CORNCON 2026 · DAVENPORT, IA

TRACK: LEADERSHIP

Hack Yourself First.

The case for moving 15% of your defensive budget into continuous offensive security, before an adversary makes the argument for you.

Jason Rowland

Chief Delivery Officer, Evolve Security

45 minutes · 7 hard numbers
1 uncomfortable ask

LET'S START HERE

Your last pen test was a compliance receipt, not a security test.

Fixed scope. Fixed window. PDF at the end. No / limited re-test.
Nobody in this room would accept that as proof of anything else.

THE ARGUMENT IN THREE MOVES

01

Spend went up. Outcomes didn't.

Security budgets are compounding at double digits. Breach costs just hit an all-time record. That is not a coincidence, it's a strategy failure.

02

Defense-only loses on the clock.

Attackers break out in 29 minutes. We contain in 247 days. You cannot win a race you enter eight months late.

03

Validation is the cheapest control you own.

Not a bigger stack. Proof that the stack you already bought stops a real operator.

Ground rule: every number on these slides is cited. Including three of the industry's favorites that don't survive contact.

WHY I'M THE ONE MAKING THIS ARGUMENT

Eighteen years on the defensive and offensive side. Here's what each stop taught me.

2007

Global hotel company

Major breach. Two years building security operations from the incident outward.

2009–12

Post-breach rebuilds

Stood up operations capability capability for organizations that that had already been hit.

2012

Built an MSSP

From zero: monitoring, detection, and the economics of selling both.

2016

Offensive Security

Switched sides. Led offensive delivery at scale, thousands of of engagements.

2020

Threat management

Ran managed threat services at the largest possible scale.

TODAY

Evolve Security

Chief Delivery Officer. Building Building the thing the last five stops told me was missing.

LESSON

Nobody funds prevention until after the loss. The budget arrives the week it stops mattering.

LESSON

Almost every one of them already had a report describing the path that was used.

LESSON

Monitoring scales beautifully. It does not reduce exposure, it narrates it.

LESSON

Offensive security is essential, but delivered as a project, it doesn't move the needle.

LESSON

The gap in most managed services: they monitor controls nobody ever validated.

THE THROUGHLINE

Continuous, managed, and validated, or it's theater with a report attached.

I spent eighteen years building defense. That is exactly why I'm up here arguing for offense.

PART ONE

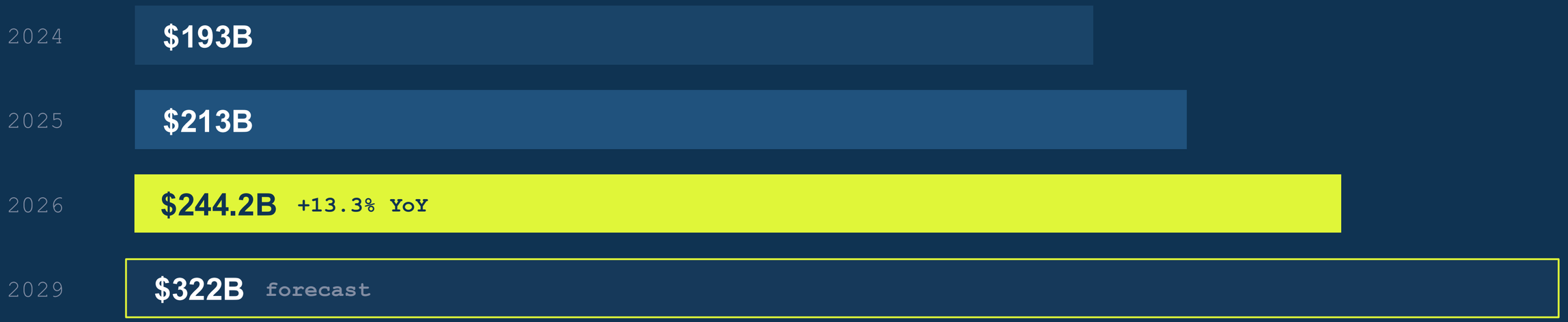
The spending paradox

We are buying more security than at any point in history, and losing more money to attackers than at any point in history.



EXHIBIT A · THE MONEY WE SPEND

Global security spend, in one direction only



Source: Gartner, Forecast: Information Security, Worldwide (2Q25, 3Q25, 4Q25 updates) and Forecast Analysis: Information Security, Worldwide, 2026.

