Plumcot

The Security Correlation Problem

Why Your Security Tools Give You Three Different Answers

The CISO pulled up the quarterly risk report. Something was off.

Defender said 847 vulnerable endpoints. Qualys said 1,203. CrowdStrike showed 412 high-risk detections.

Three tools. Three numbers. Three versions of the truth.

The board meeting was in two days. She needed one answer.

The Problem Nobody Talks About

Every security team has this problem. They just do not talk about it.

You buy best-of-breed tools. Defender for endpoint security. Qualys for vulnerability scanning. CrowdStrike for EDR. Each one is excellent at what it does.

But none of them talk to each other.

So you end up with three dashboards. Three risk views. Three different answers to the same question: what is our actual risk posture?

The Spreadsheet Solution

You know what happens next. Someone builds a spreadsheet.

Export from Defender. Export from Qualys. Export from CrowdStrike. Paste into Excel. Build formulas. Reconcile duplicates. Normalize asset names. Try to match endpoints across systems.

It takes days. It is out of date the moment it is finished.

And next quarter, you do it all over again.

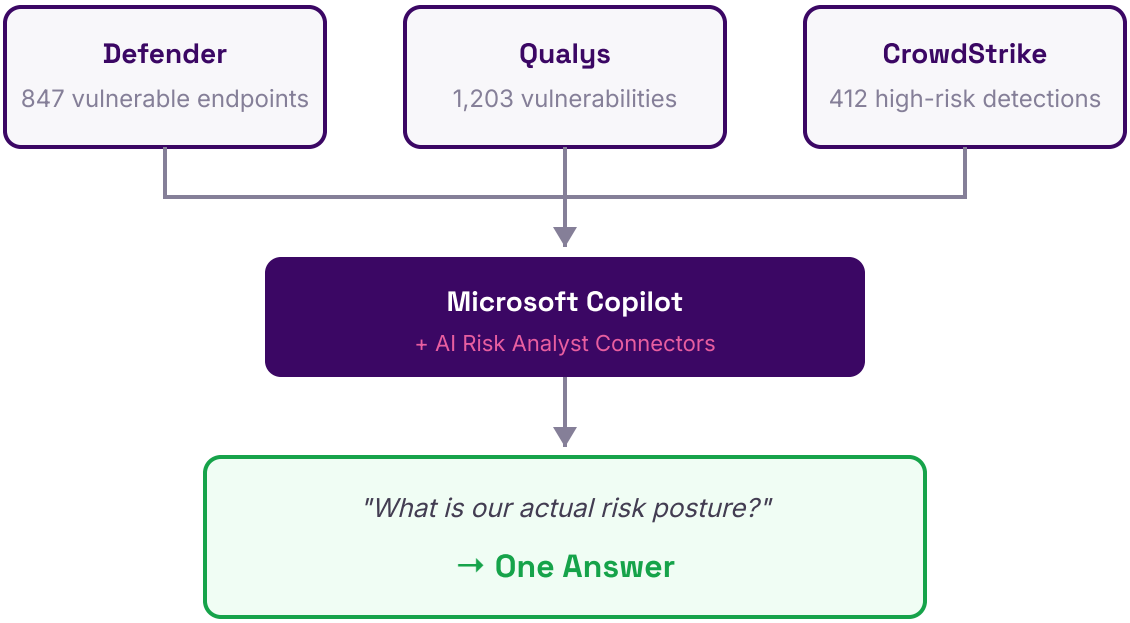
The Conversational Layer

What if you could just ask?

Connect your security tools to Copilot. Then ask questions in plain language.

ASK QUESTIONS LIKE:

- *Which endpoints are in Defender but missing from Qualys?"*
- *Show me vulnerabilities that appear in multiple tools."*
- *What is our actual risk posture when you correlate all three?"*
- *Which assets have the highest combined exposure?"*



No spreadsheets. No manual correlation. Just ask.

What the AI Does

Asset correlation.

Same endpoint, different names in each system. LAPTOP-47829 in Defender. 10.0.1.45 in Qualys. Workstation-Marketing in CrowdStrike. The AI knows they are the same machine.

Vulnerability deduplication.

Defender found CVE-2024-1234. Qualys found the same one. CrowdStrike flagged the exposure. The AI counts it once, not three times.

Risk scoring normalization.

Qualys uses CVSS. CrowdStrike uses their own severity model. Defender uses threat levels. The AI maps them to a single framework your board can understand.

Gap identification.

Which assets are in Defender but missing from Qualys? Which vulnerabilities does CrowdStrike see that your scanning tools missed? The AI finds the gaps.

Conversational interface.

Ask follow-up questions. Drill down on specific assets. Explore the data the way you think about it.

The Outcome

One truth. Accessible by asking.

The CISO walks into the board meeting with one number. Not three numbers she has to explain away.

When the CFO asks about cyber risk, there is one answer. Not "well, it depends on which tool you look at."

When audit asks for evidence, there is one source. Not three exports stapled together with formulas you hope are correct.

What It Takes

The AI Risk Analyst connects to your existing tools. No rip and replace. No new agents to deploy.

Keep Defender. Keep Qualys. Keep CrowdStrike. Add a conversational layer that makes them work together.

Uses your existing Microsoft Copilot licenses. The capability sits on top of what you already have.

The Point

> *Your tools are not the problem. The gap between them is.*

You hired experts. You bought best-of-breed. You still have three versions of the truth because nobody built the bridge between them.

Until now.

Want to Ask Questions Across Your Security Tools?

Your tools, your gaps, what conversational correlation looks like.

Book a Call

30 minutes. See your risk data unified.

Plumcot

plumcot.ai · pgoyal@plumcot.ai