# Rethinking Cybersecurity: Making Proactive Defense Affordable and Available in the age of AI.

MARCH 19

AUTNHIVE INC
Authored by: Devi Narayan

# Rethinking Cybersecurity: Rethinking Cybersecurity: Making Proactive Defense Affordable and Available in the age of AI.

Foreword from our CEO,

Cybersecurity is broken. For years, companies have thrown money at firewalls, antivirus software, and security teams—only to get hacked anyway. The truth? Traditional security isn't built for the AI-driven threats we face today. Attackers are evolving faster than defenders. The old approach—react, patch, repeat—is a losing game.

At Authnive, we don't play that game. We rewrite the rules.

We built an AI-powered security platform that makes cybersecurity defendable, defensible, and actually useful. Our work is recognized by experts from all kind of organizations ranging from U.S. Department of Defense, Intelligence agencies, Enterprise, MSSP's, Educational Intuitions and more.  We've got 27 patents issued, 32 more pending, and partnerships with governments and top institutions.

Security shouldn't be an expensive mess of tools that don't talk to each other. It should be available, affordable, and intelligent. That's why we built SAMI, an AI-driven system that turns cybersecurity noise into real intelligence—reducing liability, automating risk assessments, and stopping threats before they happen.

The further of cybersecurity isn't about waiting for an attack and scrambling to fix it. It's about seeing the cyber and business risks and cutting liabilities before they become disasters. That's what we do.

This article isn't just about security. It's about changing the way we think. The goal? Help you ask the right questions so you can build a real, practical, and complete defense in the AI era.

Devi Narayan
CEO & Founder, Authnive.

1. **CURRENT STATE OF CYBERSECURITY?**
   a. Cybersecurity is the art of protecting digital systems, networks, and information from unauthorized access, cyber attacks, and threats. Traditionally, cybersecurity has been a means to prevent threat actors from accessing an organization's IT environment and sensitive information.
   b. With the emergence of sophisticated threats such as AI driven attacks growing digital profile and risk for organizations, both enterprise and Small and Medium (SMB) organizations are increasing at risk, and such reactive thinking is no longer sufficient. The greater exposure to risk requires a more strategic defense.
   c. It is unrealistic and dangerous for organizations and security professionals to state their goal is to completely eradicate all cyberattacks/breaches. This kind of thinking places them in an untenable position, making them more personally at risk. For instance, companies promising complete security could suffer legal, financial, or reputational costs when a unavoidable breach happens. (Examples might be data breaches in spite of best practices, legal liability for not disclosing threats, or CEOs and CISOs being personally held responsible for security breaches.)

2. **THE EVOLVING CYBERSECURITY THREAT LANDSCAPE**
   a. As AI and automated bots are employed by cybercriminals to test vulnerabilities and launch attacks, every enterprise—large and small—is on the target list. Traditional security methods no longer suffice.
   b. With security talent in short supply and security budgets competing with other business objectives, businesses need a smarter solution. By making security Available (Defendable and Defensible) and Affordable, businesses can build a strong, long-lasting defense addressing real-world problems and sustained success.
   c. Traditional cybersecurity requires the support of numerous tools and resources to create a Defendable and Defensible security. Even though this abundance of tools theoretically raises protection, deployment proves challenging for organizations of all sizes:
      i. **Small and Medium Businesses (SMBs):** Lack the financial and operational means to maintain strong security.
      ii. **Enterprises:** They can afford the budget, but their enormous online presence multiplies risk, making end-to-end protection challenging. High-profile breaches are characterized by such challenges. Toyota has experienced various compromises in recent years, and T-Mobile was breached nine times in four

years. These were not due to cost constraints but the challenge of having security availability at scale.

d. **LIMITATION OF TODAYS CYBERSECURITY: Known Devil and Unknown Angel, A Learning from Abraham Wald**

i. Likely one of the most common mistakes organizations make in cybersecurity is prioritizing apparent vulnerabilities over unseen risk and liabilities.

ii. World War II military strategists analyzed returning planes filled with bullet holes to decide where armor plating should be placed. The logical conclusion was to reinforce the damaged areas. But statistician Abraham Wald recognized a fatal flaw in this strategy, survivorship bias.

iii. He argued that the observable holes were representative of damage planes may have endured, but those planes hit in critical areas (such as the engine or cockpit) never returned and therefore did not appear within the statistics. Instead of reinforcing the most damaged areas, Wald proposed the reinforcing of those areas with minimal to no damage whatsoever, as these would have been where planes were severely damaged and therefore never returned.

