AUTNHIVE
ELEVATE SECURITY

Cybersecurity That Keeps you Ahead

How AI-Powered Threat Exposure Management Protects Your Business and Bottom Line

AUTNHIVE
ELEVATE SECURITY

Foreword

Cybersecurity is broken. If companies spend billions on tools and resources, why do we so often see security breaches and liability increases? Because they're fighting today's war with yesterday's weapons. It's reactive, slow, and fragmented.

Right now, security means stacking expensive tools that flood you with data. Some of these tools may convert this data into information. But acting on raw information? That's risky. So companies spend even more—hiring expensive talent just to translate it into knowledge - something useful that can be acted upon, only then can they attempt to reduce liability.

It's inefficient. It's backwards. It's broken.

Cybersecurity doesn't need to be complex. It needs to work. The future of cybersecurity isn't about waiting for an attack and scrambling to fix it. It's about seeing the cyber threats and business risks and cutting liabilities before they become disasters. That's what we do.

Meet SAMI — *Security Assisted by Machine Intelligence*. A fully autonomous AI platform that makes proactive risk management simple, smart, and effective. It cuts through noise and helps reduce real business liability.

Backed by 28 patents, reviewed by the US Department of Defense, 5-Eyes intelligence agencies, enterprises, MSSPs, and leading universities, we're not tweaking the past. We're building the future.

SAMI is designed to be affordable, available, and adaptable, for critical infrastructure enterprises and SMBs alike. We are compliant with global standards like NIST Zero Trust Architecture (data), GDPR, ISO 27001, HIPPA, CCPA, SBOM, CSA Star, 21-CFR 211 (US FDA Pharmaceutical's) 21-CFR 117 (US FDA Food).

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, Autnhive

AUTNHIVE
ELEVATE SECURITY

Executive Summary

Cybersecurity is not just an IT issue — it's an issue of business survival. While investing in cybersecurity can be costly, the consequences of a data breaches have never been more dire — fines, downtime, and reputational damage. How do businesses manage this difficult position between costly risk management and even costlier potential outcomes? To date, manual risk assessments along with multiple disparate tools have been the primary defense, but the process is slow, expensive, fragmented and it fails to consider the effects the cyber-risks can have on the organization while prioritizing remediations.

SAMI (Security Assisted by Machine Intelligence) is a new AI-assisted tool by Autnhive for continuous risk and liability management. By replacing manual review (resource-intensive in terms of tools, people, and money) with a unified AI-assisted platform for assessment and analysis, SAMI reduces costs, streamlines processes, and makes it manageable for organizations of any size to maintain a more robust threat management system than ever. For executives, MSPs, and MSSPs looking for an edge, this approach is faster, smarter, and more defensible than legacy approaches to cybersecurity.

The Problem with Traditional Approaches to Cybersecurity

Many executives treat proactive cybersecurity as an IT problem — most likely so they can hand it off to the IT team and not have to think about it, preoccupied as they are with hundreds of other fires to put out every day.

But it's not merely an IT problem, it's an existential problem for the whole business. In 2024 the average cost of a cyber breach tipped the scales at $4.88[1] million, the largest ever and a whopping 10% increase from the previous year.

Imagine if a $4.88 million sales pipeline just disappeared overnight, or you got $4.88 million in excess return orders. Would *that* be merely an IT problem?

And then there's the dire statistic that 60% of small-to-medium-sized businesses that experience a data breach close their doors for good within six months[2]. This is not just an IT problem — it's a *business* problem, and an existential one at that.

The Heavy Resource Investment of Cybersecurity

Despite the dire nature of the risk, most companies are stuck with woefully inadequate or unsustainable proactive cybersecurity strategies and protocols. For example:

- Microsoft 365 and Google Workspace, Cloud Review, CIS Benchmarking require tedious manual review of settings and configurations, requiring specialized knowledge and manual compiling of reports over a period of weeks.
- Expensive device security scans often neglect surfaces for "Living Off The Land" attacks and OS-level risks, software and its component (Supply chain) level risks.
- Binary risk analysis on third-party or in house applications involves exhaustive reverse-engineering, component mapping, threat/business liability correlation, documentation, and more, making it hopelessly unscalable. Additionally, it only targets the source code, not the compiled code you will encounter in the real world.
- Mobile app security assessments, if conducted, rarely digs beyond surface-level threats unless security teams engage in extensive, time-consuming efforts to understand the components involved, risks within the components (eg.Log4J attack), IP addresses these applications are talking to, the companies that owns these IP's, their geo-graphic locations etc.
- Vendor risk assessment is expensive.
- Penetration tests ("pentests") can take 2-3 days to perform on a small website and even more time to report on. The tests generate vast quantities of data from which "true positives" vulnerability must be manually identified, and even then they only represent a snapshot in time, not a continuous scan of the system.

