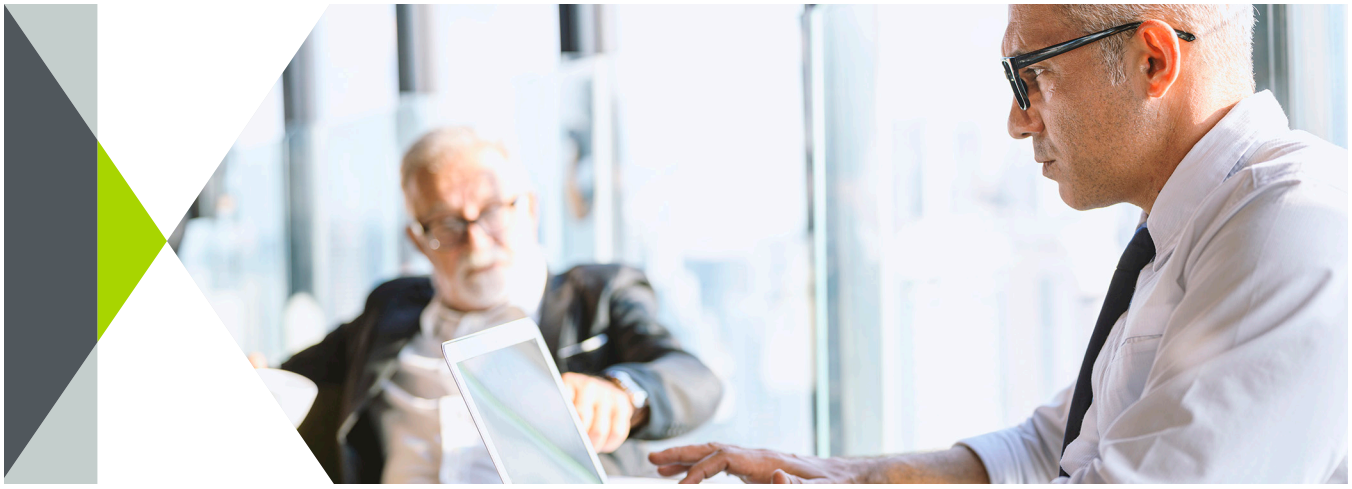


EXECUTIVE INSIGHTS

Threat Intelligence: As Threats Escalate, the Market Evolves

Threats to organizations — across many dimensions, including cyber, physical and corporate brand — are on the rise and increasing in frequency, intensity and sophistication. At the same time, the need for actionable intelligence within organizations has never been greater. Those two factors, taken together, are driving the growth and rapid evolution of the threat intelligence market.

In this *Executive Insights*, we will frame the landscape and the ecosystem, discuss major trends, and identify risks and opportunities for both industry participants and investors.

Threat intelligence fundamentals

To understand the dynamics of the rapidly evolving threat intelligence marketplace, it is important to start with a definition.

In the most fundamental terms, threat intelligence involves the production, aggregation and enrichment of data to deliver threat insights and to mitigate and remediate these risks.

The responsibility for delivering threat insights, mitigation and remediation falls to a wide array of players that comprise the threat intelligence ecosystem. Within that ecosystem, vendors focus on basic data production; data aggregation and enrichment; and detailed analysis of threat insights, mitigation and remediation. At every level, this work is backed by varying degrees of technology and human analysis.

The ecosystem is dynamic. Marketplace participants are moving rapidly to take advantage of emerging opportunities, including in entirely new threat intelligence use cases and areas of focus.

Several trends are driving the growth and evolution of the threat intelligence space:

- **Cyberattacks, social media attacks and physical threats are becoming more frequent and more severe.** The frequency and intensity of attacks from both state and nonstate actors has been on the rise for years.
- **Information security budgets are growing.** Organizations understand the risks and are scaling up IT security programs accordingly.
- **Cybersecurity skills are in short supply.** A persistent shortage of talent is causing organizations to increase their reliance on outside partners and consultants.
- **The COVID-19 pandemic has driven an increase in remote work.** This trend shows every sign of persisting.
- **There is a growing awareness that the response to threats and risks cannot be siloed in the cybersecurity team.** Organizations are moving to unite, or at least connect, their security operations centers (SOCs), network operations centers (NOCs) and outside vendors. Both regulatory drivers and the rapid adoption of industry standards point toward an imminent future in which threat intelligence is the responsibility of a closely linked complex of entities and in-house functions tasked with protecting and supporting the full organization.

