

# Cybersecurity – Solutions and Services

## Extended Detection and Response (XDR)

A research report comparing provider strengths,  
challenges and competitive differentiators

Customized report courtesy of:

**kaspersky**

Executive Summary	03	<b>Extended Detection and Response (XDR)</b>	18 – 23
Provider Positioning	07	Who Should Read This Section	19
Introduction		Quadrant	20
Definition	15	Definition & Eligibility Criteria	21
Scope of Report	16	Observations	22
Provider Classifications	17	Provider Profile	23
Appendix			
Methodology & Team	25		
Author & Editor Biographies	26		
About Our Company & Research	28		

Report Author: David de Paulo Pereira

### In Brazil, cybersecurity services and products have become increasingly indispensable

Brazil has the second highest number of cyberattacks in Latin America, second only to Mexico. In other words, it continues to be one of the most attacked countries in the world. In fact, cyberattacks are causing financial, operational and reputational damage to victims, as well as compromising data security and privacy. It is difficult to identify a sector that has not been hit by cyberattacks in Brazil. Government agencies, hospitals, education groups, manufacturing, retail chains and technology companies have been attacked and made news in several newspapers.

Cybersecurity is a strategic issue to ensure business continuity and customer confidence. Therefore, it is essential to be prepared to face the threats and minimize the impacts of attacks. Based on data from CERT (Center for Studies, Response and Treatment of Security Incidents in Brazil), it can be seen that cyberattacks had a

peak in 2020 and showed a drop in the following year, but grew again in 2022.

As technology continues to advance at a rapid pace, the cybersecurity threat in Brazil grows constantly. In 2022, organizations across the country faced a range of cybersecurity threats, from ransomware attacks to data breaches and more. There were many different types of cybersecurity threats that businesses in Brazil had to encounter.

**Ransomware attacks:** Ransomware attacks are becoming increasingly common in Brazil, and this trend is likely to continue. Cybercriminals are often asking for payment in cryptocurrencies to make it harder to trace. Ransomware is a type of malware that encrypts an organization's data, rendering it unusable until a ransom is paid. These attacks can be devastating to businesses, causing significant data loss and downtime. To protect against ransomware attacks, organizations must invest in technology and rethink processes and provide security awareness training to employees to help them identify and avoid phishing scams.

In Brazil,  
cybersecurity  
measures are a  
**strategic**  
**investment** to  
ensure **business**  
**continuity**.



**Supply chain attacks:** Supply chain attacks are another growing threat in Brazil. In these, cybercriminals target a vendor or third-party supplier with the goal of gaining access to their customer networks. This can be particularly dangerous for organizations that rely heavily on third-party vendors or suppliers.

**Social engineering attacks:** Social engineering attacks, such as vishing, phishing and spear-phishing, continue to be a significant threat in Brazil. They involve cybercriminals tricking individuals into divulging sensitive information, such as login credentials or financial information. To protect against social engineering attacks, organizations should provide security awareness training to employees to help them identify and avoid these.

**IoT-based attacks:** With the growing adoption of IoT devices, the risk of IoT-based attacks is also increasing. IoT devices are often poorly secured, making them an attractive target for cybercriminals. To protect against IoT-based attacks, companies must ensure that IoT devices are properly secured with strong passwords and updated firmware.

**Insider threats:** Insider threats such as employee theft or sabotage continue to pose a significant risk to organizations in Brazil. To mitigate this risk, companies must implement strict access controls and monitor employee activity for suspicious behavior. In addition to the set of threats described above, other factors becoming a challenge for most organizations are:

**Rapidly evolving threat landscape:** Cyberthreats are constantly evolving, with new danger possibilities and attack methods emerging all the time.

**Lack of cybersecurity expertise:** Many companies lack the internal expertise needed to effectively manage their cybersecurity risks. This can make identifying and mitigating cyberthreats difficult, leaving companies vulnerable to attack.

**The increasing complexity of IT environments:** As companies adopt new technologies, their IT environments become more complex, with a greater variety of devices, applications and systems to manage. This complexity can make it difficult to effectively protect an organization's data and infrastructure.

**Human error:** Employees can be a weak link in an organization's cybersecurity defenses as they may inadvertently click on phishing emails, use weak passwords or fall for social engineering scams. To mitigate this risk, companies should provide security awareness training to employees and implement strict security policies and procedures.

**Budgetary constraints:** Cybersecurity solutions can be expensive, so many companies struggle to allocate enough resources to handle them. This can make investing in new technologies and hiring the expertise needed to effectively manage cyber risks difficult.

**Compliance requirements:** Companies must comply with regulatory requirements on cybersecurity, but these can be complex and difficult to understand and require significant resources and expertise. Even so, companies must ensure that they comply with these regulations, such as LGPD.

ISG has clearly observed this evolution in the cybersecurity market in Brazil and elsewhere, as vendors have had to adapt their security posture and solution architecture to better meet customers' needs for next-generation security by evaluating some major themes in quadrants.

Below we describe some trends presented by Brazilian and global companies.

### **Identity and Access Management (IAM)**

IAM is a critical component of a company's cybersecurity strategy because it helps control access to sensitive data and systems. In this year's study, we looked at the following trends in IAM:

**Cloud-based IAM:** Cloud-based IAM solutions are becoming increasingly popular as more companies move their data and applications to the cloud.