These are just a handful of examples of things you have to do to reduce the risks for your organization.

The list goes on and on — firmware assessments, dynamic application security testing (DAST), network security ... every one of them expensive, tedious, resource-intensive, unscalable, and frequently overlooked.

In addition to the cumbersome nature of manual cybersecurity protocols, most organizations rely on a patchwork of tools that don't talk to each other. And even if human labor were preferable to AI automation, there aren't enough cybersecurity professionals to go around as the world sinks into a global cybersecurity personnel shortage.

Managing risk isn't the same thing as managing the liabilities associated with it. Businesses need to focus on reducing risks based on the liabilities those risks could create. Take a vulnerability, for instance—it could lead to liabilities such as data breaches, hefty regulatory penalties, or increased insurance exposure. So liability based cyber-risk reduction is an existential business issue to be taken up in board rooms, not IT departments.

Why Cybersecurity Routinely Fails to Identify True Business Liabilities

Even with the heavy investment of resources, the traditional approach to proactive cybersecurity is shockingly inadequate to the task of properly identifying true business liabilities.

Why is this?
It stems directly from the fact that **so many companies treat cybersecurity as an IT problem rather than a business problem.**

A multitude of current cyber-security tools and resources are needed to identify **risks and threats**, but they are very bad at identifying corresponding business **liabilities.**

- **Risks** — an area of vulnerability.
- **Threats** — a bad actor who might try to exploit the vulnerability.
- **Liabilities** — the actual consequences to the business where a threat to exploit that risk.

Why is liability-based cyber management important?
Consider this scenario: Two cyber-risks are identified in your system. One is labeled a critical cyber risk found on your website, but if exploited, it would have minimal business impact. The other is labeled a *medium* risk but exists within your cloud storage, which holds sensitive customer, employee, and business data.

So which one would you fix first?
From a business standpoint, it makes far more sense to address the cloud-based risk first. It's not the bigger risk, but it's the bigger *liability*. Unfortunately, today's cybersecurity prioritization methods typically rank threats based purely on technical severity, without factoring in real-world business consequences. As a result, organizations may overlook the issues that pose the greatest actual liability.

To achieve such liability-based risk management takes much more than raw data on risks and threats. Vast quantities of data must be meticulously collected, indexed, and converted into information. Then relevant information must then be parsed to form actionable knowledge — a painstaking and cumbersome process by modern methods.

- **Data** – Raw facts - Random numbers, words etc completely useless until transformed into something meaningful.
- **Information** – Cluster of data points, looks like knowledge but isn't – acting on this can be dangerous.
- **Knowledge** – Synthesis of multi-dimensional information – this is where smart decisions can happen based on reality instead of noise.

This reveals two fatal problems with the traditional, human-driven approach to proactive cybersecurity. First, a multitude of traditional tools and resources are required to collect risk, threat and business data from limited types of assets. Secondly, most tools only collect data. At the very best, some tools may convert data to information in a limited way, but almost none of them produce actionable *knowledge (this helps you understand your liabilities)* by default. Converting data to information and information to knowledge is a manual and inefficient process – and hence, it is largely overlooked, to the great peril of the organization.

CTEM: The Future of Cybersecurity

Given the obvious limitations of the "risk based" approach to proactive cybersecurity the paradigm is shifting to **CTEM — Continuous Threat Exposure Management**.

As opposed to cumbersome cyber-risk based audits, CTEM adopts a paradigm of ongoing visibility, prioritization and action based on what matters to the business the most

"Zero risk" is impossible to achieve, but continuous risk, threats and liability assessment (as opposed to periodic snapshots) empowers organizations to understand evolving risks, threats & liabilities and prioritize the biggest or most consequential risks.

According to Gartner (2024), "By 2026, organizations that prioritize security based on Continuous Threat Exposure Management (CTEM) will see two-thirds fewer breaches."

So what's the problem? If periodic audits (pen tests, DAST, mobile app assessments, M365 assessments, etc.) are cumbersome and expensive, imagine the expense and resource drain it would take to maintain **constant** surveillance for business risks and threats from an already-limited pool of human cybersecurity experts, along with the additional resources it would take to correlate exposed vulnerabilities to business liabilities. For most organizations, it's out of the question under conventional cybersecurity practices.