We anticipate that consolidation will be one of the key features of the landscape as the market matures and the value chain evolves.

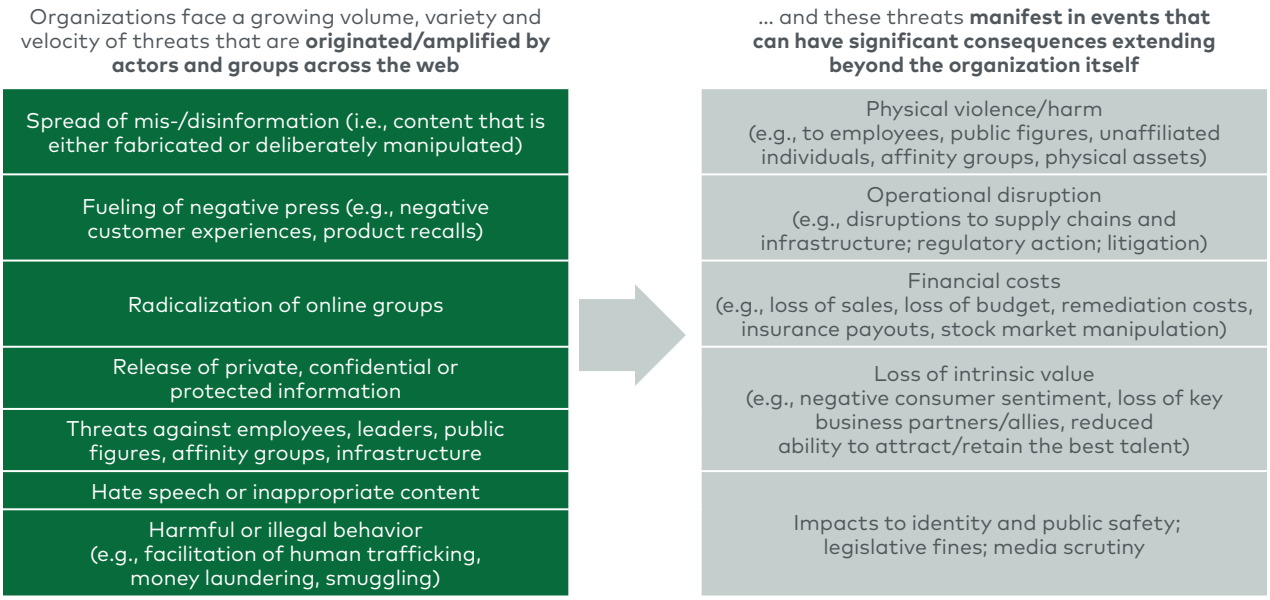
The threat intelligence ecosystem today

We have spoken about the increasing frequency and severity of threats that, at the most extreme level, can put an organization's finances, reputation or even viability at risk (see Figure 1).

How is the universe of in-house threat intelligence personnel and vendors responding to organizations' perceptions of escalating and intensifying levels of threat? Today the threat intelligence ecosystem is highly fragmented. One useful way for organizational customers to make sense of it — and to think about the array of vendors and their capabilities — is to locate them within one or more of the three main pillars of the threat intelligence value chain: data production, data aggregation/enrichment, and threat insights, mitigation and remediation (see Figure 2).

Within this value chain, an evolving market has resulted in the emergence of multiple competing (and, at times, cooperating) entities. Both small and enterprise vendors have entered the market to address threat intelligence needs from different angles. Organizations can choose

Figure 1
Threats identified through digital chatter and their potential impact



Source: L.E.K. research and analysis

from a mix of vendors and capabilities, including data production vendors, traditional and next-generation threat intelligence platforms (TIPs), threat intelligence insight platforms, cybersecurity detection and response tools, and managed security service providers (MSSPs).