**Zero trust IAM:** Zero trust IAM is an approach that assumes that all users and devices are untrusted until they are verified.

**Identity Governance and Administration (IGA):** IGA solutions are becoming increasingly important as companies seek to manage many identities and access permissions across their networks and systems.

**Consumer IAM:** Consumer IAM solutions are becoming more important as companies seek to provide a seamless and secure user experience for customers accessing their applications and services.



**Machine-to-machine (M2M) IAM:** With the increasing adoption of IoT devices, M2M IAM solutions are becoming more important.

Companies must keep up with the latest trends and technologies to effectively manage their IAM risks and invest in the solutions and expertise needed to protect their systems and data.

### **Extended Detection and Response (XDR)**

XDR is an emerging cybersecurity technology that aims to improve threat detection and response by integrating multiple security data sources and applying advanced analytics to identify and respond to threats. Here are some of the key trends in XDR:

**Integration with cloud security:** XDR solutions are increasingly being integrated with cloud security solutions as more companies move their data and applications to the cloud.

**Automation and orchestration:** XDR solutions increasingly incorporate automation and orchestration features to help streamline the threat detection and response processes.

**Threat intelligence integration:** XDR solutions increasingly integrate threat intelligence feeds to provide context and prioritize potential dangers.

**Behavioral analysis:** XDR solutions increasingly incorporate behavioral analysis capabilities to help detect threats that may not be visible through traditional signature-based detection methods.

**Managed XDR services:** As XDR solutions become more complex, some companies are turning to managed XDR services to help them implement and manage these capabilities.

As companies look to improve their threat detection and response methods, XDR solutions will likely become an increasingly important part of their cybersecurity strategy.

### **Technical Security Services**

Technical cybersecurity services encompass a wide range of services that help organizations manage cybersecurity risks. Here are some of the key trends observed in technical cybersecurity services:

**Penetration testing and vulnerability assessments:** Penetration testing and vulnerability assessments are becoming more important as organizations seek to identify and remediate vulnerabilities in their networks and systems.

**Incident response services:** Incident response services are becoming more important as organizations seek to prepare for and respond to cybersecurity incidents.

**Security training and awareness:** Security training and awareness services are becoming more important as organizations seek to improve their employees' cybersecurity awareness and skills.

**Cybersecurity automation and orchestration:** Automation and orchestration are becoming more important in technical cybersecurity services as organizations seek to streamline security operations and respond to threats more quickly.

Technical cybersecurity services are evolving rapidly as organizations seek to effectively manage cybersecurity risks.

### **Strategic Security Services**

Cybersecurity consulting and strategic services help organizations develop and implement effective cybersecurity strategies to manage cybersecurity risks. Here are some of the key trends in cybersecurity consulting and strategic services observed in the ISG study:

**Risk management:** Risk management is becoming increasingly important in cybersecurity consulting and strategic services as it helps organizations identify, assess, and prioritize their cybersecurity risks, as well as develop risk mitigation strategies aligned with business objectives.

**Compliance and regulatory requirements:** Compliance and regulatory requirements are becoming more complex, with new regulations such as LGPD.

**Cybersecurity governance:** Cybersecurity governance is becoming more important as organizations seek to ensure that their cybersecurity policies and procedures are effective and aligned with their business objectives.



### **Developing cybersecurity programs:**

Effective cybersecurity development and programs include incident response plans, security awareness training, and vulnerability management.

**Cybersecurity analysis:** Cybersecurity analysis is becoming more important in cybersecurity consulting and strategic services.

Cybersecurity consulting services and strategic services are evolving rapidly as organizations seek to manage their cybersecurity risks more effectively.

### **Managed Security Services - SOC**

Managed security services (MSS) are outsourced cybersecurity services that provide organizations with comprehensive security solutions. Here are some of the key trends seen in the Managed Security Services - SOC quadrant:

**Cloud-based MSS:** With the increasing adoption of cloud computing, cloud-based MSS are becoming more popular.

### **Advanced threat detection and response:**

MSS vendors are increasingly using advanced analytics, ML and AI to detect and respond to threats more quickly and effectively.

**Zero trust security:** Zero trust security is becoming more important in MSS as organizations seek to improve their security posture.

### **Managed detection and response (MDR):**

MDR is an emerging trend in MSS that focuses on detecting and responding to threats more quickly and effectively.


### **Security automation and orchestration:**

Automation and orchestration are becoming more important in MSS as organizations seek to streamline their security operations and respond to threats more quickly.

To effectively manage cybersecurity risks, organizations must stay up to date with the latest trends and technologies in MSS and invest in the solutions and expertise needed to protect their systems and data.

Today, organizations in Brazil and around the world face a variety of cybersecurity challenges, including ransomware attacks, supply chain attacks, social engineering scams, IoT-based attacks and insider threats. It is no longer enough to just update antivirus to ensure information security. A broader, more strategic approach is needed to address these challenges.