EXHIBIT B · THE MONEY WE LOSE

Average breach cost just set a record. Again.

GLOBAL AVERAGE

$4.99M +12%

UNITED STATES AVERAGE

$11.5M +14%

63%

of breach cost is detection, escalation and lost business money spent *after* you've already lost.

Source: IBM / Ponemon, Cost of a Data Breach Report 2026 (602 organizations, 16 countries, incidents Mar 2025–Feb 2026).

EXHIBIT C · THE MONEY THEY TAKE

US cybercrime losses crossed $20B for the first time

$20.9B

reported losses in 2025, up 26% YoY

1.01M

Complaints, a first in 25 years of IC3

$3.0B

business email compromise losses alone

63

new ransomware variants identified in one year

Reported. Voluntarily. To one agency. In one country. Treat it as a floor.

Source: FBI Internet Crime Complaint Center, 2025 Internet Crime Report (published April 6, 2026).

PART TWO

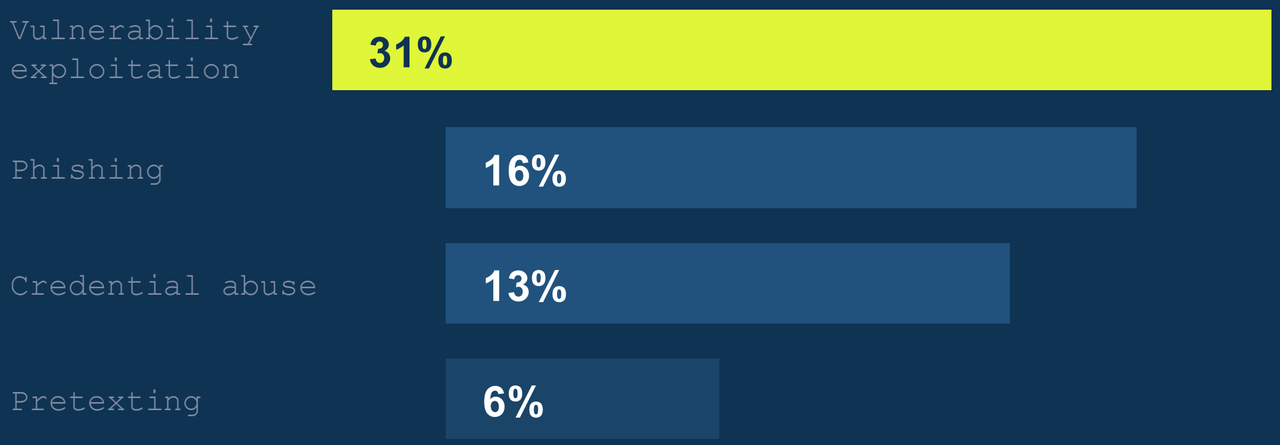
Why defense only loses

It isn't that your tools are bad. It's that the game is timed, and nobody told the defenders the clock changed.



FIRST TIME IN 19 YEARS

Exploitation is now the #1 way in



Known initial access vectors, 2026 DBIR dataset (n≈19,905).

The honest caveat, so nobody can ambush you with it:

Credential abuse still appears **somewhere** in 39% of breach chains, more than any other technique. Pretexting was newly split out this year.

Identity still matters. But the front door is now an unpatched, unvalidated, internet-facing asset that a scanner either never saw or ranked as "medium."

Source: Verizon 2026 DBIR, pp. 10, 15.

THE NUMBER NOBODY PUTS IN A BOARD DECK

In 1 of every 6 organizations, one low-privilege foothold gives an attacker an 80%+ shot at the whole estate.

Your vulnerability count doesn't measure this. Your CVSS scores don't measure this. Only walking the paths measures this, which means somebody has to actually walk them.

Source: Verizon 2026 DBIR — attack graph analysis of contributed environments (16% of orgs at ~80% exposure from low-privilege initial access).

THE CLOCK CHANGED

Breakout time: 98 minutes → 29 minutes



98 min

2021

48 min

2024

29 min

2025

27 sec

fastest breakout ever recorded. In one intrusion, data exfiltration began **four minutes** after initial access.

Source: CrowdStrike 2026 Global Threat Report (Feb 24, 2026) — average eCrime breakout time, 65% faster than 2024.

THE ASYMMETRY, TO SCALE

They move in minutes. We respond in seasons.