Fragmentation is particularly high in some segments, making it challenging for the corporate security team to identify and select the right combination of providers (see Figure 3).

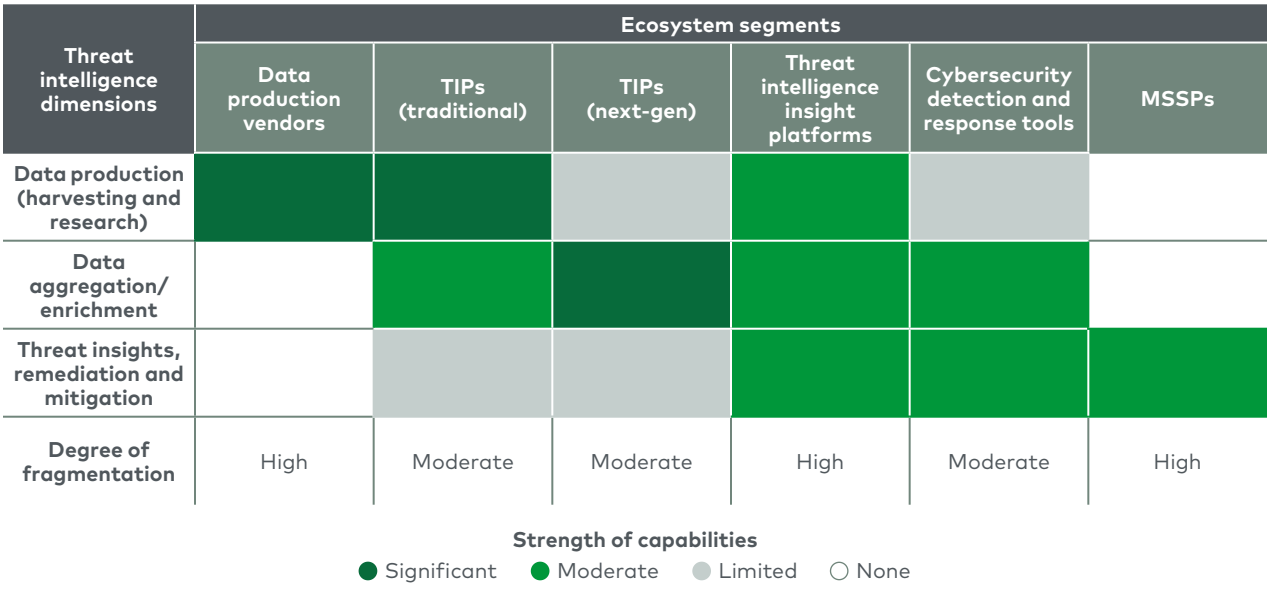
Figure 2
The threat intelligence value chain

	Threat intelligence value chain		
	Data production (harvesting and research)	**Data aggregation/enrichment**	**Threat insights, mitigation and remediation**
Overview	Data from both structured (e.g., network and endpoint telemetry) and unstructured sources (e.g., open source — clear web and social data)	Aggregation, cleansing, mapping and enrichment of structured and unstructured data; often includes adding visualization/search capabilities	Identification of threat insights and mitigation/remediation strategies per customer needs
Key differentiators	Breadth of data Access to deep/dark web (e.g., creation of pseudo-profiles to access private forums)	Data visualization Data normalization/relevance Ease and speed of search Integration of data sources Ability to combine unstructured and structured data Reduced false positives	Context on risks Customization on risks to ensure maximum relevance for end customer Ability to prevent risks from manifesting Remediation/mitigation of active risks/threats

Source: L.E.K. research and interviews

Figure 3
Primary segments of threat intelligence vendors/service providers

NOT EXHAUSTIVE



Note: TIP=threat intelligence platform, MSSP=managed security service provider
Source: Gartner; L.E.K. research and interviews

These vendors address a variety of use cases and offer a wide range of different methodologies. Vendors have focused on carving out niches in specific use cases and approached the discipline of threat intelligence from multiple angles. Customers, meanwhile, are still learning which tools are the most appropriate for their needs. They have historically shopped around and tried multiple vendors but are now beginning to settle on solutions as the market matures.