 Provider Positioning

Page 1 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Accenture	Not In	Not In	Not In	Leader	Leader	Leader
Agility	Not In	Not In	Not In	Leader	Not In	Leader
Atos	Not In	Not In	Not In	Not In	Product Challenger	Product Challenger
BluePex	Not In	Contender	Not In	Not In	Not In	Not In
Broadcom	Leader	Leader	Product Challenger	Not In	Not In	Not In
Capgemini	Not In	Not In	Not In	Leader	Leader	Product Challenger
Cato Networks	Not In	Not In	Leader	Not In	Not In	Not In
Check Point	Contender	Product Challenger	Not In	Not In	Not In	Not In
Cipher	Not In	Product Challenger	Not In	Contender	Market Challenger	Product Challenger
Cirion	Not In	Not In	Not In	Not In	Not In	Leader



 Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Cisco	Contender	Contender	Leader	Not In	Not In	Not In
Claranet	Not In	Not In	Not In	Product Challenger	Product Challenger	Rising Star ★
Cloudflare	Not In	Not In	Market Challenger	Not In	Not In	Not In
Compugraf	Not In	Not In	Not In	Contender	Not In	Not In
CrowdStrike	Not In	Leader	Not In	Not In	Not In	Not In
CyberArk	Product Challenger	Not In	Not In	Not In	Not In	Not In
Cybereason	Not In	Product Challenger	Not In	Not In	Not In	Not In
Deloitte	Not In	Not In	Not In	Leader	Leader	Product Challenger
DXC Technology	Not In	Not In	Not In	Product Challenger	Not In	Contender
Edge UOL	Not In	Not In	Not In	Not In	Not In	Leader






## Provider Positioning

Page 3 of 8


	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Ericom Software	Not In	Not In	Product Challenger	Not In	Not In	Not In
E-TRUST	Leader	Not In	Not In	Not In	Not In	Not In
EY	Not In	Not In	Not In	Not In	Leader	Not In
FastHelp	Not In	Not In	Not In	Contender	Not In	Contender
Forcepoint	Not In	Not In	Leader	Not In	Not In	Not In
ForgeRock	Product Challenger	Not In	Not In	Not In	Not In	Not In
Fortinet	Contender	Rising Star ★	Product Challenger	Not In	Not In	Not In
GoCache	Not In	Contender	Not In	Not In	Not In	Not In
HackerSec	Not In	Not In	Not In	Not In	Contender	Not In
HPE (Aruba)	Not In	Not In	Rising Star ★	Not In	Not In	Not In



 Provider Positioning


	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Huge Networks	Not In	Contender	Not In	Not In	Not In	Not In
IBLISS	Not In	Not In	Not In	Not In	Product Challenger	Not In
IBM	Leader	Product Challenger	Not In	Leader	Leader	Leader
iboss	Not In	Not In	Product Challenger	Not In	Not In	Not In
Infinite Networks	Not In	Not In	Contender	Not In	Not In	Not In
ISH	Not In	Not In	Not In	Leader	Leader	Leader
iTeam	Not In	Not In	Not In	Contender	Not In	Contender
Italtel	Not In	Not In	Not In	Not In	Not In	Contender
Kaspersky	Not In	Leader	Not In	Not In	Not In	Not In
KPMG	Not In	Not In	Not In	Not In	Product Challenger	Not In



 Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Kyndryl	Not In	Not In	Not In	Rising Star ★	Product Challenger	Not In
Logicalis	Not In	Not In	Not In	Leader	Leader	Leader
Lookout	Not In	Not In	Contender	Not In	Not In	Not In
Microsoft	Leader	Leader	Not In	Not In	Not In	Not In
NEC	Not In	Not In	Not In	Not In	Market Challenger	Not In
Netskope	Not In	Not In	Leader	Not In	Not In	Not In
Nextios	Not In	Not In	Not In	Contender	Not In	Not In
NTT Ltd.	Not In	Not In	Not In	Leader	Rising Star ★	Leader
Okta	Leader	Not In	Not In	Not In	Not In	Not In
One Identity (OneLogin)	Product Challenger	Not In	Not In	Not In	Not In	Not In



 Provider Positioning

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
Open Systems	Not In	Not In	Contender	Not In	Not In	Not In
OpenText	Rising Star ★	Leader	Not In	Not In	Not In	Not In
Oracle	Contender	Not In	Not In	Not In	Not In	Not In
Palo Alto Networks	Not In	Product Challenger	Leader	Not In	Not In	Not In
Perimeter 81	Not In	Not In	Contender	Not In	Not In	Not In
Ping Identity	Product Challenger	Not In	Not In	Not In	Not In	Not In
Proofpoint	Not In	Not In	Contender	Not In	Not In	Not In
PwC	Not In	Not In	Not In	Leader	Leader	Not In
Redbelt	Not In	Not In	Not In	Not In	Contender	Not In
RSA	Leader	Not In	Not In	Not In	Not In	Not In




## Provider Positioning

Page 7 of 8

	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
SailPoint	Product Challenger	Not In	Not In	Not In	Not In	Not In
senhasegura	Leader	Not In	Not In	Not In	Not In	Not In
Service IT	Not In	Not In	Not In	Product Challenger	Not In	Not In
Skyhigh Security	Not In	Not In	Product Challenger	Not In	Not In	Not In
SONDA	Not In	Not In	Not In	Market Challenger	Not In	Market Challenger
Sophos	Not In	Product Challenger	Not In	Not In	Not In	Not In
Stefanini	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
TCS	Not In	Not In	Not In	Product Challenger	Product Challenger	Not In
TDEC	Not In	Not In	Not In	Not In	Not In	Contender
Thales	Product Challenger	Not In	Not In	Not In	Not In	Not In