AUTNHIVE
ELEVATE SECURITY

SAMI: Solution to affordable CTEM

SAMI (Security Assisted by Machine Intelligence) by Autnhive disrupts that conventional standard. It's an AI-assisted platform that automates the discovery, documentation, analysis of risk, threats and business impact to facilitate remediation or mitigation of risks based on business liabilities.

SAMI works across a wide range of internal and external assets – from **end points** to servers, mobile apps to M365, **cloud, mobile, desktop applications, firmwares**, and much more – to constantly scan, assess, and prioritize security vulnerabilities and associated liabilities. It's like having full teams of cybersecurity, analytics, financial, compliance, and IT experts all working together on demand – minus the delays, headcount, cost or tool sprawl.

Whereas the standard pentesting or M365 / google drive/ third party android/iOS / desktop applications etc. can take a weeks to months to produce actionable insights (by which point the data is already practically out of date),

SAMI produces the same result with as little as 30 seconds of manual intervention, and by non-technical personnel.

Once initiated, it will run continuously. Results that take weeks and months to produce manually take hours with SAMI, sometimes even minutes. Its complex computing model identifies and analyses risks, threats and liabilities based on global and local industry landscape helping organizations prioritize the risks with the most tangible potential business consequences.

Best of all, **SAMI is easy to use**. Simply copy/ paste a website into the platform interface and let SAMI go to work. It can initiate reports within seconds and then run continuously in the background. It's user-friendly enough for end users, managed service providers (MSP) and managed security service providers (MSSP).

AUTNHIVE
ELEVATE SECURITY

Key Benefits of SAMI

There are many benefits to SAMI, but primary among these is that SAMI goes beyond risk and threat identification and expands all the way to actual potential consequences to the business. Not just raw data or even processed information, but actionable knowledge.

Put simply, it empowers organizations to treat cybersecurity as the business problem that it is, without a heavy expenditure of extra resources. It does all this with many more benefits too, including:

Speed and Efficiency

SAMI turns days of manual work into seconds of human interaction to setup. After initial setup, it runs on its own, no humans needed. It maps risks to real business impact continuously, Better yet, it eliminates the need for manual report generation. Fully autonomous. Insanely efficient.

It also includes **Assisted Autonomous Remediation features** for a limited but expanding list of assessment categories to streamline and automate the process of remediating risks.

Consider the following a few estimated time comparison of SAMI vs. human resources or consultants across a variety of cybersecurity vectors:

Process	Traditional User Action Time*	SAMI User Action Time*
M365 Security	4-6 weeks w/ huge people & tool bandwidth	~ 1 minute**
CIS Windows Security	10-15 days w/ huge people & tool bandwidth	~ 1 minute**
Binary Risk Analysis	5-6 weeks w/ huge people & tool bandwidth	~ 1 minute**
Firmware Assessment	5-6 weeks w/ huge people & tool bandwidth	~ 1 minute**
Mobile App Security	4-6 weeks w/ huge people & tool bandwidth	~ 1 minute**
Penetration Testing & Reporting	3 to 7 Days w/ people & tool bandwidth	~ 1 minute**

** User Action Time: The total amount of time it takes for a human user to perform all necessary actions from the initiation of a scan to the generation of a report.*

*** This time measurement applies only to the initial scan setup, while the Autonomous Analysis and Assessment process may take longer, typically no more than a few hours, it operates entirely without human intervention. Minor delays may occur during initiation due to internet upload speeds when transferring files.*

Cost Savings

SAMI's automation solution reduces the staffing pressure for cybersecurity — high salaries for a talent pool that is already limited. It replaces multiple tools, reduces the need for expensive consultant fees, and its user friendly interface results in lower license, maintenance, and training fees.

Consider the following a few estimated cost comparison of SAMI vs. human resources or consultants across a variety of cybersecurity vectors:

Process	Traditional Cost	SAMI Cost
M365 Security	$10,000 per assessment	$2-3 per inbox per month
CIS Windows Security	$5,782 for 100 assets per year	$2-3 per endpoint per month
Mobile App Security	$20,000 per year	$15-$20 per app per month
Dynamic Application Security Testing (DAST)	$59 per month	$5-7 per month
Identity Thread Detection and Response (ITDR)	$18,000 per assessment	$0.08-0.12 per ID per month

Total Risk Visibility. Tool Consolidation & Correlation

SAMI delivers wide-ranging risk assessment across devices, cloud platforms, M365, networks, third-party apps (mobile and desktop), vendors, firmware, and more. Turning siloed raw data into a cohesive risk picture you can act on. One platform. One dashboard. One source of truth.