ATTACKER: INITIAL ACCESS → LATERAL MOVEMENT

29 minutes



DEFENDER: IDENTIFY → CONTAIN

247 days



That yellow sliver is the entire window in which detection-and-response is even a theory. Everything else is cleanup, lawyers, and disclosure.

Sources: CrowdStrike 2026 Global Threat Report (29 min); IBM Cost of a Data Breach 2026 (247-day mean time to identify and contain).

"WE'LL JUST PATCH FASTER"

You won't. The data says you're losing ground.

26% was 38%

of CISA KEV vulnerabilities fully remediated in 2025, these are the ones we *know* are being exploited.

43 days was 32

median time to fully resolve a critical vulnerability.

+50%

more critical vulnerabilities in the median organization's queue than the prior year.

26% / 11%

of organizations still carry privilege escalation vulnerabilities from **2021** / from **2018**.

Patching is a queue problem. Queues don't get shorter by working harder, they get shorter by knowing which twelve items actually reach something that matters.

Source: Verizon 2026 DBIR, pp. 10, 17.

PART THREE

The offensive stack

Attack surface management, continuous penetration testing, adversarial exposure validation, red teaming - four layers, four different questions.

Point-in-time testing vs. continuous offensive operations

WHAT MOST ORGS BUY

Annual, scoped to what was in scope last year

Tests the environment as it was 11 months ago

Findings land in a PDF and age out

Measures the tester's week, not your resilience

Success = report delivered, auditor satisfied

Never touches the detection and response team

WHAT ACTUALLY REDUCES RISK

Continuous, scoped to what changed this week

Discovery runs before the testers do

Findings enter the ticket queue with a re-test SLA

Measures exploitable paths closed over time

Success = the same attack no longer works

Every exercise is also a detection test

THE STACK

Four layers. Four questions. One program.

01	**Attack surface mgmt**	"What do we actually expose (prioritize external) including what nobody told us about?"	CONTINUOUS
02	**Exposure validation**	"Of those thousands of findings, which ones are genuinely exploitable here, today, against our controls?"	CONTINUOUS / WEEKLY
03	**Continuous pen testing**	"Can a skilled human chain our medium-severity findings into something catastrophic?"	MONTHLY / ON CHANGE
04	**Emulation / purple team**	"When someone is already inside, does our detection, response and decision-making actually work?"	1–2× PER YEAR

THE FRAMEWORK YOUR BOARD HAS ALREADY HEARD OF

CTEM: five stages, and the one everybody skips

01	02	03	04	05
Scoping	**Discovery**	**Prioritization**	**Validation** ← the offensive layer	**Mobilization**

Why validation is the highest-leverage stage

Stages 1–3 produce a longer list. Validation is the only stage that *shortens* it, by proving which exposures actually reach a critical asset through your real controls.

It's also the stage that requires an adversary's skill set. Which is exactly why it's the one that gets deferred.

INTELLECTUAL HONESTY

Gartner predicted CTEM adopters would be **3× less likely** to be breached by 2026. That milestone year is now — and no independent study has yet measured the actual breach-rate difference.

Roughly **16%** of organizations have operationally implemented CTEM. Adopt the framework because the mechanism is sound. Don't quote the prophecy as a result.

Sources: Gartner, Implement a Continuous Threat Exposure Management (CTEM) Program (Oct 2023); CTEM adoption analyses, 2026.

WHAT GOOD LOOKS LIKE

Cadence beats intensity

ACTIVITY	CADENCE	TRIGGER
External asset discovery	**Daily**	Always on. New DNS, new cert, new cloud tenant.
Exploitability validation	**Weekly**	New KEV entry, new exposed service.
Human-led pen testing	**Monthly / on change**	Release to a critical app, new external system, M&A close.
Identity & AD path review	**Quarterly**	Privilege sprawl accumulates silently between reviews.
Adversary emulation exercise	**1–2× / year**	Tests people and decisions, not just systems.
Purple team detection tuning	**After every exercise**	The finding isn't the deliverable. The new detection is.

BUILD OR BUY

Why most organizations should not build this in-house

IN-HOUSE OFFENSIVE TEAM

Right answer if you're large enough to keep three-plus operators busy year-round and can pay market rate for talent that gets recruited constantly.

