?" The question clients are actually asking is "how do we make sure this never touches our data in the first place?" Those are different questions, and the second one is the one that shows up in board meetings.

THE QUESTION CLIENTS ARE ACTUALLY ASKING

"HOW DO WE MAKE SURE THIS NEVER TOUCHES OUR DATA IN THE FIRST PLACE?"

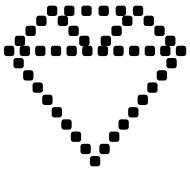
There's a second-order problem for you specifically. Because detection-and-response tools all answer the same question, they're hard to differentiate and easy to commoditize. Adding another EDR, or a thicker tier of the one you have, deepens your exposure to the same limitation and does little to set your practice apart. The gap isn't a product you're missing. It's a category the prevailing stack doesn't cover: preventing the data damage itself, rather than detecting and chasing it.

© Arms Cyber 2026. All Rights Reserved.

SECTION 04

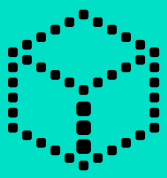
THE MSSP OPPORTUNITY

For a managed security provider, a preemptive layer isn't just better protection for clients, it's a better business. The economics line up on four fronts.



NEW RECURRING MARGIN YOU OWN.

Raven is a managed service line you price, package, and keep, not a third-party box you resell at thin vendor margin. It adds high-margin recurring revenue on top of the services clients already buy from you, and because it's delivered as part of your practice, the margin and the relationship stay yours.



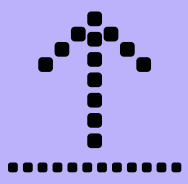
A DIFFERENTIATOR NO COMPETITOR CAN CLAIM.

Every provider in your market sells detection. None of them can say they make client data invisible to attackers. Stealth-driven, preemptive protection is a genuinely distinct capability, a category of one that sets your proposals apart in a field where most offerings read the same.



STICKIER ACCOUNTS AND LOWER CHURN.

Protection woven into the resilience a client depends on you for is protection that's hard to rip out. Raven deepens the account, strengthens the renewal conversation, and makes switching costs real, the opposite of a commoditized add-on.



NEAR-ZERO OPERATIONAL LIFT.

A new service line usually means new overhead. This one doesn't. Raven deploys as a lightweight sensor with no reboots and no downtime, overlays the tooling you already operate, and scales across your book without re-architecting client environments, so the margin isn't eaten by the cost to deliver it.

© Arms Cyber 2026. All Rights Reserved.

SECTION 05

OPERATIONAL FIT

The business case only holds if the service is easy to run at scale, and Raven is designed for exactly that. Deployment is a lightweight sensor that installs without system reboots or operational downtime, so onboarding a client doesn't mean a maintenance window or a disruption you have to explain.

OVERLAY, NOT REPLACEMENT



RAVEN

NO SYSTEM REBOOTS

NO OPERATIONAL DOWNTIME

NO RIP-AND-REPLACE

CROWDSTRIKE

Microsoft Defender

SentinelOne

and the rest

THE PLATFORMS YOUR CLIENTS ALREADY HAVE

Because Raven is an overlay, it runs alongside the platforms your clients already have including CrowdStrike, Microsoft Defender, SentinelOne, and the rest rather than displacing them. There's no rip-and-replace, no retraining your team on a new primary stack, and no competitive conflict with the EDR investment a client has already made.

Coverage spans the whole estate: modern cloud infrastructure and the critical legacy systems clients still depend on. The footprint is minimal by design and built for resource-constrained hardware and high-availability production systems where uptime is non-negotiable. For a provider managing many environments at once, that combination of broad coverage and low overhead is what makes the service deployable across the entire book rather than a handful of premium accounts.

COVERAGE SPANS THE WHOLE ESTATE



CRITICAL LEGACY SYSTEMS



MODERN CLOUD INFRASTRUCTURE

© Arms Cyber 2026. All Rights Reserved.

SECTION 06

WHAT GOOD LOOKS LIKE

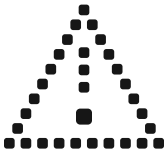
The point of a preemptive layer is the outcome it produces, and the outcome is simple to state: no breaches, no ransom payments, no downtime. For the client, that changes the conversation from “how quickly can we respond when we’re hit” to “this won’t reach our data in the first place,” which is the answer their board is actually asking for.

NO BREACHES

NO RANSOM PAYMENTS

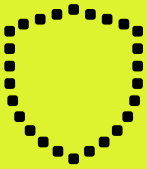
NO DOWNTIME

FROM



“HOW QUICKLY CAN WE RESPOND WHEN WE’RE HIT”

TO



“THIS WON’T REACH OUR DATA IN THE FIRST PLACE”

For you, the shift is just as meaningful. Fewer incidents to firefight means fewer tense recovery calls and less margin lost to emergency response. A differentiated outcome gives you something concrete to put in front of a prospect that competitors can’t match. And a client who hasn’t suffered a loss on your watch is a client who renews and who refers. The preemptive model doesn’t just protect the client’s data; it protects the health of the account.

© Arms Cyber 2026. All Rights Reserved.

SECTION 07

GETTING STARTED

Becoming an Arms Cyber partner is built to get you to your first wins quickly. Partners get a co-branded campaign-in-a-box: ready-to-run assets your team deploys under your own brand, so pipeline can start on day one, along with sales and technical enablement, margin-forward economics designed for recurring services revenue, and hands-on support from the Arms Cyber team through onboarding and beyond.



CO-BRANDED CAMPAIGN-IN-A-BOX



SALES AND TECHNICAL ENABLEMENT



MARGIN-FORWARD ECONOMICS



HANDS-ON SUPPORT

ARMS CYBER

SELL WHAT CAN'T BE FOUND

THE FIRST STEP

The first step is a short conversation to map the margin and the fit for your book. From there, we'll help you package the service, enable your team, and put the first assets in market.

© Arms Cyber 2026. All Rights Reserved.