From Risk to Impact: Managing Liability, Not Chasing Zero Risk

SAMI translates technical vulnerabilities into tangible business impact, helping you quantify the financial, legal, and operational consequences of cyber risk. You can finally answer, "What will this breach really cost us?".

This helps the boardroom conversation shift from an IT question to liability management - a business question.

Proactive Security

Instead of waiting for a breach to happen, SAMI identifies the paths attackers are most likely to exploit and addresses them before they're used — not just preventing incidents, but preventing the business liability those incidents cause.

Strategic Prioritization

SAMI's Strategic Priority Index (SPI) is SAMI's proprietary scoring system that scores each risk based on business liabilities — telling you not just what's wrong, but what's most urgent to fix based on liability and impact.

Knowledge-Centric Security

Most tools stop at information. SAMI delivers knowledge. By automating the conversion of raw signals into actionable, ranked business intelligence, SAMI ensures your team acts on what matters — not just what's noisy.

Audit Trail & Justification Layer

SAMI gives you the audit-ready evidence that your risk decisions were informed, rational, and timely — protecting you during audits, lawsuits, and insurance disputes. It's not just defense. It's defensibility.

Business Alignment

SAMI helps the IT and non-IT stakeholders within the business speak the same language, prioritizing risks based on their liabilities ie. the business impact by asset value, financial loss, operational loss (ransomware, data loss, brand value loss etc), compliance issues etc.

Enhanced Reporting

SAMI generates detailed reports in minutes, cutting time and costs for security and IT teams, while putting clear liability insights directly into the hands of business leaders.

Upstream and Downstream Integrations

SAMI seamlessly integrates with upstream systems (your existing security tools such as tenable to pull in risk data, enabling comprehensive business impact analysis and downstream systems such as IT Service Management Systems (Such as Jira, Service Now). Security system (SIEM etc), Analytic Systems etc. integrations are available on demand.

Use Cases for SAMI

- **Insurance Underwriting.** Organizations can use SAMI to document and demonstrate reductions in risk exposure for the purpose of reducing insurance expenses.
- **Compliance Prep.** SAMI's data record can be used to prove that you are proactively managing data vulnerability to comply with regulations.
- **MSPs/MSSPs.** Data security service providers can use SAMI to offer their clients a premium service — the competitive edge of CTEM including a wide range of coverage.
- **Mobile or Web App Security.** CTOs or developers can use SAMI to provide fast security and vulnerability of apps in development or on the market.
- **ROI on Cyber Investments.** With SAMI, you can easily quantify the return on your proactive cybersecurity efforts, translating technical work into clear business value and demonstrating the impact of your security investments.

Case Studies

Case Study #1: Big Impact from a Small Deployment – SAMI at a major public regional board serving multiple communities

Overview

In a limited deployment, SAMI was implemented for a major public regional board serving multiple communities with a budget exceeding $2 billion. Within 10 minutes, SAMI scan was setup for M365, Azure, Dynamic Application Security Testing, Vendor risk assessment, Third-party mobile apps, CIS benchmarks, Legacy desktop applications etc. Despite the limited scope, the system generated comprehensive assessments and reports in just a few hours, a task that would have required months of work plus of effort from a cross functional IT, compliance, analytical, business and finance teams.

High-Value Results in Minimal Time: Even with a small rollout, SAMI uncovered:

- 1,500+ risks and over $3.5 million in potential liabilities across 8 operational areas
- 200 + known threat actors/malwares actively targeting similar organizations were identified
- Third-party mobile app risks identified, leading for a path to informed discussions with the vendors
- Assisted auto remediation of CIS Benchmarking issues.
- C-Suite–ready reports outlining financial exposure, legal risk, and strategic impact

Outcome

This limited deployment demonstrated SAMI's ability to deliver enterprise-grade visibility, speed, and business relevance—with minimal time, cost, and effort.

Case Study #2: Automating CIS Benchmarking with SAMI

Challenge

A large enterprise needed to conduct CIS benchmarking and remediation, a process that traditionally required up to six months of manual effort across teams.

Solution

By deploying SAMI, the company fully automated its CIS benchmarking assessment and remediation.