· Deep environment context, day one

· Fixed cost, unlimited internal demand

· Single skill set, single point of failure

· Grades its own homework — and knows where not to look

· Hardest hiring market in security: a multi-million-role workforce gap

MANAGED OFFENSIVE SERVICES

Right answer if you need continuous coverage now, across web, cloud, identity and social, without a twelve-month hiring cycle.

· A bench, not a person, vacations don't pause the program

· Tradecraft refreshed across hundreds of environments

· Independent finding, credible to auditors, insurers and the board

· Scales up for M&A, down between waves

· Contractual re-test SLAs: the fix gets proven, not assumed

The honest version: most mature programs run both, internal operators for depth and context, external for independence and surge.

PART FOUR

The money argument

A break-even model with every assumption on the slide.

WORKED EXAMPLE

The only ROI question worth asking

A · MODELED LOSS EVENT

$4M

Mid-market extortion event: business interruption, IR, legal, notification, churn. Bookends: $4.99M global average, $11.5M US average.

B · ANNUAL PROBABILITY

12%

Your number, not mine. Derive it from your incident history, sector peer data, and insurer's loss model, then defend it.

C · A × B = ANNUALIZED LOSS

$480K

The expected annual cost of doing nothing differently. This is the line item the board never sees.

D · MANAGED OFFENSIVE PROGRAM

$250K/yr

ASM + continuous validation + monthly human-led testing + one red team exercise, with re-test SLAs.

D ÷ C = BREAK-EVEN RISK REDUCTION

52%

The program pays for itself if it cuts annual breach probability from 12% to 5.8%. Everything beyond that is return.

Illustrative model — all four inputs are assumptions, stated deliberately so a CFO can change them. Loss bookends: IBM Cost of a Data Breach 2026.

"CAN YOU REALLY HALVE THE PROBABILITY?"

I won't promise it. I'll show you the mechanism.

31%	of breaches now start by exploiting a vulnerability, the single largest slice of initial access, and the one offensive testing directly addresses.
26%	of known-exploited vulnerabilities get fully remediated. The gap between "we have a patch program" and "the path is closed" is where breaches live.
1 in 6	organizations are one low-privilege foothold from ~80% of the estate. Closing two or three chokepoints changes the shape of every future incident.
63%	of breach cost accrues in detection, escalation and lost business , so shortening or preventing the intrusion attacks the expensive tail, not the cheap part.

Every other line in your budget is also a bet on mechanism. The difference is that this one comes with evidence attached every single month.

THE ASK

Reallocate 15%. Don't ask for new money.

15%

of a $2M security budget is **$200K–$300K** . That is a rounding error against a $4.99M average loss event — and it is almost certainly already sitting in your renewal stack.

New money requires a business case and a budget cycle. Reallocation requires only that you be honest about what isn't working.

FOUR QUESTIONS TO FIND THE MONEY

01 Which tools has nobody logged into in 90 days?

02 Which two products overlap on the same control, and which one would you keep if forced?

03 Which deployment is under 60% coverage and has been for a year?

04 Which control has *never* been tested against a human operator?

Question four is the punchline: you can't answer it without the very capability you're being asked to fund.

OBJECTION HANDLING · 1 OF 2

What the board will say, and what you say back

"We already do an annual pen test."	Then you have a verdict on an environment that no longer exists. Attackers exploit in 29 minutes; your median critical fix takes 43 days. An annual test is a photograph of a moving vehicle.
"Our MDR / EDR covers this."	MDR's clock starts *after* the adversary is inside, and 82% of intrusions are now malware-free. Offense reduces the number of doors; detection watches the ones that remain. You need both, and only one of them is funded.
"Red teaming is too risky for production."	Rules of engagement, kill switches, agreed blast radius, a named executive who can stop it in one phone call. Meanwhile the unauthorized red team currently in your environment negotiated none of that.
"We can't afford another line item."	Agreed, so don't add one. This is 15% moved from controls you cannot demonstrate work, into the one activity that produces evidence either way.

OBJECTION HANDLING · 2 OF 2

The three that need the sharpest answer

"Compliance doesn't require it."	Compliance is the floor, and the floor is exactly where breaches happen. Note that regulators and insurers are converging on the opposite direction, and executives are increasingly named personally in the fallout.
"Our team can do this internally."	Some of it, yes, and they should. But continuous coverage across web, cloud, identity and social needs a bench, not a hero. And nobody grades their own homework honestly, including me.
"We just finished zero trust."	Then you have an architecture. An architecture is a hypothesis until somebody tries to violate it. Congratulations, you've just built the most testable environment you've ever had. Test it.