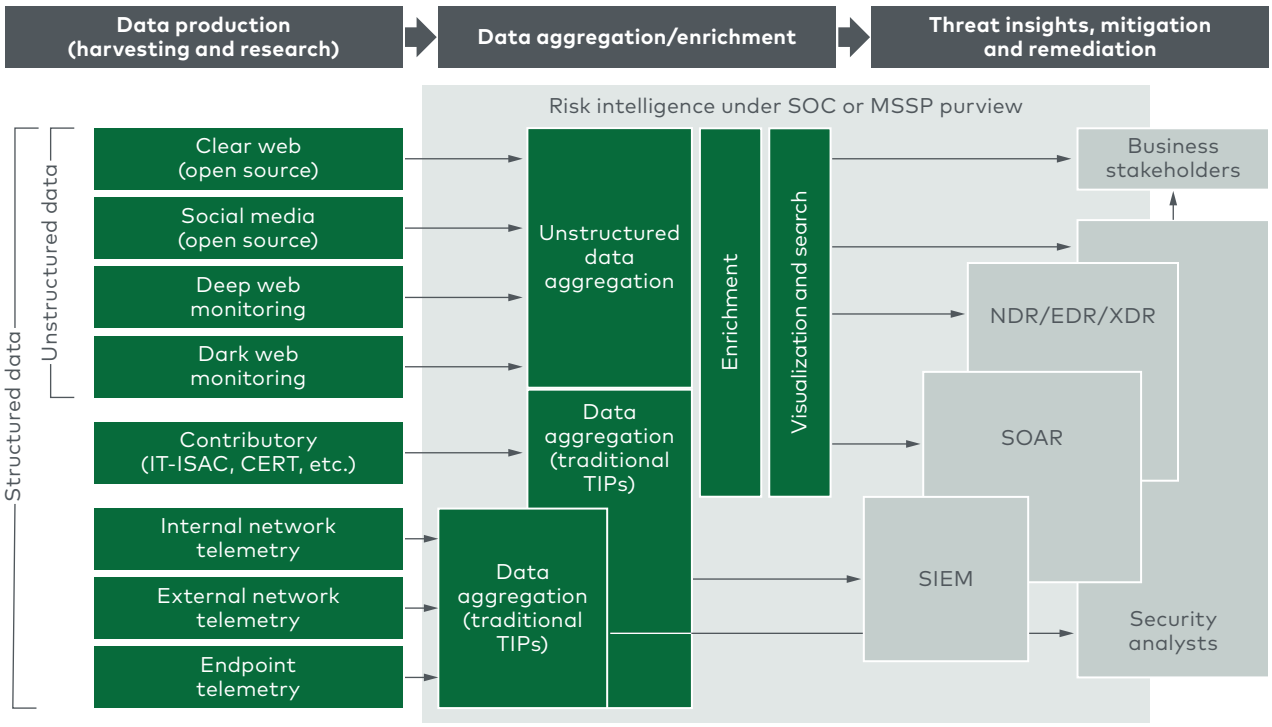
Within each value chain pillar, machine and human intelligence solutions interact to inform risk identification (see Figure 4). As a rule, the greater the amount of value-added interpretation and analysis, the greater the role for human intelligence. But this may change in the future.

Customers are evolving their expectations and capabilities

We have touched on the increasing risk to organizations, and their increasing awareness of threats both cyber and physical. Let's examine in more detail the operating environment and organizations' response.