*Wald's airplane A hypothetical diagram of known bullet holes in returning airplanes, illustrated as red points.*

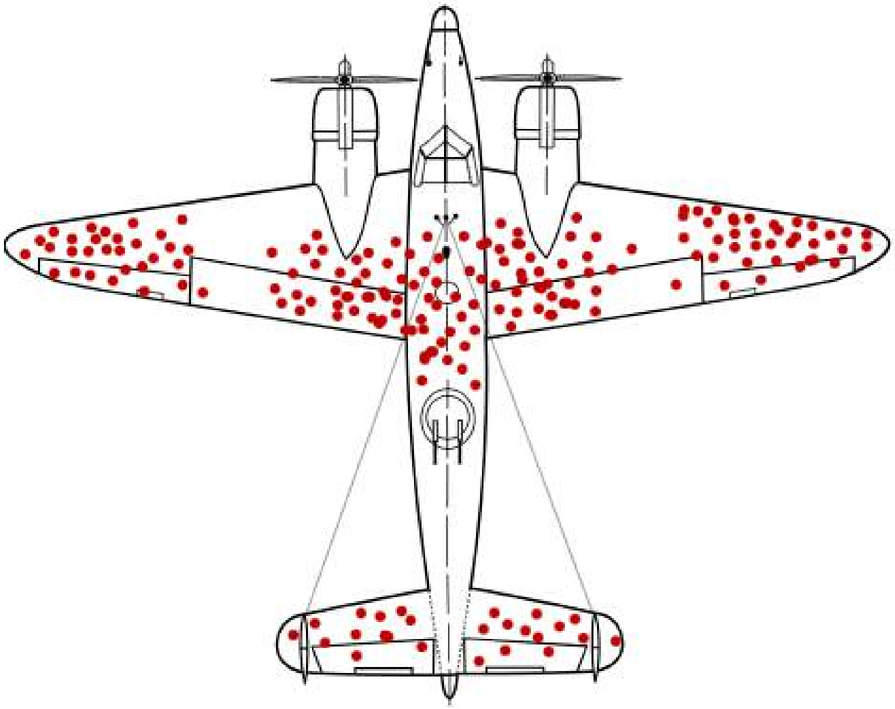


*Image courtesy: McGeddon, Wikimedia Commons user.*

iv. Wald's recommendation significantly is improved the rate of survival of aircraft. By redirecting attention from visible damage and developing the riskiest points of damage as more resilient, the military managed to reduce losses when fighting and enhance the chances of planes returning safely.

v. This knowledge altered war and is an example of how actions based on information at hand with out converting it to knowledge (see Devi's Triangle below to know about Data, Information and Knowledge) will lead to erroneous conclusions. The same bias occurs in cybersecurity today: businesses focus on visible vulnerabilities and ignore unseen risk to business that may be significantly more dangerous to business liabilities.

vi. In his research paper "The Bullet Holes We See"[1] Juan Pablo Castro, a seasoned security expert with two decades of security experience, discusses Abraham Wald's lesson and how it can be applied to cybersecurity. He points out the way that security teams tend to focus on visible threats while neglecting less apparent but no less important risk and liabilities.

vii. While firms spend vast amounts on reactive and proactive security solutions to identify and act against obvious risks, they tend to be making the same efforts that WWII intelligence analysts made by acting on information instead of knowledge (see Devi's Triangle below to know about Data, Information and Knowledge).

viii. By merely acting on what they can see ie. information from the tools, they ignore unseen threats such as financial, operations, and compliance risks, unpatched third-party vulnerabilities, penetration testing gaps, red teaming discoveries, and threat intelligence etc.

ix. Real cybersecurity resilience entails correlating these inputs to overall vulnerability risk to detect and remediate unseen vulnerabilities to reduce liabilities.

## 3. PRACTICAL AND MORDEN APPROACH TO TANGIBLE LIABILITY REDUCTION

a. Building a available and affordable security system for an organization requires a unified platform and vision. Such a unified platform and vision, will help businesses to build a strong, long-lasting defense addressing real-world problems and reduce liabilities. In order to be effective at all, cybersecurity must be:

i. **Available** – Security solutions must be made available to all the key stakeholders, not just cybersecurity teams. IT, executives, compliance officers, and other decision-makers must have access to simple-to-use, autonomous security solutions that minimize complexity and human intervention. In order to make security available to everyone, it must be Defendable and Defensible.