 Provider Positioning

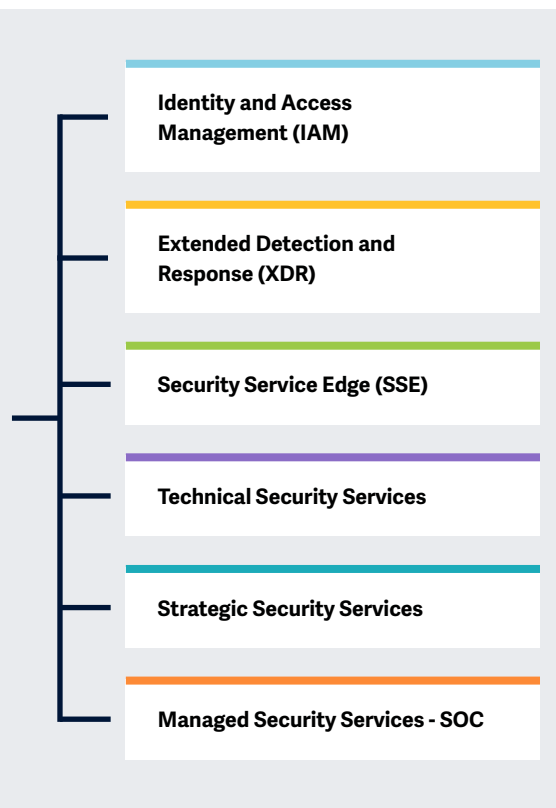
	Identity and Access Management (IAM)	Extended Detection and Response (XDR)	Security Service Edge (SSE)	Technical Security Services	Strategic Security Services	Managed Security Services - SOC
TIVIT	Not In	Not In	Not In	Product Challenger	Not In	Product Challenger
Trellix	Not In	Product Challenger	Not In	Not In	Not In	Not In
Trend Micro	Not In	Leader	Not In	Not In	Not In	Not In
T-Systems	Not In	Not In	Not In	Product Challenger	Not In	Leader
Unisys	Market Challenger	Not In	Not In	Not In	Product Challenger	Leader
Versa Networks	Not In	Not In	Leader	Not In	Not In	Not In
VMware	Not In	Leader	Contender	Not In	Not In	Not In
Wipro	Not In	Not In	Not In	Product Challenger	Product Challenger	Leader
Zscaler	Not In	Not In	Leader	Not In	Not In	Not In



In this study, the following quadrants were evaluated as main focus areas for IPL

## Cybersecurity – Solutions and Services 2023

Simplified Illustration; Source: ISG 2023



### Definition

The year 2022 could be termed as tumultuous from a cybersecurity perspective; although there was a decrease in data breach incidents, the year saw significantly increased sophistication and severity in the attacks. In 2022, enterprises increased their investment in cybersecurity and prioritized relevant initiatives to prevent attacks and improve their security posture. The continued learnings from the 2021 attacks led to executives and businesses of all sizes and across industries investing in measures to respond to and survive cybersecurity threats and cyberattacks.

From an enterprise perspective, even small businesses understood the impact of cyber threats and realized that they are actively targeted and are highly vulnerable to cyberattacks. This reinforced the need for (managed) security services and cyber resiliency services that would enable businesses to recover and resume operations quickly after a cyber incident.

Service providers and vendors are, therefore, offering services and solutions that help in recovery and business continuity.

From the perspective of the cybercriminals, they began exploiting large-scale vulnerabilities, such as Log4shell, and continued using ransomware to disrupt business activities, specifically targeting healthcare, supply chain and public sector services.

These prompted businesses to invest in capabilities such as identity and access management (IAM), data loss prevention (DLP), managed detection and response (MDR) and securing cloud and endpoints. The market is shifting toward integrated solutions, such as security service edge (SSE) and extended detection and response (XDR), which leverage the best tools and human expertise and are augmented with behavioral and contextual intelligence and automation to deliver a superior security posture.



### Scope of the Report

In this ISG Provider Lens™ quadrant report, ISG covers the following six quadrants for services/solutions: Identity and Access Management (IAM), Extended Detection and Response (XDR), Security Service Edge (SSE), Technical Security Services, Strategic Security Services and Managed Security Services (SOC), the latter of which is divided into Large Accounts and Midmarket quadrants.

Vendors offering Security Service Edge (SSE) solutions are analyzed and positioned from a global perspective, rather than by individual regions, as the market is yet in the early stages of maturity.

This ISG Provider Lens™ study offers IT decision-makers:

- Transparency about the strengths and weaknesses of the relevant software vendors
- A differentiated positioning of suppliers by segments (quadrants)
- Focus on the regional market

Our study serves as the basis for making important decisions about positioning, key relationships and market entry considerations. ISG's consultants and corporate clients also use the information in these reports to evaluate their existing supplier relationships and potential engagements.

