

11,000+ Cybersecurity Products. Why Do So Many Sound the Same?

A study of language convergence across the cybersecurity, GRC and trust landscape

Author: Chris Els

Founder & CEO: Resolut

Research paper | October 2026

85	64	11+
Test Sample	Converged Language	Different Solutions

Executive Summary

Cybersecurity investors and buyers face an unusual problem.

There is no shortage of categories. There may, however, be too little distinction in the language used to describe the products within and across them.

Leading analyst IT-Harvest tracks more than **11,000 cybersecurity products from more than 4,000 vendors across 18 categories**. Other market taxonomies divide cybersecurity into considerably more categories.

Against this wider market context, we reviewed the public positioning of **85 products and solutions** across GRC, risk, compliance, third-party risk, assurance, privacy, software security, cyber resilience, AI governance and adjacent markets.

64 of the 85 products reviewed used one or more of the same broad positioning concepts, including:

Trust | Continuous | Connected | Network | Governance | Compliance Automation | Third-Party | Assurance | Resilience | Operating System | Infrastructure

Yet these products span **at least 11 materially different types of solution**.

The finding is not that these products all compete. It is almost the opposite.

Products managing fundamentally different things are increasingly being described using similar language. For investors and buyers, this creates an important distinction:

Semantic similarity is not the same as competitive similarity.

As AI becomes an increasingly common tool for market research and competitor discovery, understanding that distinction may become more important.

1. The Question That Started the Research

This research began with a relatively simple challenge.

While reviewing the competitive landscape surrounding Resolut, an investor conducted their own research using AI alongside conventional internet searches.

Their results identified numerous established cybersecurity and GRC companies that were not included in our competitor analysis. It was a reasonable challenge so we repeated the exercise.

The investor's results were not wrong. The companies existed, their products were relevant to cybersecurity, risk, compliance or trust, and their public positioning often appeared surprisingly similar.

But closer examination revealed something else. Many of the products appearing alongside one another in searches were not solving the same problem.

- Some managed controls.
- Some managed evidence.
- Some assessed suppliers.
- Some observed external cyber exposure.
- Some protected software.
- Some governed data.
- Some provided recovery and resilience.
- Some governed AI.
- Others mapped relationships, dependencies or compliance status.

The search results were identifying similarity in **language** as well as similarity in **function**. That distinction became the subject of our initial research.

The first output was **The GRC & Trust Landscape: Different Solutions. Different Problems. Different Forms of Assurance.**

Rather than grouping products solely by the categories assigned to them, the landscape applied a more practical set of questions:

1. **What does the product manage?**
2. **What does it actually do?**
3. **What value does it deliver?**
4. **What does it establish or provide?**
5. **What should not be inferred from that?**

We published the resulting comparison table: you can download it [here](#)

But the research raised another question.

As the landscape expanded, products that were clearly different when examined functionally were frequently describing themselves using remarkably similar language. That observation led to the research presented in this paper.

2. A Very Large Market

The scale of cybersecurity makes this problem particularly important.

IT-Harvest reports a continuously maintained market dataset containing more than **4,000 cybersecurity vendors and 11,000 products across 18 categories**.

Other approaches produce very different taxonomies. CyberDB, for example, divides the market into around 150 categories.

Neither approach is necessarily wrong.

A broad taxonomy helps explain the major structure of a market. A granular taxonomy helps distinguish specialised technologies.

The difference does, however, illustrate an important point:

Categories are analytical constructs. Products are not. A product ultimately manages something, performs an activity and produces an outcome. Understanding these three things can sometimes tell an investor or buyer considerably more than the category name attached to it.

3. What We Reviewed

This research was not intended to catalogue the entire cybersecurity market. That work is better undertaken by specialist industry analysts with extensive market databases.

Instead, we established a defined review set of products relevant to the areas in which terminology appeared to be converging.

The review covered **85 products and solutions** across:

- enterprise GRC and integrated risk management;
- compliance automation;
- continuous controls monitoring;
- third-party and vendor risk management;
- supply-chain and nth-party risk;
- cybersecurity ratings and external risk intelligence;
- privacy and data governance;
- application security;
- software supply-chain security;
- cyber resilience and data protection; AI governance, AI security and emerging trust infrastructure.