Outcome

This rapid automation not only accelerated compliance but also led to significant cost savings. What once took months now takes a single afternoon, freeing up critical resources and delivering faster, more actionable insights.

Case Study #3: Supercharging an MSSP's Efficiency with SAMI

Overview

A Managed Security Service Provider (MSSP) serving 40+ customers integrated SAMI into its cybersecurity toolkit to enhance service delivery and scale operations.

Challenge

The MSSP's pentesting and M365 security assessments required significant manual effort:

- **3–4 days** of skilled labor per client for pentesting and reporting
- **4–6 weeks** for comprehensive M365 security reviews

Solution & Impact

With SAMI, those same services now take less than a minute of human interaction each. The result?

- Dramatic reduction in time and cost
- Freed-up expert resources for higher-value work
- Ability to serve more clients, faster—without increasing headcount

Outcome

SAMI transformed the MSSP's operations from labor-intensive to lightning-fast, enabling them to scale with confidence while delivering deeper insights at unmatched speed.

Case Study #4: Identifying Hidden Risks in Third-Party Software and Devices with SAMI

Overview

Organizations routinely purchase and deploy third-party software—such as CRMs, ERPs, Adobe products etc and install applications on their mobile devices, use firmwares and use external vendors. The security vetting for these applications is seldom conducted with the thoroughness it demands due to the extensive resources, time, and specialized expertise typically required. As a result, critical vulnerabilities and compliance gaps often go undetected until it's too late.

Challenge

Many procurement teams lack the tools or expertise to assess the true security posture of third-party software or applications before purchase. This creates hidden liabilities that can lead to data breaches, regulatory violations, or reputational damage. For instance, a best-selling security camera widely adopted across North America required its users to download accompanying Android and iOS applications for control and monitoring. Traditionally, thoroughly vetting such applications would take weeks or months of coordination across multiple IT and security teams with deep, specialized knowledge.

Solution & Impact

The camera's mobile apps was uploaded into SAMI for assessment, a process that took less than a minute. SAMI then automatically analyzed the applications and revealed:

- That the app had 100+ components – these are third-party pre-made code added to apps for extra features, often with hidden security risks.
- This app had 500+ identified risks which treats can use to compromise the app
- 5 cryptographic components were identified and these had 10 cryptographic risks, including deprecated or insecure algorithms.
- There were 68 outdated components ie these components are no longer receiving updates or security support. Which means the security risks go unremidated.
- The application was making 40+ API call connecting to 73 external IP locations. Communicating with infrastructure linked to 80 companies across 7 countries, including entities tied to military organizations in high-risk jurisdictions.

Armed with this insight, the organization was able to evaluate the risks holistically and make an informed decision about whether and where to deploy the cameras, something that would traditionally take months of analysis and coordination.

Outcome

What once required intensive, cross-functional efforts became a streamlined process handled in under a minute. This kind of due diligence is now scalable, allowing procurement teams to:

- Pre-emptively evaluate third-party apps, vendors etc before purchase
- Reduce hidden liabilities from shadow IT or vendor-supplied applications
- Make smarter procurement decisions backed by detailed, real-time risk intelligence

AUTNHIVE
ELEVATE SECURITY

SAMI is transforming how organizations assess third-party risk—bringing clarity, speed, and security to an often overlooked but critical part of enterprise operations.

As more and more companies wake up to the business risk of cybersecurity, CTEM will become more and more of the standard, and as always **early adopters will have the edge.**

SAMI offers a rare opportunity to quickly and economically become an early adopter of CTEM — continuous threat assessment and remediation, without the long waits or the labor costs, and none of the burden of long integration, complex training, or reliance on consultants.

With SAMI, you can:

- Discover every asset and vulnerability — internal and external.
- Prioritize the threats that matter to your business.
- Fix what you can, and manage what you can't.
- Auto-generate reports for compliance, legal, or insurance defense.
- Replace fragmented tool stacks and reduce your total cost of ownership.
- Collaboration /Integration with the Existing Ecosystem

For executives, MSPs, and MSSPs, now is the time to embrace tools like SAMI and transition to a 21st-century approach to digital risk management — one that reduces costs, identifies true liabilities, obtains more buy-in from stakeholders, and makes fast cybersecurity experts out of even the least tech-savvy human resources.

Reference

1 Cost of Cyber attack: https://www.ibm.com/reports/data-breach

2 Effects of Cyber attack: https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/