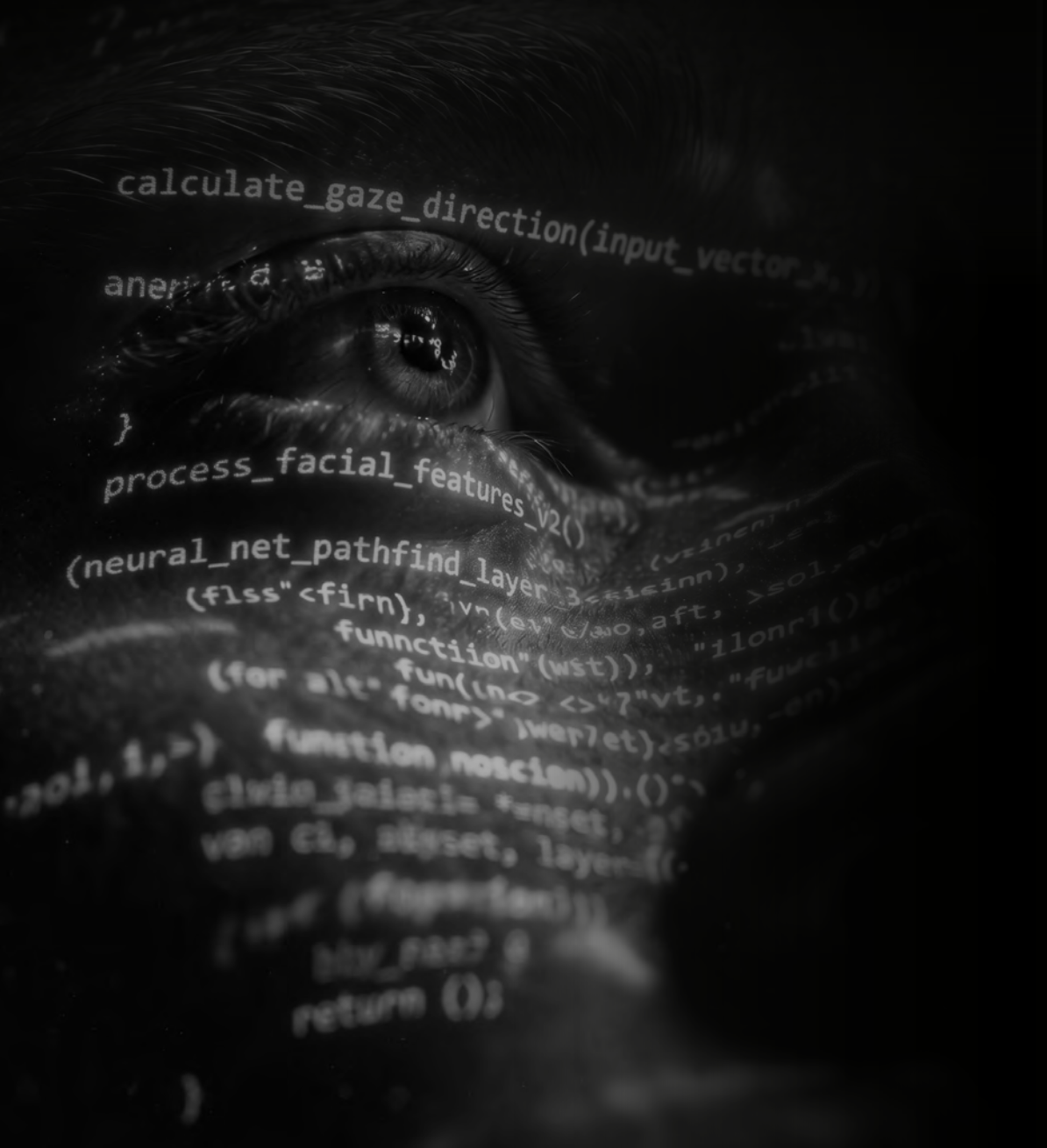
©2026

MANIFESTO ON THE ERA OF AUTONOMOUS ATTACKS



VULTUS

WE HAVE ENTERED A NEW ERA OF DIGITAL SECURITY



For several months, organizations have watched their attack surfaces grow exponentially without the appropriate sense of urgency or recognition of the stakes.

Using Artificial Intelligence to accelerate business growth is essential. Yet alongside that intended growth, as the digital surface expands, previously invisible risks accumulate exponentially, exposing operations to threats that often have not yet been identified, validated, or prioritized.

Attackers already understand: with Artificial Intelligence, exploiting vulnerabilities has become faster, cheaper, and more scalable.

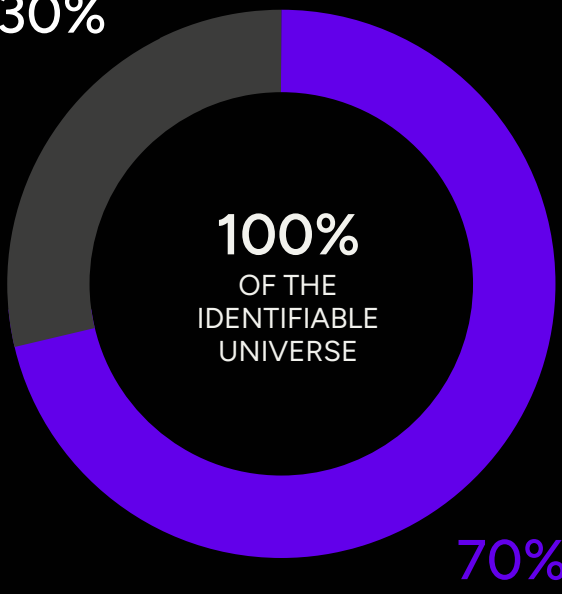
For many years, a significant share of companies' vulnerabilities and risks was discovered only when someone, usually with strong technical knowledge of digital environments, had the time, context, patience, and budget to look deeply.