1. Defend and Defense: When an attack is launched, organizations are not only required to defend against the attack but also have a defense (justification), usually such a defense is mounted by their security team, regulatory, compliance team, and business team, executive team etc. A defensible cyber strategy eliminates financial, legal, and reputational risks while promoting resilience and accountability.

ii. **Affordable** – Security should not be an expensive overhead. Organizations of any scale ought to be able to implement defendable and defensible protection without endangering their funds. Cybersecurity should provide a clear return on investment in the sense that defense is both justified and sustainable.

## 4. CHALLENGES IN IMPLEMENTING THIS PRACTICAL, MODERN APPROACH

a. To implement this modern approach to cybersecurity effectively, it is critical to determine when, where, why, and in what order security actions must be triggered in order to maximize liability reduction.

b. Traditionally, cybersecurity professionals analyze security device data to make decisions. However, this is not scalable or sustainable due to its heavy reliance on large numbers of security personnel.

c. Such experts not only install, operate, and maintain security equipment but also translate raw data into actionable intelligence for IT personnel – this latter aspect depends on the experience and expertise of the professional and is therefore hard to scale and standardize.

d. The assignment becomes even greater in the face of resolving compound, strategic problems beyond the competency of traditional security technology. An example is, in answering chief questions like "Why and in what order must I remediate security threats for the best chance to reduce liability?" security, business, legal, and fiscal expertise etc are needed.

## 5. CLOSING THE GAP: FROM PROBLEMS TO INTELLIGENCE

a. The increasingly sophisticated nature of cybersecurity and the need to rely on expert professionals to interpret and act upon security data makes the traditional model unavailable and unaffordable.

b. Organizations need a more normalized and scalable approach—a one that transcends data collection for security and instead translates it into actionable intelligence that supports superior decision-making.

c. It is from here that understanding what differentiates Data, Information, and Knowledge is critical. Without it, security teams are left with a snowstorm of alerts and bare signals without the right guidance on what matters.

d. To achieve this, we introduce the Devi’s Triangle, a framework that turns intimidating security data into real, usable intelligence. Through the application of this structured approach, organizations are able to successfully prioritize threats, reduce liability, and achieve maximum cybersecurity controls without overly relying on human inference.

## 6. DEVI'S TRIANGLE: CONVERTING NOISE TO ACTIONABLE INTELLIGENCE

a. The Devi's Triangle is the practice of turning raw security data into actionable intelligence.  Cybersecurity today is like drinking from a firehose, tons of data, endless alerts, no sense.

b. Most security solutions dump you with data and may even convert them into information, acting on such information without converting to knowledge is risk as we saw before.

c. That's where the Devi's Triangle comes in. The Devi's Triangle helps you understand the difference between data, information and knowledge and helps you ensure that you are acting on knowledge rather than information.

d. **Data (Raw Signals) -** Data is individual pieces of facts that lack context. On their own, they do not provide enough meaning to make decisions.

   i. General Example:

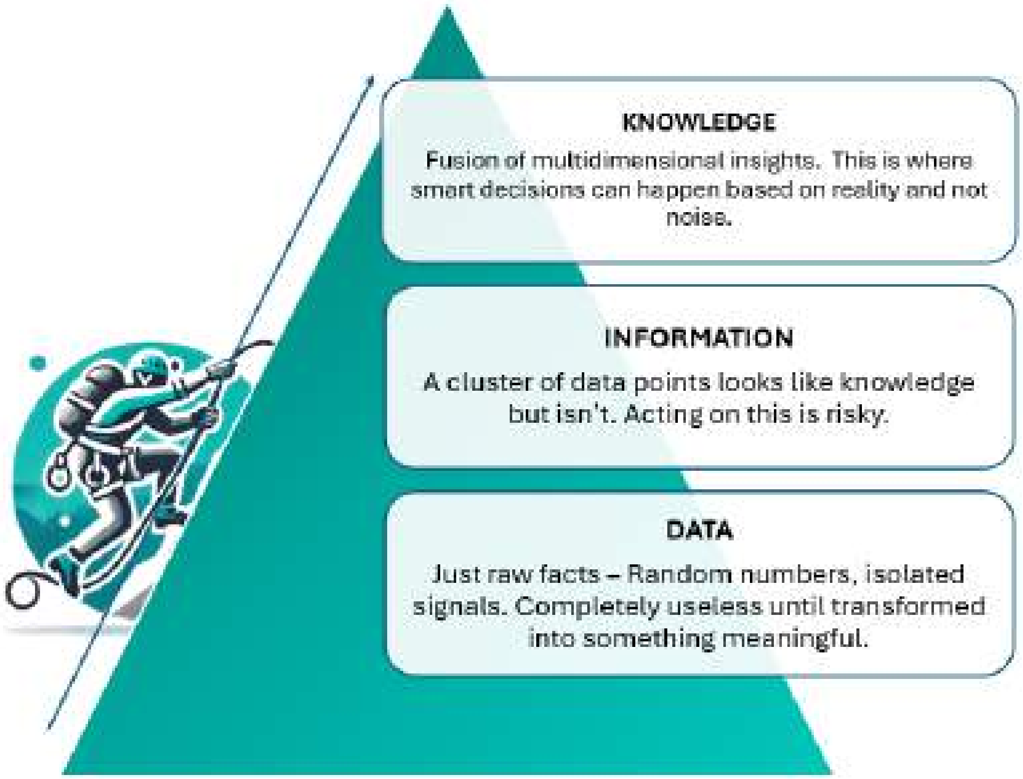
      1. “105”, “Body Temperature”, “John”
      2. On their own? Completely meaningless. These are just random facts floating in space.