### Provider Classifications

The provider position reflects the suitability of IT providers for a defined market segment (quadrant). Without further additions, the position always applies to all company sizes classes and industries. In case the IT service requirements from enterprise customers differ and the spectrum of IT providers operating in the local market is sufficiently wide, a further differentiation of the IT providers by performance is made according to the target group for products and services. In doing so, ISG either considers the industry requirements or the number of employees, as well as the corporate structures of customers and positions IT providers according to their focus area. As a result, ISG differentiates them, if necessary, into two client target groups that are defined as follows:

- **Midmarket:** Companies with 100 to 4,999 employees or revenues between \$20 million and \$999 million with central headquarters in the respective country, usually privately owned.
- **Large Accounts:** Multinational companies with more than 5,000 employees or revenue above \$1 billion, with activities worldwide and globally distributed decision-making structures.

The ISG Provider Lens™ quadrants are created using an evaluation matrix containing four segments (Leader, Product Challenger, Market Challenger and Contender), and the providers are positioned accordingly. Each ISG Provider Lens™ quadrant may include service providers that ISG believes have strong potential to move into the Leader quadrant. This type of provider can be classified as a Rising Star.

- **Number of providers in each quadrant:** ISG rates and positions the most relevant providers according to the scope of the report for each quadrant and limits the maximum of providers per quadrant to 25 (exceptions are possible).







### Provider Classifications: Quadrant Key

**Product Challengers** offer a product and service portfolio that reflect excellent service and technology stacks. These providers and vendors deliver an unmatched broad and deep range of capabilities. They show evidence of investing to enhance their market presence and competitive strengths.

**Contenders** offer services and products meeting the evaluation criteria that qualifies them to be included in the IPL quadrant. These promising service providers or vendors show evidence of rapidly investing in products/ services and a follow sensible market approach with a goal of becoming a Product or Market Challenger within 12 to 18 months.

**Leaders** have a comprehensive product and service offering, a strong market presence and established competitive position. The product portfolios and competitive strategies of Leaders are strongly positioned to win business in the markets covered by the study. The Leaders also represent innovative strength and competitive stability.

**Market Challengers** have a strong presence in the market and offer a significant edge over other vendors and providers based on competitive strength. Often, Market Challengers are the established and well-known vendors in the regions or vertical markets covered in the study.

★ **Rising Stars** have promising portfolios or the market experience to become a Leader, including the required roadmap and adequate focus on key market trends and customer requirements. Rising Stars also have excellent management and understanding of the local market in the studied region. These vendors and service providers give evidence of significant progress toward their goals in the last 12 months. ISG expects Rising Stars to reach the Leader quadrant within the next 12 to 24 months if they continue their delivery of above-average market impact and strength of innovation.

**Not in** means the service provider or vendor was not included in this quadrant. Among the possible reasons for this designation: ISG could not obtain enough information to position the company; the company does not provide the relevant service or solution as defined for each quadrant of a study; or the company did not meet the eligibility criteria for the study quadrant. Omission from the quadrant does not imply that the service provider or vendor does not offer or plan to offer this service or solution.





# Extended Detection and Response (XDR)

## Extended Detection and Response (XDR)

### Who Should Read This Section

This report is relevant to companies across all sectors in Brazil, aiming to evaluate vendors of extended detection and response (XDR) products designed to provide workspace security, network security or workload security.

In this report, ISG highlights the current market positioning of XDR product vendors working on threat detection and response in enterprises in Brazil and how each vendor addresses the key challenges faced in the region.

Agility is key in threat detection and response, as the cybercriminal's access time in the environment is proportional to the damage caused. Thus, companies are looking at XDR platforms with AI and automation tools to decrease the average time to detect and respond to threats.

The constantly emerging threats, such as new scams, new social engineering attacks and new ransomware tactics, are concerning for organizations. Vendors are investing in integrating their XDR platforms with intelligence feeds, to enable the tool to act against new threats.

Visual control of security, with dashboards, is increasingly demanded by companies, as it facilitates and simplifies the visualization of data, such as suspicious behaviors, protected assets and detected threats.



**Information Security Directors** should read this report to understand how XDR solution providers are upgrading to address new types of attacks.



**Chief Technology Officers (CTOs)** should read this report to understand the capabilities of XDR solution providers and how they can help them with their company's cybersecurity strategy.



**Data privacy professionals** should read this report to understand the relative positioning of XDR solution providers and how they assist in responding to data incidents.