The escalation of cyberattacks in terms of both severity and frequency has been dramatic. An L.E.K. Consulting banking industry client reports undergoing up to 1,000 attacks per day. There are multiple reasons for the upsurge. Geopolitics is a significant factor; Russia's invasion of Ukraine and the resulting war, for example, only adds to organizations' sense of vulnerability, but there are others. Threat and risk emerge in a complex interplay between the

Figure 4
Machine and human intelligence interactions that inform risk identification and stratification
ILLUSTRATIVE



Note: ISAC=Information Sharing and Analysis Center; CERT=computer emergency response team; NDR=network detection and response; EDR=endpoint detection and response; XDR=extended detection and response; SOAR=security orchestration, automation and response; SIEM=security information event management
Source: L.E.K. research and interviews

capabilities of the attacker and the organization. Case in point: The frequency of cyberattacks increased by approximately 40% during the COVID-19 pandemic. Remote work has created a significantly less secure network environment. Home networks are an inviting target, and bad actors are taking full advantage. At the same time, increased remote work has reduced the SOC's visibility into the organization and compromised its ability to intervene. Increased investment in threat intelligence solutions is the probable response.

The near-term shortage of cybersecurity talent has made it difficult for firms to find and retain in-house resources. This primarily impacts small businesses and the midmarket. The shortage continues to drive adoption of vendor-provided solutions, with increasing demand for both insights and remediation.

The development of regulatory and industry standards is also driving change. For example, adoption of industry-standard assessments like the MITRE Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) framework are expected to continue driving investment in threat intelligence solutions globally. In Europe, the increased focus on consumer

data protection and privacy under the General Data Protection Regulation is expected to continue supporting growth in the threat intelligence market.

How are organizations responding?

They are increasing their information security budgets. According to Gartner, chief information officers (CIOs) expect IT budgets to grow 3.6% in 2022, the fastest growth in over a decade, with 66% planning to increase the amount they spend on cyber/information security.[1]

They are becoming more holistic by evolving their expectations and their organizational approach. Risk/threat detection cannot be limited to the cybersecurity team as risks/threats affect the entire organization.

They are demanding more integrated data and higher-level analysis. Most customers have a fragmented approach to gathering and executing on threat intelligence, with purchase decisions made in silos across stakeholders (see Figure 5). While the pace of change is gradual, the savviest organizations are looking to move to more integrated operations — sharing data and analysis among the SOC, NOC and other parties.

Figure 5
Approaches to investing in threat intelligence

Note: CISO=chief information security officer
Source: L.E.K. research and interviews

Vendors are evolving their offerings to provide not just data, but also insights

As customers begin to settle on solutions, vendors are evolving their offerings. While there are many vendors aggregating data today, this is likely to become an increasingly commoditized activity. The end customer is interested in insights — placing risks within the appropriate

business context, preempting threats before they mature into crises and identifying actionable steps to mitigate risks.

Vendors are coming to realize that lasting sources of differentiation will only be in these two pillars — enrichment and enhancement of data, and the delivery of threat insights. More specifically, we expect that:

- **Data production vendors will increasingly become commoditized and undifferentiated.** Data production capability will increasingly be embedded in other tools.
- **Traditional TIPs will increasingly dwindle as a category.** Basic TIP functionality will be built into cybersecurity detection and response tools. Existing TIP vendors are already moving into these ecosystem segments.
- **Next-generation TIPs have an opportunity to remain relevant.** Providing truly differentiated data enhancement tools, which are difficult for other tool segments to replicate, next-generation TIPs are likely to be embedded into other tools versus being purchased by end customers.
- **Threat intelligence insight platforms are likely to remain relevant.** These platforms will likely maintain their position, especially as investment grows in the midmarket.
- **Cybersecurity detection and response tools are expected to see significant growth.** These tools will become increasingly effective at providing automated risk remediation and mitigation.
- **MSSPs will likely benefit from increased growth in the midmarket.** Similar to threat intelligence insight platforms, these providers will benefit from increased investment by this market segment.

We expect vendors to expand in two dimensions. The first is greater emphasis on value-added analysis and insights — helping customers make sense of data. This includes an expanded role for artificial intelligence (AI) and machine learning, higher in the value chain, in identifying and analyzing threats, mitigating risks, and proactively stopping them.

The second dimension is expansion into new use cases — the application of threat analysis tools to respond to a wider array of threats. The same threat analysis tools currently used in cybersecurity can be applied to address other threats to the organization — including physical, brand, strategic, corporate and political risks.