   ii. Cybersecurity Example:

      1. Your vulnerability scanner detects CVE-2025-XXXXX.
      2. Great. So what? What is the risk for you? Is anyone taking advantage of it? Does it even matter? How to correct it? And many more questions remain unanswered.

   iii. At this point, data is merely a puzzle with missing pieces. It informs you that something exists but not why you should care.

### Devi’s Triangle



KNOWLEDGE

Fusion of multidimensional insights. This is where smart decisions can happen based on reality and not noise.

INFORMATION

A cluster of data points looks like knowledge but isn't. Acting on this is risky.

DATA

Just raw facts – Random numbers, isolated signals. Completely useless until transformed into something meaningful.

e. **Information (Context and Correlation)** – Information is created when multiple data are connected to provide some context. However, information alone isn't always actionable.

   i. General Example:

      1. Now let's connect the dots: John + Body Temperature = John's temperature is 105°F.
      2. Helpful, but not exactly. Is something amiss? Is he sick? Do we need to act? We do not know yet.

   ii. Cybersecurity Example:

      1. Your scanner now co-relates data and gives you with more information: CVE-2025-XXXXX and it is a categorized as critical by security agencies, its risk scoring, where it is found and even how to fix it.
      2. But we don't know yet how it will affect our liabilities. Ie. who is exploiting these problems, what can be the cost and operational losses, are there other policy violations or vulnerabilities that could make this riskier and what order should the correction of these problems by be accomplished to keep the liability reduced as much as possible.

3. You have context here, but no priority or correlation. Do you leave all of it to fix it, or is there a bigger risk somewhere else?

f. **Knowledge (Context & Correlation) –** Knowledge is generated if multiple cross dimensional information are connected to each other in such a way that they communicate some level of context. Now We Know What to Do, here decisions are taken.

i. General Example:

1. Now lets connect three pieces of cross dimensional information, (1) John's temperature is 105°F (2) Normal body temperature is 97-99°F (3) If the temperature is over 98 Tylenol has to be administered.
2. Now with the above knowledge the doctor concludes that John's temperature is high enough to administer Tylenol and he administers it. By action on Knowledge the doctor has defended John against the high temperature and he also put himself in a defensible position that reduces his liabilities.

ii. Cybersecurity Example:

1. Now, let's take your vulnerability intelligence to the next level:
2. The vulnerability (CVE-2025-XXXXX) is being actively exploited by ransomware gangs. If compromised, your company may suffer $2M in financial losses + regulatory fines. It exists in conjunction with other vulnerabilities that may amplify the attack. A risk model puts this your #1 priority because it impacts revenue-critical systems.
3. Now you KNOW this is bad. Now you have real intelligence—not alerts. Now you know just what to address first.

g. Most cybersecurity products today truncate at information–they call actionable intelligence, however true actionable intelligence that reduces your liability is obtained only from Knowledge.

h. You have to always ask yourself if you are acting on information or knowledge. Converting information to knowledge is resource intensive and doing it through cyber-security resources is expensive and wasteful.

i. **Security isn't about knowing everything, it's knowing what matters** – By automating conversion of Data to Knowledge, you're saving time, money, and resources.