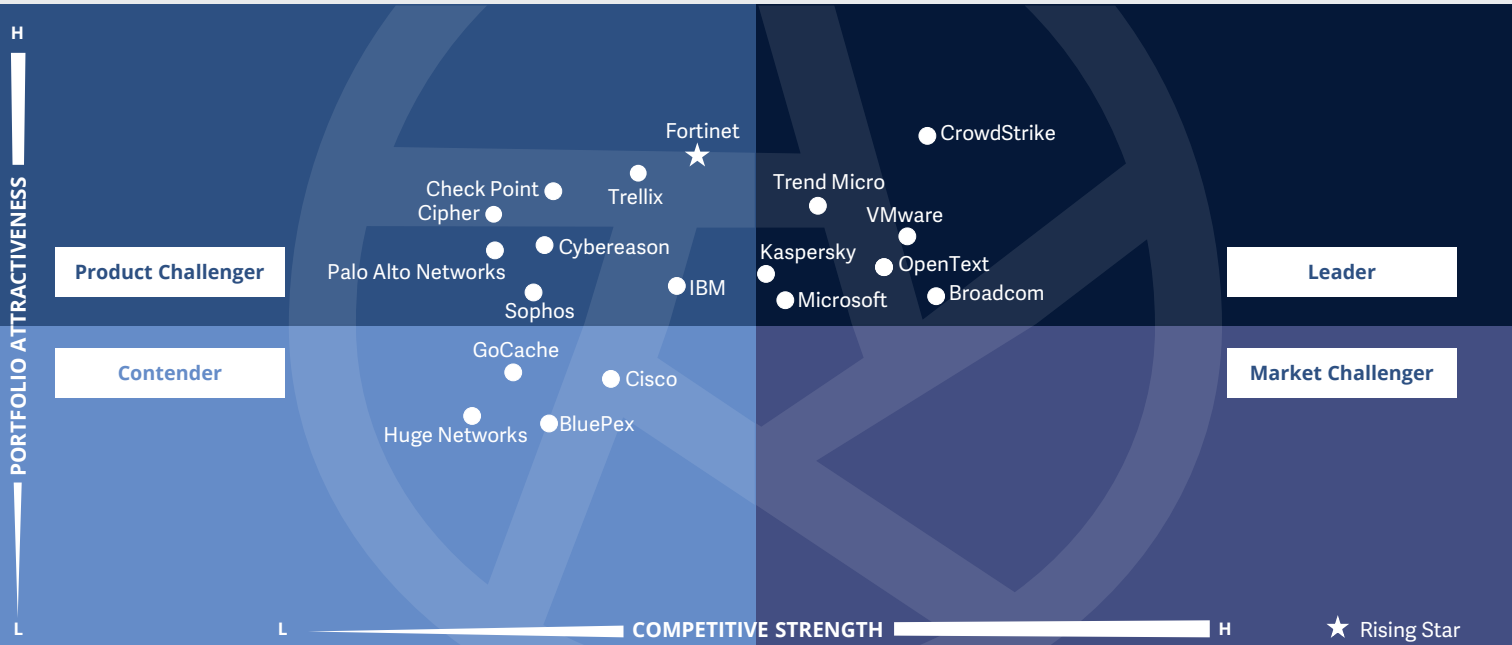


**Digital product professionals** should read this report to understand how XDR vendors can help with product stabilization to increase the safety of their customers.



**Cybersecurity – Solutions and Services**  
**Extended Detection and Response (XDR)**

Brazil 2023



This quadrant evaluates **XDR solution** vendors that provide software and services to continuously monitor all endpoints and provide full visibility. They can **analyze, prevent and respond to advanced threats.**

*David de Paulo Pereira*



## Extended Detection and Response (XDR)

### Definition

The XDR solution providers evaluated for this quadrant are characterized by their ability to provide a platform that integrates, correlates, and contextualizes data and alerts from various threat prevention, detection, and response components.

XDR is a cloud-delivered technology comprising multi-point solutions. It uses advanced analytics to correlate alerts from multiple sources, including weak individual signals to enable accurate detections. XDR solutions consolidate and integrate multiple products and are designed to provide comprehensive workspace, network, or workload security. Typically, XDR solutions aim to greatly improve the visibility and context of the identified threat across the enterprise. Therefore, these solutions include specific features including telemetry and contextual data analysis, detection, and response.

XDR solutions also comprise multiple products and solutions integrated into a single dashboard to visualize, detect and respond with sophisticated capabilities. High automation maturity and contextual analysis provide unique response capabilities customized to the affected system and prioritize alerts based on severity relative to known baseline structures.

Pure service providers that do not offer an XDR solution based on proprietary software are not included here. XDR solutions aim to reduce product dispersion, alert fatigue, integration challenges, and operational overhead, and are particularly well suited for security operations teams that have difficulty managing a portfolio of leading-edge solutions or deriving value from a security information and event management (SIEM) or security, orchestration, automation, and response (SOAR) solution.

### Eligibility Criteria

1. The XDR offering must be based on **proprietary software** and not on third-party software
2. An XDR solution **needs to have two main components: front-end XDR and back-end XDR**
3. **The front-end must have three or more solutions or sensors, including but not limited to endpoint detection and response, endpoint protection platforms, network protection (firewalls, IDPS), network detection and response, identity management, email security, mobile threat detection, cloud workload protection, and fraud identification**
4. The solution must provide **comprehensive and total coverage and visibility of all endpoints** in a network
5. The solution must demonstrate **effectiveness in blocking** sophisticated threats such as advanced persistent threats, as well as **ransomware and malware**
6. The solution must utilize **threat intelligence**, as well as analyze and provide **real-time information about the dangers emanating** from the endpoints
7. The solution should include **automated response capabilities**



## Extended Detection and Response (XDR)

### Observations

XDR solutions employ advanced analytics to investigate alerts from multiple sources, from weak individual signals to accurate threat detection. These solutions are designed to provide comprehensive security for spaces, networks and workloads by integrating multiple products into a single platform. The primary goal of XDR solutions is to increase the visibility of threats across an enterprise and provide context to identified threats.

These solutions incorporate specific capabilities, such as telemetry and contextual data analysis, as well as detection and response to enhance the custom capabilities of the affected system. Contextual analysis is highly automated and can prioritize alerts based on severity relative to known baseline structures.

Most companies offer integrations with other security tools and have built portfolios around endpoint detection and response capabilities. Successful product offerings often take a platform-based approach to be the leading solution provider in the market.