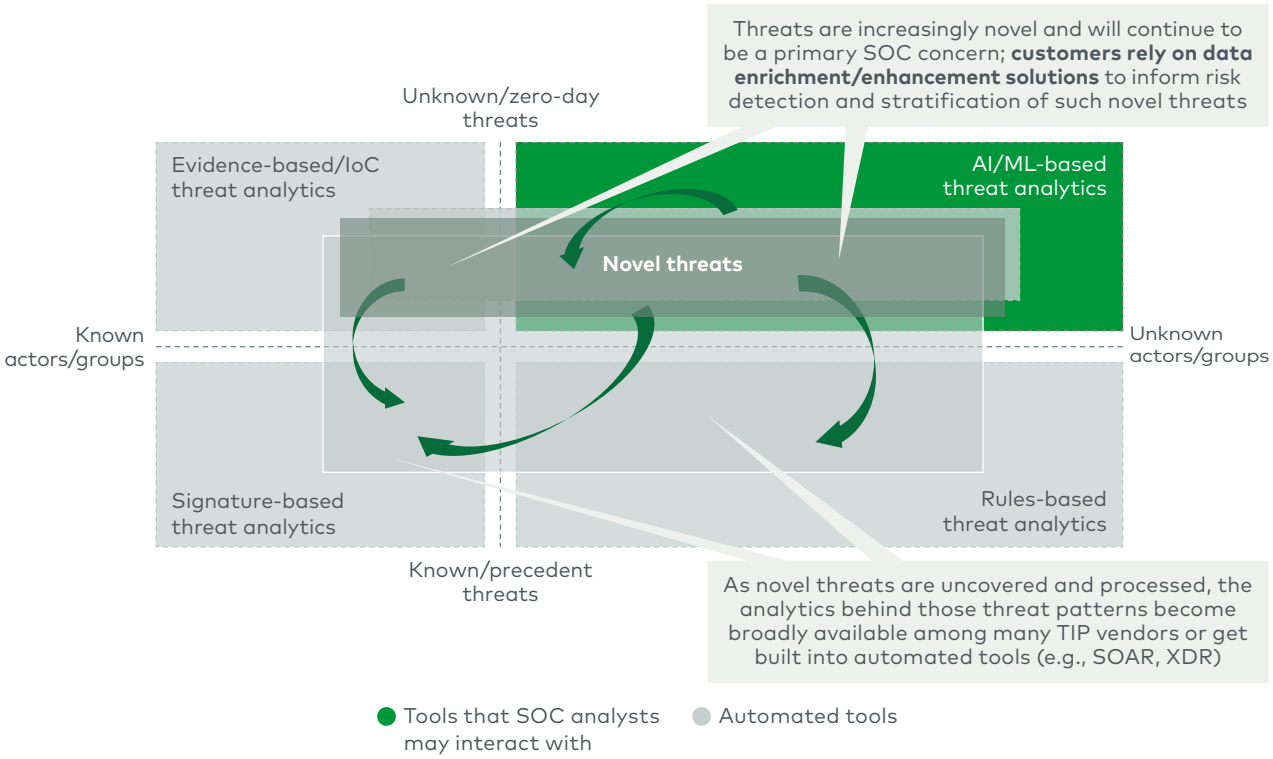
The shape of the future threat intelligence value chain

The trends we have described will change the shape of the threat intelligence landscape and its value chain. We expect an evolved threat intelligence value chain to feature:

- **A more holistic and less siloed approach to purchasing threat intelligence solutions.**
- **More analytic solutions that add more value** and target customers higher in the organization.
- **Vendors focusing on data enrichment and insights.**
- **The expanded use of AI.** AI will be used higher in the value chain, in data enhancement and enrichment, to detect and stratify unknown threats. The AI tools that enrich and enhance data will remain relevant in the detection and stratification of novel threats, such as zero-day threats by unknown actors or groups.

We also anticipate the increased application of AI to known threats. As vendors build automated workflows around those risks, increasingly, over time, the other quadrants will scale (see Figure 6).