## 7. PROACTIVE AND REACTIVE CYBERSECURITY

a. With this understanding of how Affordable and Available cybersecurity can reduce liability while being scalable to businesses of all sizes and shapes, the question then becomes where and how it should be implemented to give a complete and realistic security plan. Cybersecurity must be proactive and reactive to enable organizations to avoid attacks as well as react well when the attack does occur.

i. **Reactive Security** - Reactive security comprises products and methods used that helps during or after a cyber attack to mitigate damage and restore functions. These products help organizations respond to threats, limit damage, and restore normalcy after an attack. Key examples include but are not limited to:
   1. Extended Detection and Response (XDR)
   2. Antivirus and Endpoint Protection
   3. Data Backup and Recovery
   4. Forensics and Incident Response
   5. IAM Systems etc.

ii. **Proactive Security-** Proactive security targets risk detection and diminution before the occurrence of an attack and the resulting in reduce liabilities. With hardening across an entire orgnaisation infrastructure, proactive security measures secure the security gaps before exploitation. Proactive measures include but not restricted to:
   1. Risk Assessments on
      a. Endpoints
      b. Third-Party & In-House:
         1. Mobile Application Risk Assessment
         2. Application Risk Assessment
         3. Firmware Risk Assessment
      c. M365
      d. Google Workspace
      e. Software Source Code
      f. Cloud & Container
      g. Network
      h. Self and Vendor External Attack Surface Risk Assessments
      i. Dynamic Application Security Testing
      j. Infrastructure-as-Code (IaC) Risk Assessment
   2. Security Testing & Intelligence
      a. Penetration Testing
      b. Red Teaming (Simulated Cyber Attacks)
      c. Threat Intelligence
   3. Cyber-Related Business Risk Evaluation
      a. Cyber-Related Financial, Operational, and Compliance Risk Assessment

4. Knowledge Creation Through Correlation
    a. Effective security isn't merely about finding vulnerabilities—it's about knowing their implications. Proactive security allows organizations to correlate points of data and respond to fundamental questions, including:
        1. What are the risks in our environment?
        2. Who is targeting us actively?
        3. What are the most prevalent vulnerabilities attacked by attackers?
        4. How would an attack impact our finances, operations, and compliance position?

b. Using proactive security technologies, organizations gain broad visibility into threats, which allows them to prioritize remediation and reduce risk before it's an active attack.

**8. THE CHALLENGE OF PROACTIVE SECURITY**

a. Making proactive security affordable and accessible is a significant challenge because it requires them to use more than one tool, resource, and time—luxuries few organizations can afford.

b. In contrast to reactive security, which tends to be standardized and automated, proactive security entails ongoing assessments, intelligence gathering, and risk / financial / compliance  and other analysis, co-relating these information to form knowledge, all requiring skilled staff and substantial investment.

**9. AUTOMATING PROACTIVE SECURITY – SAMI**

a. Automation is the solution to this gap closing. SAMI (Security Assisted by Machine Intelligence) has been designed to make proactive security more automated, with fewer reliance on human abilities while still enabling business to gain actionable knowledge and indeed reduce their liabilities.

b. Using state of art technologies, techniques and concepts such as but not limited to advanced scans, integrations, AI, algorithms etc, SAMI automates proactive cyber-security like none other, to provide organizations affordable, available, scalable, and effective proactive security. Making preventive measures as accessible as response mechanisms have been in the past.

c. SAMI is built to brige the gap between security team and other stake holders and allows security providers to:

    i. Minimize liability by automating defensible proactive defense processes.

    ii. Minimize expenses by streamlining proactive security operations and reducing the necessity to utilize multiple tools and number of personnels required to acquire, analyze and co-relate visible and hidden risk data.

iii. Stand out from the competition by offering integrated, proactive security solutions to customers that covers a vast array of their digital foot print.

iv. Maximize customer loyalty by automating security reporting to non-technical stakeholders so that clients can visually comprehend the ROI on their security investment.

v. Provide seamless upstream and downstream integrations with other security and productivity tools.

## 10. SAMI CHANGES THE GAME

Want to see how SAMI makes cybersecurity proactive, affordable, and actually useful? Reach out to us and let's talk.

CITATION:

Castro, J. P. (2024). *The bullet holes we see: Abraham Wald's WWII lesson applied to cyber risk management*. ResearchGate. https://www.researchgate.net/publication/389840248_The_Bullet_Holes_We_See_Abraham_Wald's_WWII_Lesson_Applied_to_Cyber_Risk_Management