Brought to you by Informa Tech

Publication date:
02 Nov 2023
Author(s):
Curtis Franklin, Principal Analyst, Enterprise Security Management

On the Radar: Interpres Threat Exposure Management Platform offers effective ways to identify and remediate cyberthreats

Summary

Catalyst

Risk has become the tie that binds all the pieces of a cybersecurity infrastructure into a seamless whole. Determining threat exposure is a critical component of cybersecurity risk, and the sole focus of the Interpres Threat Exposure Management Platform is to put threats in context, allowing an organization to prioritize threats and the steps to take to deal with the risk they present.

Omdia view

Omdia sees market momentum for solutions that improve an organization's risk posture, especially those that allows for proactive management of risk. The Interpres Threat Exposure Management Platform places threats into context, offers direction on prioritizing threat remediation, and provides guidance on how that remediation should proceed.

One of the primary issues with acting on risk is the complexity that can accompany turning data from individual cybersecurity components into information on risk, and then turning that information on risk into action on managing risk. Interpres' platform is intended to reduce the time and effort to get from data to risk management action. It does this not by aiming for full process automation, as many cybersecurity solutions do, but instead by assisting human analysts to do their jobs faster and more accurately. This

human assistance model fits squarely into trends being seen across cybersecurity, from training to generative artificial intelligence (AI) deployment.

Why put Interpres on your radar?

The Interpres Threat Exposure Management Platform does not replace existing cyberdefense products. Rather, the company wants to assist customers to make the most of the security products they own and the infrastructure they already have in place. This precise targeting will help Interpres sell “in conjunction with,” rather than in competition with, established cybersecurity players. In a time of a human skills shortage, a message of human amplification is compelling, especially when it does not require replacing or significantly rethinking existing systems.

Market context

Threat management is one of several prisms through which enterprises seek to identify and understand the risk facing the organization and whether that risk is acceptable. Three specific topics—vulnerability management, threat management, and risk management—are closely related and, in many ways, build one upon another in support of successful enterprise risk management.

One way to think about the three management systems is in the context of their intended audience. Vulnerability management systems tend to be used by those responsible for mitigating vulnerabilities through patches, updates, and other direct actions on software and firmware. Threat management’s human component generally falls onto managers at the heart of an audience that extends "downward” to hands-on analysts more often than “upward” to executives. Risk management, on the other hand, is quite frequently an executive function, extending in more and more cases all the way to the company’s executive board.

- **Vulnerability management:** a continuous, proactive, process of identifying, assessing, reporting, managing, and remediating cyber vulnerabilities. The process extends across endpoints, workloads, and systems. The goal of vulnerability management is generally to minimize the universe of potential security flaws and points of successful attacks that a malicious actor could use to launch a campaign.
- **Threat management:** most often thought of as a framework used by cybersecurity professionals to manage the lifecycle of a threat. The goal of the framework is to identify and respond to threats with speed and accuracy. Threat management involves identifying, prioritizing, managing, and monitoring threats to information systems.
- **Risk management:** in cybersecurity this involves identifying risks and vulnerabilities, and using policies, processes, and actions to ensure that the organization’s ongoing level of risk is acceptable. Cybersecurity risk management identifies a risk, assesses its likelihood and potential impact, prioritizes it for mitigation, follows through on mitigation, and continuously monitors the cyber infrastructure for new risks and the effects of risk mitigation.

The Interpres Threat Exposure Management Platform keeps to the middle path, helping customers understand the number of campaigns relevant to a given vulnerability, the techniques that are applicable to those campaigns, how frequent the campaigns have become, what the existing defense surface looks like, and then how the organization should figure out what to fix.

Interpres' platform faces competition on a number of different levels. Competitors on the vulnerability management detection and response (VMDR) side include Qualys, Rapid7 (InsightVM), Tenable (Vulnerability Management), and GFI (LanGuard). It is notable that the Qualys, Rapid7, and Tenable products fall into the category of risk-based vulnerability management (RBVM), which bases management decisions and remediation on the risk a particular vulnerability poses to the organization. It is also important to note that the Interpres Threat Exposure Management Platform integrates with many of these vulnerability managers, augmenting the vulnerability management data with Interpres' threat-prioritization information.

At the more-comprehensive risk management end of the scale, the competition includes Riskonnect's Active Risk Manager, Pathlock, and CURA's Enterprise Risk Management, as well as a variety of security information and event management (SIEM), next-generation firewall (NGFW), endpoint detection and response (EDR), and extended detection and response (XDR) tools.

And there are tools that are directly marketed as threat managers. These include Fortinet's FortiRecon, Recorded Future, Cisco Secure Malware Analytics, IntSights External Threat Protection (ETP) Suite, and Qualys VMDR. Just as with the VMDRs, Interpres' platform will integrate with many of the threat managers, using the output from those products as an input for Interpres threat prioritization.