There is a growing demand for XDR solutions that can provide visibility across all assets and promptly detect and respond to threats. Metrics such as mean time to respond or detect are now widely used in marketing efforts for key players to differentiate themselves from competitors.

From the 261 companies assessed for this study, 19 have qualified for this quadrant, with seven being Leaders and one a Rising Star.

### Broadcom

**Broadcom** introduces a solution that uses ML and AI to offer a wide coverage of features, including adaptive protection, threat defense, firewall and intrusion prevention system and Symantec CloudSOC CASB.

### CrowdStrike

**CrowdStrike's** Falcon offers extensive experience in endpoint detection and response, cloud-native architecture for scalability and flexibility, real-time visibility and flexibility of acquisition through different bundles, from basic to the most advanced option.

### kaspersky

**Kaspersky's** Endpoint Security suite, with centralized management capabilities, provides advanced protection from cyberthreats, including real-time behavioral analysis, ML and signature-based scanning.

### Microsoft

**Microsoft** offers an integrated platform for threat detection and response, which includes Microsoft Sentinel and Microsoft Defender, as well as Microsoft Defender for Cloud. Microsoft's constant innovation is a highlight in all the security solutions presented.

### OpenText

**OpenText** acquired Micro Focus, bringing in important technologies such as AI categories, application development and digital operations management. The company's ArcSight Intelligence, with its XDR capabilities, offers panel detection, integration and customization.

### Trend Micro

**Trend Micro's** Vision One offers a converged security approach, integrating multiple security solutions into a single platform and unified policy management.

### VMware

**VMware's** Carbon Black solution involves the use of ML and AI for real-time threat detection and response, as well as a native multicloud architecture that allows you to deploy and manage multi-cloud environments.

### Fortinet

**Fortinet's** (Rising Star) FortiXDR platform offers an integrated and extensible security approach with AI and ML-driven threat detection. It uses a Security Fabric concept that integrates FortiGuard security services natively to provide coordinated detection and enforcement across the entire attack surface.



# Kaspersky



"Kaspersky has a sophisticated XDR solution for IT/TO protection and a portfolio of services ranging from security education and threat intelligence to solutions adhering to data sovereignty requirements in on-premises or cloud environments."

*David de Paulo Pereira*

## Overview

Kaspersky is an international private company headquartered in Moscow, Russia, with its holding company registered in the U.K. and its data processing infrastructure located in Switzerland. The company has subsidiaries in 31 countries and has some 4,000 highly qualified specialists. Its solutions protect about 240,000 corporate clients with performance in advanced cloud native endpoint protection EDR, XDR, MDR and threat intelligence. Kaspersky Latin America, headquartered in Brazil, is a business entity registered in the country since 2013 and a subsidiary of the holding company Kaspersky Limited, which is headquartered in the U.K.

## Strengths

**Advanced threat protection:** Kaspersky XDR collects data from multiple sources providing a complete view with integration to existing security tools providing unified visibility and correlation of security data through advanced analytics and machine learning identifying patterns and anomalies to improve threat detection and incident response.

### Centralized management and customizable policies:

The suite offers centralized management capabilities, allowing one to monitor and manage the security of endpoints and devices with visibility into security status and automated issue remediation. It also allows for the creation of customizable and tailored policies.

## Regional focus:

With over 1,600 partners in Brazil and 6,000 in Latin America, a regional team of over 130 employees, 64 of these in Brazil, Kaspersky offers Incident Response, SOC Management and Threat Research Center services. These services provide support in Portuguese and Spanish, ranging from user education to automated awareness programs.

### Kaspersky Transparency Centers:

The centers in Zurich, Madrid, Kuala Lumpur, Rome, Singapore, Tokyo, Utrecht, Woburn (Boston Region) and São Paulo share information about products, source code and performance with partners and governments.

## Caution

Kaspersky uses partners to serve the national market and has a Loyalty program with discount offers based on sales result certifications. However, some partners offer solutions from other manufacturers, which may result in a sales process guided by the partner's criteria.





# Appendix



The ISG Provider Lens™ 2023 – Cybersecurity Solutions and Services report analyzes the relevant software vendors/service providers in the Brazilian market, based on a multi-phased research and analysis process, and positions these providers based on the ISG Research™ methodology.

**Lead Author:**

David Pereira

**Research Analyst:**

Gabriel Sobanski

**Data Analysts:**

Rajesh Chillappagari and Shilpashree N

**Project Manager:**

Donston Sharwin

Information Services Group Inc. is solely responsible for the content of this report. Unless otherwise cited, all content, including illustrations, research, conclusions, assertions and positions contained in this report were developed by, and are the sole property of Information Services Group Inc.

The research and analysis presented in this report includes research from the ISG Provider Lens™ program, ongoing ISG Research™ programs, interviews with ISG advisors, briefings with services providers and analysis of publicly available market information from multiple sources. The data collected for this report represents information that ISG believes to be current as of April 2023, for providers who actively participated as well as for providers who did not. ISG recognizes that many mergers and acquisitions have taken place since that time, but those changes are not reflected in this report.

All revenue references are in U.S. dollars (\$US) unless noted.

