NO VENDORS WERE HARMED IN THE MAKING OF THIS DECK



CYBERSECURITY

The Big Pharma of Tech

WHY ZERO TRUST WINS

Dr. Louis DeWeaver III • b1kgh0st

They call me the Katt Williams of cybersecurity.
I am not sure if that is a compliment, a warning, or a HIPAA violation.

Spoiler: there is no magic pill. There is a protocol. And it is rude on purpose.

HOUSE RULES

Before we write any prescriptions

01 Authorization first

Ethical hacking means rules of engagement. If you test without permission, you are not a hacker. You are a defendant.

02 No vendor worship

Tools are medicine. Vendors are pharmacies. You still need a diagnosis. Buying 47 dashboards is not a security program.

03 Laugh, then do the work

If the joke lands and the control does not, we failed. Funny is the delivery. Zero Trust is the payload.

04 Assume I am already in

That is not paranoia. That is Tuesday. We design like the attacker has a badge, a VPN, and your help desk on speed dial.

THE ITINERARY

What we are about to do to your mental model

01 The metaphor

Why cybersecurity acts like Big Pharma — recurring revenue, side effects, and no actual cure.

02 The diagnosis

What is actually killing networks in 2026. Spoiler: it already has a badge.

03 The over-the-counter era

Firewalls, VPNs, and hope. How we treated symptoms and called it strategy.

04 The prescription

Zero Trust principles that actually change blast radius.

05 The side effects

Where implementations go to die. And how not to join them.

06 The discharge papers

A starting dose you can take Monday morning.

THE METAPHOR

Cybersecurity is the Big Pharma of tech

Not because security people are villains. Because the business model rhymes.

THE PATIENT

Big Tech + every enterprise that copied them

Always-on platforms. Infinite surface. AI agents with more permissions than your CISO. The organism is huge and slightly allergic to patching.

THE PHARMACY

Vendors, MSSPs, and your tool graveyard

Subscriptions forever. New SKU every quarter. "This dashboard will change everything." It will not. It will generate tickets.

THE DISEASE

Assume-breach reality

Ransomware, stolen sessions, identity abuse, supply chain, unpatched KEVs. The infection is already in the waiting room wearing a lanyard.

THE DIAGNOSIS

The patient is not "at risk." The patient is occupied.

80%

of enterprise servers are reachable from inside once an attacker gets a foothold. East-west is the open bar.

82% / 17%

say Zero Trust is essential. Only 17% have actually finished it. That gap is where ransomware lives.

$1.76M

average breach-cost reduction when Zero Trust is in place. That is not marketing. That is fewer funerals.

Identity

is where the attack unfolds. Credentials, sessions, OAuth grants. The perimeter retired. Nobody sent flowers.

THE OVER-THE-COUNTER ERA

We kept buying cough syrup for a gunshot wound

Castle-and-moat	Works great if attackers honor the moat. They do not. They phish the drawbridge operator.
VPN as identity	Congratulations. You built a long, encrypted hallway into the same flat network. Now ransomware has a tunnel.
More alerts	A SIEM is not a strategy. It is a notification tax. Alert fatigue is just burnout with a dashboard.
"We have MFA"	MFA on the front door and Domain Admin on a sticky note is not a flex. It is a eulogy waiting to be written.
Tool sprawl	26% of orgs say vendor chaos is the #1 Zero Trust blocker. You cannot verify everything if you cannot find the login.
Hope as a control	"We have not been hit yet" is not risk management. It is a calendar appointment you have not opened.

WHY THE OLD MODEL LOSES

Trust is a terrible default setting

THEN

Inside = safe
Outside = scary

That made sense when the office had a door, the servers had a room, and "remote work" meant a hotel fax machine.

Then we invented cloud, SaaS, contractors, BYOD, APIs, and AI agents that can click faster than your SOC can sigh.

NOW

Inside is just another attack path

Once they have a session, they walk servers like a mall. RDP, SMB, WinRM, leftover NTLM — the greatest hits album of lateral movement.

Your firewall is still proud of itself. Your domain is already writing a ransom note in Comic Sans.

THE PRESCRIPTION

Zero Trust is not a product. It is a personality.

John Kindervag did not invent paranoia. He productized good manners for hostile networks.

1

Never trust

Not the user. Not the device. Not the subnet. Not the "trusted" vendor VPN. Especially not the account named admin.

2

Always verify

Identity, device health, context, and the thing they are trying to touch. Every time. Yes, even Bob from accounting.