Finally, Interpres sees consulting firms with cybersecurity expertise as competitors for its platform. The manual (or automated, with proprietary internal tools) threat assessments that come from these consultants contain the sort of threat prioritization that is available from the platform on a continuous, automated basis.

Product/service overview

The Interpres Threat Exposure Management Platform is a software-as-a-service (SaaS) platform that explores the customer's infrastructure and compares the findings against lists of known vulnerabilities and the campaigns exploiting them. It does this in order to provide both a customized numerical threat level and a list of actions to remediate threats and improve the threat-level metric.

Interpres' platform provides four major capabilities:

- Defense readiness: this automates the process of pulling together data on the state of infrastructure readiness and matches it with current cyberthreat advisories from various sources.
- Defense surface optimization: the threats that exist are filtered for those that could target the customer's infrastructure and existing cybersecurity controls. This optimization includes recommended improvements to the cybersecurity infrastructure to address prioritized threats.
- Prioritized vulnerability intelligence: this prioritizes the vulnerabilities that could be exploited in the customer's organization, according to their severity, the customer's exposure, and the state of existing deployed vulnerability management solutions.
- Exposure trend analysis: a step that examines the state of the customer's exposure over time in quantified form, showing its improvement or degradation in relation to the remediation suggested and acted upon.

In order to provide these capabilities, the platform integrates the results from a variety of different cybersecurity products and services—including cyber asset attack surface management (CAASM), cloud

security posture management (CSPM), SIEM, XDR, and vulnerability managers—then uses the data from them to build threat models and analytics, before incorporating the results into an Interpres Exposure Index score, along with recommendations for prioritized remediation of existing vulnerabilities.

It is notable that the Interpres Threat Exposure Management Platform does not deploy any sensors or monitors of its own. All of the data in the organization's computing infrastructure comes from existing security infrastructure devices. Interpres takes the data from these devices, combines it, and normalizes it into a single dataset that overlays the existing solutions and presents information in a way that cybersecurity staff can understand and act upon.

The platform uses the MITRE ATT&CK framework as one of its tools to categorize and prioritize threats based on the adversaries most likely to target an organization; the tools, tactics, and techniques those adversaries use; and how often the attacks are being seen in the wild. Interpres then recommends the mitigations, telemetry collection strategies, and detection logic best suited to fill the gaps in defenses across the enterprise, and prioritized to find and mitigate the threats most likely for the organization.

Interpres' scoring is along three major axes:

- Threat exposure scoring: profiles and rates an organization's exposure to threats including adversarial techniques, malware families, and threat groups.
- Defense posture scoring: profiles an organization's defensive capability against prioritized threats.
- Asset exposure scoring: looks at the assets in an organization's defense surface, and scans and identifies vulnerabilities in every network element.

A key point of the Interpres Threat Exposure Management Platform is that the monitoring is continuous and not at a single point in time. For this reason, results are shown as a graph that includes the current, ongoing score, rather than as a single score in isolation.

Score-trending is based on real-time information about vulnerabilities, including the specific common vulnerabilities and exposures (CVE) and common vulnerability scoring system (CVSS) information, as well as data drawn from the specific customer infrastructure and environment. The score is displayed as a number alongside a graph on the management console, showing cybersecurity managers the threat exposure as it exists at a point in time and as it compares to the score in both the immediate and the long-term past. Since the console also provides detailed information on how to most effectively improve the threat exposure score (also known as defense readiness), the graph is a good indicator of how effective previous remediation instructions have been.

Interpres says that, according to customers, the defense readiness information is the most valuable analysis. This information is developed from the data provided by cybersecurity infrastructure components and measured against a combination of factors including the MITRE ATT&CK framework, the severity of vulnerabilities discovered in the IT infrastructure, and the combination of those vulnerabilities weighed against the likelihood (given the organization's size, industry, and geography) of the vulnerabilities being exploited.

The Interpres Threat Exposure Management Platform can be deployed in three separate manners:

- SaaS deployed through Amazon Web Services (AWS): has the advantage of rapid deployment—some customers can deploy in as little as one day.

- Customer on-premises: deployed on the customer infrastructure with more-granular license control available to the customers, and comes with professional services for deployment and optimal use.
- Defense surface diagnostic: a turnkey offering deployed and managed by Interpres, with professional services for interpreting results and prioritizing responses.

Company information

Background

Interpres was founded in 2022 and emerged from stealth later that year with $8.5m in seed financing led by Ten Eleven venture capital firm. Its co-founders are Ian Roth, Michael Jenks, Michael Maurer, and Nick Lantuh, with Lantuh serving as CEO. All the founders are veterans of numerous cybersecurity startups and government organizations.

Interpres was founded in Mount Pleasant, South Carolina, with its headquarters currently in Virginia. The company has 24 employees, mostly concentrated in development and technical areas.

The strongest initial interest in the platform has come, according to the company, from organizations with strong fiduciary responsibilities—most notably financial and financial services companies required to answer to regulators, legislators, and customers. These companies tend to have extensive and complex reporting requirements that can take advantage of the platform's information-packaging and -formatting capabilities.