Each product's public positioning was examined for substantive use of a defined group of terminology families. An incidental occurrence of a word was not sufficient.

A company saying that customers “trust” its service, for example, did not qualify as trust positioning.

Terms such as **Trust Management Platform**, **Continuous Trust**, **Trust Network** or **Trust Infrastructure** did.

The same principle was applied to the other terminology examined.

Of the 85 products reviewed, **64 met the language-convergence test**. We deliberately do not convert this into a market percentage.

The 85 products are not claimed to be a statistically representative sample of the 11,000+ cybersecurity products tracked by analysts.

The finding describes the products reviewed. It should not be extrapolated to the entire cybersecurity market.

4. Different Products. Increasingly Similar Language.

The terminology fell into several recurring families.

Trust

Trust Platform
Trust Management
Trust Infrastructure
Trust Network
Trust Center
Continuous Trust
Trusted Evidence

Continuous

Continuous Compliance
Continuous Controls Monitoring
Continuous Assurance
Continuous Governance
Continuous TPRM
Continuous Evidence
Continuous Visibility
Continuous Trust

Connected and Network

Connected GRC
Connected Risk
Connected Compliance
Connected Governance
Connected Ecosystem
Trust Network
Supplier Network

Vendor Network
Risk Network

Governance and Compliance

Governance Platform
Continuous Governance
Compliance Automation
Automated Compliance
Real-Time Compliance
Continuous Compliance

OS and Infrastructure

Compliance OS
Governance Operating System
AI Governance Operating System
Trust Infrastructure
AI Trust Infrastructure
Governance Infrastructure

Third-Party, Assurance and Resilience

Third-Party Risk
Vendor Risk
Supply-Chain Risk
Continuous Assurance
Security Assurance
Operational Resilience
Cyber Resilience

The individual expressions vary.

The underlying vocabulary is remarkably consistent.

5. “Continuous” Does Not Mean One Thing

The word **continuous** provides perhaps the clearest example.

- A compliance automation platform may use continuous to describe the collection and monitoring of evidence against controls.
- A GRC platform may use it to describe continuous controls monitoring.
- A TPRM platform may continuously observe changes in supplier risk.
- A cyber-rating platform may continuously observe an organisation's external security posture.
- An AI governance platform may continuously monitor models or agents against policies.
- A security-assurance platform may continuously test whether controls remain effective.

All are legitimately continuous. But they are not continuously doing the same thing.

The distinction matters because a search for **continuous compliance**, **continuous assurance** or **continuous trust** can place several of these products into the same consideration set.

The common adjective can obscure the different object being monitored.

6. The Expansion of “Trust”

Trust presents a similar problem.

The word now appears across compliance automation, customer assurance, third-party risk, supplier networks, identity, AI governance, AI security and emerging infrastructure platforms.

Some vendors use **Trust Management**.

Others use **Trust Network**.

Several emerging companies now use **Trust Infrastructure**.

In AI alone, the market contains propositions described as AI Trust Platforms, AI Trust Infrastructure and trust infrastructure for autonomous agents.

These products can be fundamentally different.

One may manage regulatory controls. Another may govern model behaviour. Another may establish agent identity and delegation. Another may manage evidence exchanged between organisations. Another may continuously assess third-party risk.

The terminology tells us something about the intended outcome.

It does not necessarily tell us what the technology actually manages.

7. Even “Operating System” Is Converging

The same phenomenon is appearing around the idea of an operating system.

Our research identified products positioned as:

- **Compliance Operating Systems**
- **Governance Operating Systems**
- **AI Governance Operating Systems**

and broader governance or trust infrastructure.

The metaphor is understandable. An operating system suggests an underlying layer that coordinates activities rather than another isolated application. However, investors and buyers should be cautious about treating the term itself as a category.

Two companies can both describe themselves as an operating system while coordinating entirely different objects, workflows and relationships.

The description may explain architectural ambition. It does not establish competitive equivalence.