3

Assume breach

Design so a stolen laptop is an incident, not an extinction event. Blast radius should fit in a sticky note, not a press release.

4

Limit the blast

Micro-segmentation + least privilege. Attackers hate small rooms. Give them closets.

THE ACTIVE INGREDIENTS

Four controls. Zero fairy tales.

IDENTITY

The new perimeter

MFA is the vitamin. Conditional access is the prescription. Just-in-time admin is the surgery. If identity is sloppy, everything else is cosplay.

DEVICE

Prove you are healthy

Managed, patched, encrypted, not jailbroken by a nephew. A compliant laptop is a privilege, not a birthright.

NETWORK

Tiny rooms, locked doors

Micro-seg so Finance cannot talk to the MRI machine "just because." East-west should need a reason, not a subnet.

DATA + APPS

Protect the thing, not the hallway

Classify it. Encrypt it. Log who touched it. If the crown jewels sit in a share named FINAL_FINAL_v3, we need to talk.

WHY ZERO TRUST WINS

It does not promise you will never get sick

It promises the infection stays in one organ instead of becoming a career-ending press conference.

WIN

Smaller blast radius

Compromised account ≠ domain takeover. That single change ends most ransomware fairy tales.

WIN

Identity over location

Work from Vegas, a coffee shop, or a conference Wi-Fi named "FBI Van." Policy follows the user, not the building.

WIN

Measurable outcomes

Fewer standing privileges. Faster containment. Lower breach cost. Boards understand dollars. Speak dollars.

WIN

Works with the mess

Hybrid, multi-cloud, contractors, IoT that cannot run an agent. ZT is a strategy for ugly reality, not a greenfield fantasy.

SIDE EFFECTS • READ THE LABEL

How to turn the cure into poison

Buy the logo, skip the architecture

Renaming your VPN "ZTNA" does not count. Kindervag is not impressed. Neither is ransomware.

Boil the ocean on day one

If the plan is "Zero Trust everything by Friday," the plan is a resignation letter. Pilot a crown-jewel app. Win. Expand.

Ignore identity hygiene

Orphaned accounts, shared admin, standing Domain Admin. That is not technical debt. That is an unlocked pharmacy.

Forget the humans

If help desk cannot reset without drama, users will invent shadow IT. Usability is a control. Fight me.

No telemetry, no truth

You cannot verify what you cannot see. Logs, device posture, and identity signals are the bloodwork.

One vendor to rule them all

Platforms help. Religion does not. Keep the principles. Swap the pills if they stop working.

DISCHARGE INSTRUCTIONS

A starting dose you can take Monday

1

Map one crown-jewel path

User → device → app → data. Draw it ugly. If you cannot draw it, you cannot protect it.

2

Kill standing admin

Privileged access should expire like milk, not like a national monument.

3

Segment something real

Pick a high-value zone. Stop "any-any" like it owes you money.

4

Tighten identity

MFA everywhere it matters. Conditional access. Review OAuth grants. Yes, the creepy ones.

5

Measure blast radius

Ask: if this account dies, what else dies? If the answer is "the company," keep cutting.

6

Write the story for the board

Risk reduced, cost avoided, audit evidence. Funny talks get rooms. Numbers get budgets.

IF YOU REMEMBER NOTHING ELSE

The whole talk on one slide

1. The industry sells treatments. Zero Trust is closer to a diet: annoying, daily, and the only thing that works long-term.
2. Perimeter trust is a bedtime story. Identity, device, and data are the adults in the room.
3. You will still get compromised. The win is that it does not become a company-ending event.
4. Start small, measure blast radius, and do not confuse a purchase order with a program.
5. Funny keeps people awake. Controls keep them employed. Bring both.

ETHICAL FOOTNOTE

Think like a hacker. Act like an adult.

Zero Trust is how we design systems that survive hostile intent.
Red teaming is how we prove it.
Authorization is how we stay out of federal custody.

If you take one sentence from the so-called Katt Williams of cybersecurity, take this:

Never test without authorization. Never confuse a demo with permission. Never let a punchline outrun the rules of engagement.

The truth still matters. So does the paperwork.

Q & A

Ask the hard questions. I will give the unpretty answers.

If your question starts with "which vendor," I will answer with "which problem."

No magic pills. No sacred tools. No implicit trust.

GO FORTH AND VERIFY

Dr. Louis DeWeaver III

b1kgh0st
Sometimes known as the Katt Williams of cybersecurity
(still waiting on the official diagnosis)

Assume breach. Limit the blast. Tell the truth.
Then go home before the help desk pages you.