Figure 6
Tools that enrich/enhance data for the detection and stratification of novel threats



Note: SOC=security operations center, IoC=indicators of compromise, AI=artificial intelligence, ML=machine learning
Source: Jefferies; L.E.K. research and analysis

We anticipate that a progressively greater number of vendors will expand beyond cybersecurity to address a wider range of threats and risks. Recognizing that the value chain is not limited to cybersecurity use cases, vendors will identify and migrate into adjacent use cases including monitoring and responding to threats to the corporation and the brand (see Figure 7). Other domains, including the political, can and will benefit from threat intelligence capabilities.

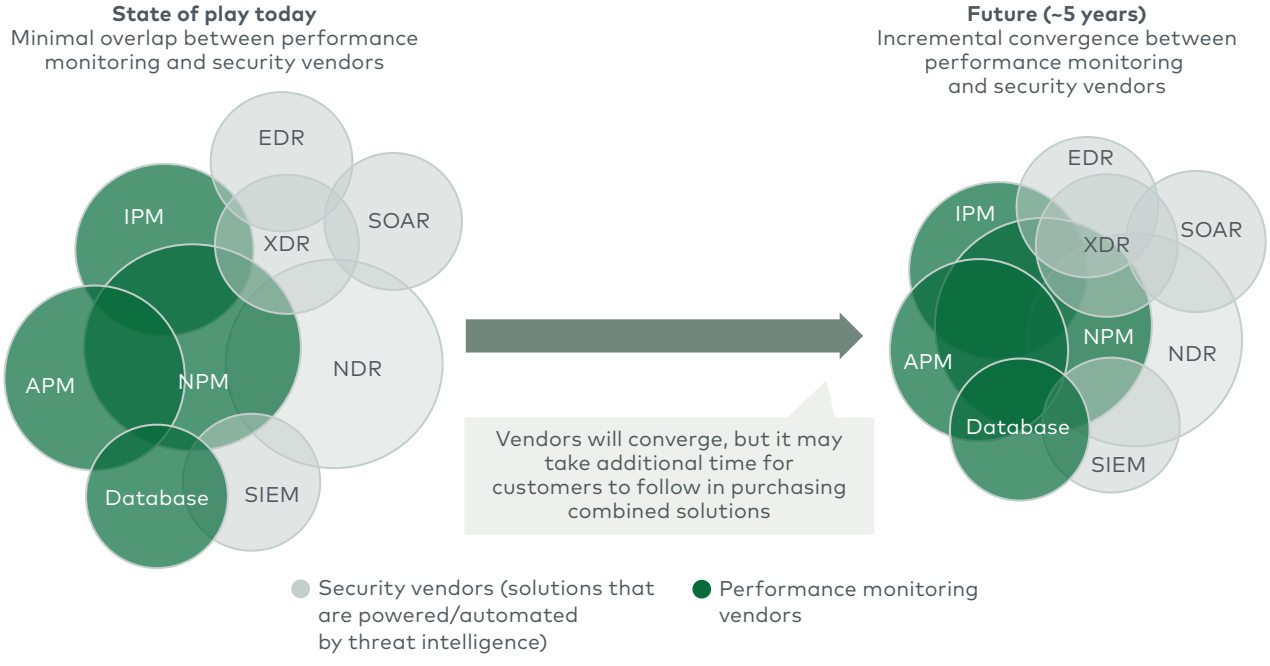
Figure 7
Potential use cases for threat intelligence

- Cyber use cases drive the majority of spend today on threat intelligence solutions
- Security operations (e.g., vulnerability intelligence, malware intelligence) account for the highest spend among cyber use cases
- Physical security and political risk drive noncyber spend in the public sector

Source: Gartner; L.E.K. research and interviews

In addition, vendors will evolve to straddle both observability/performance monitoring and threat intelligence. Performance monitoring and security solutions have historically been disparate products offered by distinct vendors with limited overlap in functionality, stakeholders and users. But recently, vendors have started to develop additional solutions to build out their product suites. This in turn is driving an incremental convergence between performance monitoring and security vendors. This trend will continue to emerge over the next five years (see Figure 8).