8. At Least 11 Different Solution Types

The 64 products demonstrating terminology convergence span at least 11 materially different functional groups.

Solution type	Primarily manages
Enterprise GRC / IRM	Risks, controls, policies and obligations
Compliance automation	Frameworks, controls and evidence
Continuous controls monitoring	Control status and effectiveness
TPRM / VRM	Vendors and third parties
Supply-chain / nth-party risk	Dependencies and extended relationships
Cyber ratings / intelligence	Observable external cyber posture
Privacy / data governance	Data, privacy obligations and processing
Application security	Code, applications and vulnerabilities
Software supply-chain security	Components, dependencies and SBOMs
Cyber resilience / data protection	Recovery, continuity and protected data
AI governance / security / trust	Models, agents, AI systems and their governance

There is significant overlap between some of these groups. That is expected.

The important finding is that they cannot reasonably be treated as one competitive market simply because they use similar terminology.

9. Three Different Forms of Competition

The research suggests that competitor analysis increasingly needs to distinguish between three things.

Functional Competition

Two products are functional competitors when a buyer could reasonably substitute one for the other to solve substantially the same problem.

They manage similar objects, address similar requirements and produce comparable outcomes. This is competition in the conventional sense.

Adjacent Competition

Products may overlap in buyers, workflows, budgets or capabilities without being direct substitutes.

A GRC platform and a specialist TPRM platform may both participate in the management of supplier risk, for example, while solving materially different portions of the problem.

These products can still compete commercially.

But the competition is partial.

Semantic Competition

The third form is increasingly important.

Products may appear competitive because they describe themselves using similar concepts.

They compete for search results, investor attention, analyst interpretation and potentially buyer discovery.

Yet they may manage fundamentally different things.

Semantic competitors compete for attention before they compete for customers.

This distinction becomes particularly important when market discovery is mediated by AI.

10. AI May Amplify the Problem

AI is exceptionally good at identifying conceptual similarity.

Ask an AI system for competitors to a company described as providing:

continuous trust infrastructure for connected compliance

and it is reasonable for the system to retrieve companies associated with trust management, continuous compliance, connected GRC, third-party networks, assurance platforms and trust infrastructure.

From a semantic perspective, those results may be excellent.

From an investment or procurement perspective, they may be misleading.

The important questions come afterwards.

1. **What does the product actually manage?**
2. **What problem is the buyer paying it to solve?**
3. **What does the product establish, prove, observe or protect?**
4. **Could the buyer genuinely substitute one product for the other?**

Those questions turn semantic similarity into competitive analysis.

11. Why Categories Alone Do Not Solve the Problem

Industry analysts provide considerably deeper analysis within defined markets.

That remains essential.

Gartner, Forrester, IDC, Verdantix and others divide the wider technology universe into markets that can be analysed in much greater depth.

But even analyst taxonomies evolve as technology changes.

A product may also participate in several adjacent markets simultaneously.

This is particularly visible across GRC, TPRM, cyber risk, AI governance and compliance automation.

The result is not that categories have become useless.

It is that **category should not be the end of the analysis.**

A simple additional question can reveal considerably more:

What does the product actually manage?

- Controls?
- Evidence?
- Data?
- Software?
- Vendors?
- Cyber exposure?
- AI systems?
- Relationships?
- Dependencies?
- Compliance status?

The answer often explains why two products that sound remarkably similar are not actually substitutes.

12. What This Means for Investors

The cybersecurity market already presents investors with an extraordinary discovery problem.

- Thousands of vendors compete across thousands of products and numerous overlapping categories.
- Language convergence adds another layer.

An investor examining a new company should therefore distinguish between the company's:

- **market category**
- **functional competitors**
- **adjacent competitors**
- **semantic competitors**

A long AI-generated competitor list should not automatically be interpreted as evidence of a crowded functional market.

Equally, a founder claiming to have no competitors should be treated cautiously.

The more useful question is:

Which products could genuinely replace this one for the customer, which could absorb part of its value proposition, and which merely sound similar?

That distinction can materially change how a market opportunity is understood.