Another significant group of customers comes from governmental organizations, such as the Department of Defense, and their suppliers. As with the companies in the financial sector, the common element among these customers is regular, detailed reporting requirements to show the company's security status and the steps taken to manage threats and mitigations.

These companies are generally capable of performing the in-depth and repetitive tasks required to meet the reporting requirements, but doing so makes significant demands on the cybersecurity staff, and makes those demands on an ongoing basis. Relieving a significant portion of the organizational pain while delivering consistent, detailed information on threats and how to remediate them is Interpres' primary selling proposition.

Future plans

Interpres sees future opportunities in several areas. The first is through managed security service providers (MSSPs), with the aim of making the Interpres Threat Exposure Management Platform available to more and smaller customers. The advantage to Interpres is twofold: first, it brings the product in front of a much larger universe of customers; second, it limits the need to sell directly to those customers, leaning on the MSSPs to bear the cost of the sales process for smaller customers.

The next block of future opportunities lies in spreading into additional critical infrastructure customers beyond the defense and financial markets where its primary strengths are today. Interpres recognizes that regulatory requirements add weight to its unique selling proposition, and that it will benefit from those requirements spreading to additional market segments.

While Interpres says that it has no immediate interest in developing full process automation capabilities, it see advantages in developing additional APIs to connect on both the input and output sides with existing pieces of customer infrastructure. Interpres has been aggressive in building the connectors to take input from a variety of monitoring and analytical systems, and the company will benefit from creating similar APIs for job-ticketing systems, SIEMs, and other systems that can take the recommendations coming from the platform and turn them into automated actions.

Key facts

Table 1: Data sheet: Interpres

Product/service name	Interpres Threat Exposure Management Platform	**Product classification**	Continuous threat exposure management, proactive security
Version number	1.1.110223	**Release date**	September 2023
Industries covered	All	**Geographies covered**	North America and Europe
Relevant company sizes	Enterprise, midsize	**Licensing options**	Interpres is an annual software subscription, which can be SaaS delivered. The license model is based on the organization's size measured by the number of employees.
URL	https://www.interpressecurity.com	**Routes to market**	Direct, reseller
Company headquarters	Founded in South Carolina, headquartered in Virginia	**Number of employees**	24

Source: Omdia

Analyst comment

Interpres' greatest strength and its primary weakness are two sides of the same coin. It is focused on solving customers' problems from a single perspective that does not require the customers to either leave existing solutions behind or to replace existing solutions. Instead, the Interpres Threat Exposure Management Platform harvests data from the tools already in a customer's infrastructure and uses that data to provide information enabling the customer to assess their current status and act accordingly to reduce any exposure to meaningful threats.

That single perspective, though, assumes that the customer does not want a single, inclusive risk and a vulnerability manager that not only harvests data but also fully automates the remediation process. Interpres is targeted at providing assistance to the customer's analyst team—an approach that assumes the existence of that team of analysts.

When it comes to assisting the analyst team (and its management), the Interpres Threat Exposure Management Platform provides encyclopedic information in a form that is clear, easily understood, and easily acted upon. And, true to the service's name, the information provided is optimized to help the cybersecurity team manage the ongoing exposure to threats and to measure how successful that effort has been.

The focus on aiding cybersecurity teams also provides Interpres with a clear path to a next stage. A multi-tenant version of the platform aimed at the needs of MSSPs would dramatically expand the market for the platform and provide much smaller organizations with access to its features and capabilities.

In a market space that has seen competitors, generally, seek to expand their remit to include everything risk and its automation, Interpres' focus on managing threat exposure allows the company to bring to bear the experience of its founders and its growing technical staff to present information in a way that makes sense for prioritizing action against the most critical threats. A growing web of API-based interactions with service-ticketing systems and vulnerability managers will increase the platform's use cases while allowing Interpres to maintain its focus.

The most significant question for potential customers is whether the renewed industry interest in mergers and acquisitions will see Interpres swept into a larger parent in the next 36 months. Aside from that, Interpres Threat Exposure Management Platform solves a real set of problems for cybersecurity staff and solves them in ways that amplify the effectiveness of the stretched-thin staff on the ground.

Appendix

On the Radar

On the Radar is a series of research notes about vendors bringing innovative ideas, products, or business models to their markets. On the Radar vendors bear watching for their potential impact on markets as their approach, recent developments, or strategy could prove disruptive and of interest to tech buyers and users.

Further reading

Cybersecurity Decision Maker Survey 2023: Overall Findings (September 2023)

Cybersecurity Decision Maker Survey 2023: Overall Findings & Enterprise Security Management (September 2023)

"Interpres Security Emerges from Stealth to Help Companies to Optimize Security Performance" (December 2022)

Author

Curtis Franklin, Principal Analyst, Enterprise Security Management

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help you. For more information about Omdia's consulting capabilities, please contact us directly at consulting@omdia.com.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the "Omdia Materials") are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together "Informa Tech") or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com