Figure 8
Vendor segments that will straddle observability/performance monitoring and threat intelligence



Performance monitoring and security solutions have historically been disparate products offered by distinct vendors with limited overlap in functionality, stakeholders, users, etc. ...

... but **recently vendors have started to develop additional solutions** to build out their suite of performance monitoring/security solutions, which is driving incremental convergence of platforms

As **vendors converge and drive the trend, customers will eventually follow**; a subset of **market-leading companies demanding a complete suite of best-in-class functionality will be early adopters** and will assist in educating the rest of the market

Note: IPM=infrastructure performance management; APM=application performance management
Source: L.E.K. research and analysis

Risks and opportunities for industry participants and investors

As the marketplace evolves, there will be emergent opportunities — and offsetting risks — for both industry players and investors. Development is likely to be uneven. Industry leaders and investors alike will need to be alert to the specifics of value chain evolution and horizontal migration and pay close attention to the pace of change.

For the industry, the vendors that win out in the long run will be those that are best able to avoid commoditization by developing more value-added offerings. For those in the data aggregation space, success means moving downstream to integration and analysis. For those already able to add more value through integration and analysis, it will be critical to strike the most effective balance between AI and human assets. Success in horizontal migration into new use cases will likely require the addition of talent with domain-specific expertise and the ability to integrate this talent effectively with existing assets and capabilities.

For investors, it will be critical to track the emergence of these trends and be alert to the pace of adoption of newer value-added capabilities and expanded use-case applications. Investors will also want to scrutinize management and identify leadership teams best able to manage the complex challenge of adding capabilities and expanding offerings.

Conclusion

Threats are not going away. We live in a world of increasing complexity, fragility and stress. That spells opportunity for vendors and investors able to respond to — and drive — value chain transformation. The threat intelligence leaders of the future will be those vendors that can take a holistic view and develop holistic offerings. One thing is certain: The array of organizational threats will be more intense in five years than it is today. And an evolved value chain will guide the response.

For more information, please contact strategy@lek.com.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Endnote

[1]Gartner, "IT Budgets Are Growing. Here's Where the Money's Going." Kasey Panetta, Oct. 21, 2021. https://www.gartner.com/en/articles/it-budgets-are-growing-here-s-where-the-money-s-going

About the Authors

Harsha Madannavar
Harsha Madannavar is a Managing Director and head of L.E.K. Consulting's San Francisco office. Harsha also leads L.E.K.'s Technology Infrastructure practice, advising U.S. and global corporates, private equity, and hedge funds on a range of shareholder value issues, including growth strategy, business model transformation, technology disruptions, product development, pricing and M&A.

Dominic Perrett
Dominic Perrett is a Managing Director in L.E.K. Consulting's San Francisco office, and a leader in the firm's Technology practice. Dominic has advised corporate and private equity clients on long-term growth strategies, new product expansion opportunities, pricing, customer segmentation and M&A transactions. His areas of expertise include technology infrastructure, IT services, data management, cloud networks and security.

Jordan Barron
Jordan Barron is a Managing Director in L.E.K. Consulting's Technology, Media and Telecom practice, based in the Los Angeles office. Jordan advises corporate and private equity clients across a range of critical strategic issues related to growth strategy, pricing and packaging, SaaS migration, customer segmentation, go-to-market approaches, and M&A support.

About L.E.K. Consulting
We're L.E.K. Consulting, a global strategy consultancy working with business leaders to seize competitive advantage and amplify growth. Our insights are catalysts that reshape the trajectory of our clients' businesses, uncovering opportunities and empowering them to master their moments of truth. Since 1983, our worldwide practice — spanning the Americas, Asia-Pacific and Europe — has guided leaders across all industries from global corporations to emerging entrepreneurial businesses and private equity investors. Looking for more? Visit **www.lek.com**.

L.E.K. Consulting is a registered trademark of L.E.K. Consulting LLC. All other products and brands mentioned in this document are properties of their respective owners. © 2022 L.E.K. Consulting LLC