13. A Different Way to Read a Technology Market

Our research began as a competitor-analysis exercise. It ended with a different conclusion.

The cybersecurity market does not appear to suffer from a shortage of categories. It increasingly suffers from a problem of **language convergence across categories**.

Our review found:

- **85 relevant products reviewed**
- **64 using one or more convergent positioning concepts**
- **At least 11 materially different functional solution types represented**

The research does not suggest that vendors are deliberately creating confusion. Much of the terminology is perfectly reasonable. Modern security and compliance genuinely are becoming more continuous.

- Systems genuinely are becoming more connected.
- Trust genuinely is becoming an important architectural and commercial objective.
- Third-party relationships genuinely are becoming more important.

The problem is what happens when those developments cause very different technologies to be described using increasingly similar words.

For investors, buyers and analysts, the response should not be to invent still more terminology.

It should be to look beneath it.

14. Related Research: The GRC & Trust Landscape

This paper builds on our earlier research, **The GRC & Trust Landscape: Different Solutions. Different Problems. Different Forms of Assurance.**

The accompanying downloadable comparison table examines individual solutions through a common lens:

- **What does it manage?**
- **What does it actually do?**
- **What value does it deliver?**
- **What does it establish or provide?**
- **What does it not provide?**

The purpose is not to rank vendors.

It is to make it easier to distinguish between products that may appear similar through category labels, search results or positioning, but deliver materially different forms of value and assurance.

Read the original research and download The GRC & Trust Landscape comparison table →

The landscape will continue to evolve as products, categories and market terminology change.

So will the research.

Conclusion

The next time two cybersecurity companies appear to compete, three questions may provide a better answer than their category or positioning:

What does each product actually manage?

What does it establish or produce?

Could a customer genuinely substitute one for the other?

If the answers are different, the products may share language without sharing a market.

Semantic similarity is not competitive similarity.

As AI increasingly shapes how investors, buyers and markets discover technology, understanding that difference may become increasingly important.

Research Methodology

This research was conducted using publicly available product and vendor information available in October 2026.

A defined review set of **85 products and solutions** was examined across enterprise GRC, risk, compliance automation, continuous controls monitoring, third-party and supply-chain risk, cyber-risk intelligence, privacy and data governance, application and software-supply-chain security, cyber resilience, AI governance/security and adjacent trust technologies.

Products were assessed for substantive use of defined positioning concepts including trust, continuous, connected, network, governance, compliance automation, third-party, assurance, resilience, operating system and infrastructure.

Incidental occurrences of individual words were excluded.

64 of the 85 products reviewed met the language-convergence criteria.

The review set is not presented as a statistically representative sample of the global cybersecurity market. Findings describe the products reviewed and should not be extrapolated to all cybersecurity products.

Product positioning and market terminology change over time. This research therefore represents a point-in-time view.

References & Further Reading

IT-Harvest

Cybersecurity industry market intelligence and vendor/product database. Market-scale figures referenced in this paper are based on IT-Harvest's publicly reported data.

Forrester Research

The Governance, Risk, And Compliance Platforms Landscape, Q4 2025.

Forrester Research

Research concerning the evolution of GRC platforms, continuous controls monitoring and cybersecurity risk-rating platforms.

Gartner

Buyer's Guide for Cybersecurity Continuous Compliance Automation, 2026.

Verdantix

Green Quadrant: Governance, Risk and Compliance Platforms 2025.

CyberDB

Cybersecurity vendor, product and category database.

Publicly available vendor product pages and positioning materials were reviewed as primary sources for the terminology analysis.

About the Research

This paper forms part of Resolut's continuing research into how trust, compliance, risk and assurance are changing as organisations, technology and supply chains become increasingly connected.

Our research examines topics relevant both to Resolut and to the wider GRC and cybersecurity market. Where useful, supporting research, comparison tables and related material are published through the Resolut Resource Centre so that buyers, investors, practitioners and other interested parties can examine the findings for themselves.

The objective is not to rank vendors or promote one approach as universally superior.

It is to make complex and increasingly overlapping markets easier to understand.

As the market evolves, we expect the research to evolve with it.