The study was divided into the following steps:

1. Definition of Cybersecurity – Solutions and Services market
2. Use of questionnaire-based surveys of service providers/ vendor across all trend topics
3. Interactive discussions with service providers/vendors on capabilities & use cases
4. Leverage ISG's internal databases & advisor knowledge & experience (wherever applicable)
5. Use of Star of Excellence CX-Data
6. Detailed analysis & evaluation of services & service documentation based on the facts & figures received from providers & other sources.
7. Use of the following key evaluation criteria:
  - \* Strategy & vision
  - \* Tech Innovation
  - \* Brand awareness and presence in the market
  - \* Sales and partner landscape
  - \* Breadth and depth of portfolio of services offered
  - \* CX and Recommendation



## Author & Editor Biographies

Author



**David de Paulo Pereira**  
**Lead Author**

David de Paulo Pereira is a seasoned professional and lead author of several IPL reports for the Brazilian market. He has a track record of successful executive experience in digital transformation, team management, and project and service delivery. David has excelled in complex environments such as post-merger companies, establishing governance models, and standardizing work methods and processes. He has gained extensive experience in multicultural environments, having worked in private, public, multinational, and family-owned companies, both in Brazil and abroad.

David's expertise includes a profound understanding of Industry 4.0, such as Cloud, Big Data, Analytics, and RPA. He is skilled in strategic planning, technological innovation, portfolio management, and change management. Before joining TGT/ISG, David served as CIO and CTO for a UK-based software company and held the position of Executive Director responsible for IT Transformation Practice at EY. He also worked as CIO and CTO for global companies like Solvay and Jakko Poyry.

Author



**Gowtham Kumar Sampath**  
**Assistant Director and Principal Analyst**

Gowtham Sampath is a Senior Manager with ISG Research, responsible for authoring ISG Provider Lens™ quadrant reports for Banking Technology/Platforms, Digital Banking Services, Cybersecurity and Analytics Solutions & Services market. With 15 years of market research experience, Gowtham works on analyzing and bridging the gap between data analytics providers and businesses, addressing market opportunities and best practices. In his role, he also works with advisors in addressing enterprise clients' requests for ad-hoc research requirements within the IT services sector, across industries.

He is also authoring thought leadership research, whitepapers, articles on emerging technologies within the banking sector in the areas of automation, DX and UX experience as well as the impact of data analytics across different industry verticals.



## Author & Editor Biographies



*Research Analyst*

**Gabriel Sobanski**  
**Research Analyst**

Gabriel Sobanski is a research analyst at ISG and is responsible for supporting and co-authoring Provider Lens™ studies on ServiceNow Ecosystem, Oracle Ecosystem, Salesforce Ecosystem, Microsoft Ecosystem, MarTech Services, Cybersecurity Solutions and Services, and SAP HANA Ecosystem Services. He supports the lead analysts in the research process and co-authors the global summary report with market trends and insights. Gabriel also develops content from a business perspective. He has been in charge of his current role since 2021.

Before that, Gabriel worked as an IT consultant, where he gained experience and technical skills in quantitative and qualitative data collection, analysis, and presentation. His areas of expertise include industry, logistics, and market research.



*IPL Product Owner*

**Jan Erik Aase**  
**Partner and Global Head – ISG Provider Lens™**

Mr. Aase brings extensive experience in the implementation and research of service integration and management of both IT and business processes. With over 35 years of experience, he is highly skilled at analyzing vendor governance trends and methodologies, identifying inefficiencies in current processes, and advising the industry. Jan Erik has experience on all four sides of the sourcing and vendor governance lifecycle - as a client, an industry analyst, a service provider and an advisor.

Now as a research director, principal analyst and global head of ISG Provider Lens™, he is very well positioned to assess and report on the state of the industry and make recommendations for both enterprises and service provider clients.



### iSG Provider Lens™

The ISG Provider Lens™ Quadrant research series is the only service provider evaluation of its kind to combine empirical, data-driven research and market analysis with the real-world experience and observations of ISG's global advisory team. Enterprises will find a wealth of detailed data and market analysis to help guide their selection of appropriate sourcing partners, while ISG advisors use the reports to validate their own market knowledge and make recommendations to ISG's enterprise clients. The research currently covers providers offering their services across multiple geographies globally.

For more information about ISG Provider Lens™ research, please visit this [webpage](#).

### iSG Research™

ISG Research™ provides subscription research, advisory consulting and executive event services focused on market trends and disruptive technologies driving change in business computing. ISG Research™ delivers guidance that helps businesses accelerate growth and create more value.

ISG offers research specifically about providers to state and local governments (including counties, cities) as well as higher education institutions. Visit: [Public Sector](#).

For more information about ISG Research™ subscriptions, please email [contact@isg-one.com](mailto:contact@isg-one.com), call +1.203.454.3900, or visit [research.isg-one.com](http://research.isg-one.com).

### iSG

ISG (Information Services Group) (Nasdaq: III) is a leading global technology research and advisory firm. A trusted business partner to more than 900 clients, including more than 75 of the world's top 100 enterprises, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; strategy and operations design; change management; market intelligence and technology research and analysis.

Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,600 digital-ready professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data.

For more information, visit [isg-one.com](http://isg-one.com).





**AUGUST, 2023**

---

**REPORT: CYBERSECURITY – SOLUTIONS AND SERVICES**