THE NEW ERA OF AUTONOMOUS VULNERABILITY DISCOVERY

Of the total universe of identifiable vulnerabilities.

2026 EXPANDS AUTONOMOUS COVERAGE

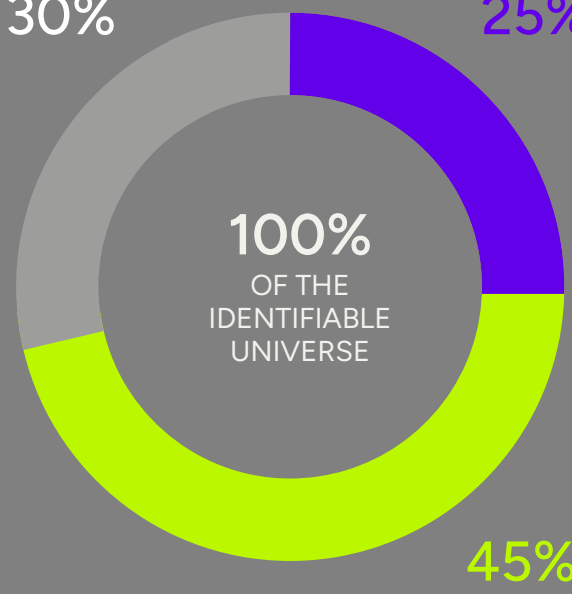
through 2025



- Autonomously identifiable SAST / DAST
- Required manual analysis

Automation covered only a fraction of the identifiable universe.

in 2026



- Autonomous via SAST / DAST
- Manual analysis
- Now autonomously identifiable with GenAI

GenAI dramatically narrows the gap between what can be identified and what can be identified autonomously.

In 2026, autonomous discovery moves beyond SAST/DAST and captures a much larger share of the universe of identifiable vulnerabilities. The space left for entirely manual analysis becomes significantly smaller.

Generative AI has made a growing share of offensive discovery autonomous. What once required exhaustive pentesting, unrestricted scope, and manual investigation is now beginning to emerge through systems that can read applications, compare responses, test hypotheses, persist through workflows, and assemble attack paths exactly as an advanced adversary would.

This changes how cyber defense strategies will be built from now on.

Companies' attack surfaces have not necessarily worsened overnight. But they have become more visible and exposed than at any point in history.

There is a short window to adapt, in which lasting digital resilience will be achieved only through strategies that adopt three fundamental principles:

• Continuous autonomous testing in place of one-time assessments and annual schedules. Prerequisites: strong technical capability to execute autonomous tests and robust processes to ensure broad test coverage and successful remediation.

• Continuous governance of AI adoption, particularly in software deployments and their direct impact on expanding the internet-facing surface.

• Hybrid adversarial simulation focused on discovering real attack paths rather than isolated vulnerability lists: "If the adversary is a human using generative AI, the simulation is equally hybrid." Prerequisite: adoption of regular Red Team Assessment schedules.

PRINCIPLES OF AUTONOMOUS TESTING

Our highest priority is to discover the attack paths already present in an organization's digital surface before an adversary does. We recognize that 2026 marks a generational shift: vulnerabilities that were once difficult, expensive, and time-consuming to find can now be revealed autonomously, repeatedly, and at scale.

Risk does not increase only when a new vulnerability is created. It also increases when an old vulnerability becomes easy to find. Security can no longer depend on the low probability that someone will look deeply. GenAI has reduced the cost of offensive attention.

Adversaries no longer need to become fixated on a target. Machines can explore surfaces without fatigue, boredom, or the economic constraints of traditional manual pentesting. Applications must be tested as living systems: with users, permissions, workflows, business rules, APIs, states, errors, integrations, and exceptions.

The focus should be on revealing paths rather than finding more tickets: from exposure to exploitation, from exploitation to impact, and from impact to remediation. Considering the new "cyber risk Pareto principle," the new testing dynamic should be #AIFirst + #InternetFacingFirst.

Traditional scanners remain useful, but they are not sufficient. At a more fundamental level of the autonomous discovery barrier lies the IoC or plugin barrier, where static patterns dynamically revealed by environments still uncover important vulnerabilities at minimal cost.

Pentesters and red teamers remain essential, but their role is changing. People should guide, validate impact, set boundaries, and turn findings into decisions. Machines should expand depth, scale, and persistence.

The question has become: "What will an adversary using autonomous agents find in my environment? How did we reach this point technologically, and how should we adapt our environments to this new reality?"

Boards, executives, and CISOs should be able to follow adaptation and ongoing oversight simply. What is the autonomous testing strategy? What is exposed? How could it be abused? What would the impact be? What needs fixing first? The false peace of what remained unseen is over. What was hidden by a lack of time, budget, or patience is likely to emerge.

Every organization must assume its surface will be examined. The only strategic choice is whether defense or the adversary examines it first.

The era when vulnerabilities survived unseen because they were costly to find is over. GenAI has lowered the price of offensive discovery.

Every surface will be attacked.

VULTUS

THE DIFFERENCE IS WHO GETS THERE FIRST: YOU OR THE CRIMINAL.

VULTUS

ELITE SECURITY WITH BUSINESS INSIGHT

ISG LEADER

Strategic Security Services
Technical Security Services
Risk-based Vulnerability Management