PART FIVE

Ninety days

No transformation program. No new headcount. Three sprints and one honest conversation with your board.

A 90-day start that needs no new headcount

DAYS 1–30

Know what you own

- Run external discovery. Count the assets nobody claimed.
- Name two crown jewels in business terms, not system names.
- Pull your last three test reports. Count findings never re-tested.
- Set one baseline metric you'll report every quarter.

DAYS 31–60

Prove the paths

- Human-led test against the real. external surface, including the unclaimed assets
- Walk identity and privilege paths to each crown jewel.
- Replay each finding against the control that should have stopped it.
- Log what the SOC saw, and what it didn't.

DAYS 61–90

Close and re-test

- Fix the two or three chokepoints, not the 400-row spreadsheet.
- **Re-test.** The step everybody skips is the only one that proves anything.
- Write the new detections the exercise earned you.
- Take one slide to the board: paths closed, time to close, what's next.

CHANGE WHAT YOU REPORT

Retire the activity metrics. Report the adversary's difficulty.

STOP REPORTING

Total vulnerabilities found

Number of tools deployed

Patch compliance percentage

Training completion rate

Tests completed this year

Each of these can improve while your actual exposure gets worse.

START REPORTING

Validated attack paths to crown jewels, and the trend line

Mean time to close a proven-exploitable path

% of critical controls tested against a live operator in the last 12 months

Detection rate on red team activity, by kill-chain stage

Unknown assets discovered per quarter — the honesty metric

Five numbers a non-technical director can interrogate — and that get worse if you stop working.

THE ASK

Move 15% of your defensive budget to continuous offense. This cycle.

Attackers break out in 29 minutes. You contain in 247 days. Nothing in your renewal stack changes that arithmetic.

31% of breaches start with an exploit. 26% of known-exploited bugs get fixed. That gap is the whole business case.

Offense is the only line item that tells you the truth whether or not you like the answer. Buy the truth.

Somebody is going to test your controls this year. Decide whether you get the report.

QUESTIONS — AND ARGUMENTS WELCOME

Thank you.



If you disagree with a number on any slide, come find me. I'd rather be corrected here than in an incident review.

Jason Rowland

Chief Delivery Officer, Evolve Security

jason.rowland@evolvesecurity.com

Evolve Security

Managed offensive security · evolvesecurity.com

SHOW YOUR WORK

Sources

Gartner — Forecast: Information Security, Worldwide (2Q25/3Q25/4Q25 updates); Forecast Analysis: Information Security, Worldwide, 2026. Spend: $193B (2024) → $213B (2025) → $244.2B (2026, +13.3%) → $322B (2029).

IBM / Ponemon — Cost of a Data Breach Report 2026 (pub. 29 Jul 2026; 602 orgs, 16 countries, Mar 2025–Feb 2026). Global avg $4.99M (+12%); US avg $11.5M (+14%); 247-day mean identify-and-contain; 63% of cost in detection, escalation and lost business; 1 in 4 malicious breaches AI-enabled (+56%).

Verizon — 2026 Data Breach Investigations Report (31,000+ incidents; 22,000+ confirmed breaches; 145 countries; Nov 2024–Oct 2025). Exploitation 31% of initial access vs credential abuse 13%; credential abuse in 39% of full chains; KEV remediation 26% (was 38%); median critical fix 43 days (was 32); attack-graph exposure finding.

CrowdStrike — 2026 Global Threat Report (24 Feb 2026). Average eCrime breakout 29 min (48 in 2024, 98 in 2021); fastest 27 sec; exfiltration within 4 min in one intrusion; 82% of detections malware-free; 42% of exploited vulns used pre-disclosure; AI-enabled adversary activity +89%.

FBI IC3 — 2025 Internet Crime Report (6 Apr 2026). $20.877B reported US losses (+26%); 1,008,597 complaints; BEC $3.0B; 63 new ransomware variants.

Gartner — Implement a Continuous Threat Exposure Management (CTEM) Program (Oct 2023); Market Guide for Adversarial Exposure Validation (24 Mar 2026).

Deliberately not used: the $10.5T annual cybercrime figure (single-firm projection); "87% breached in the past year" (vendor survey self-report); "$1 on pen testing saves $10" (no published study). The ROI model on slide 26 is explicitly illustrative — every input is stated so it can be challenged.