VENDOR VISION 2023

PRESENTED BY EMA™

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Welcome to the 2023 RSA Conference edition of EMA's Vendor Vision!

VENDOR VISION 2023
PRESENTED BY EMA

If you are a veteran of the tech industry, you have likely attended plenty of conferences. It is easy to get lost in the din of the massive exhibition floors, and how do you prioritize which vendors to visit once you are there?

Vendor Vision is an attempt to fix that. The EMA information security, risk, and compliance management team selected 10 vendors that are a "must see" while attending the conference. These "visionaries" provide products and solutions that are some of the best in the industry.

So much of the information security world is trying to cut through the noise to find the diamond in the rough. We hope these brief summaries and recommendations help streamline the conference for you.

See you at the show!

Christopher Steffen, CISSP, CISA
Managing Research Director

Ken Buckler, CASP
Research Analyst

Anomali

https://www.anomali.com
Moscone South Expo Booth 1849
Detection and Response/Threat Hunting

Solution Name(s): The Anomali Platform

Anomali is a recognized leader in transforming security operations. Founded in 2013, Anomali launched the first ever threat intelligence platform to enable customers to gain visibility into the threat landscape and the ever-evolving adversary. The Anomali Platform transforms insights into actioned intelligence through broad industry partnerships and Anomali's own Threat Research team, which provides intelligence insights across several threat categories. The categories include malware, fraud, mobile, adversary, etc., as well as automated workflows for ingestion of structured and unstructured data, machine learning-based deduplication and false positive reduction, and dissemination of intelligence to a vast set of security controls.

What Sets Them Apart

Anomali's approach to transforming security operations relies on reimagining the problem from a business outcome standpoint. The Anomali Platform helps customers maximize their visibility into their risk, their security telemetry, and the threat landscape. It complements this visibility with insights that enable prioritization of the business risk, prediction of the attacker's next steps, and resolution to reduce impact. The Anomali Platform also accelerates responses through automating core workflows across the entire risk lifecycle to maximize analyst efficiency and scale security operations. Anomali helps customers maximize their current investments while also helping assess future risk and investments through risk-informed decisioning.

One More Thing

Security operations is increasingly getting more complex and more demanding. However, it's also increasingly crucial to business growth. Modernizing security operations entails unlocking visibility into the entire digital estate, actioning that expanded visibility, and scaling it. Anomali gives organizations the confidence to improve operational resilience through actioned visibility and automated security operations, unshackling the technological transformations needed to advance business growth.

VENDOR VISION 2023
PRESENTED BY EMA

The EMA Perspective

At the RSA Conference, you will hear everyone claim to have the ultimate solution for XDR. In fact, at the 2022 conference, we counted no fewer than 70 different detection and response solutions. We promise that there are not 70 detection and response solutions that are worthy of the name, much less ones that actually solve enterprise security concerns. Anomali is the exception. In this crowded detection and response environment, The Anomali Platform's detection and response capabilities are second to none. Coupled with best-in-class threat hunting, they are a security platform that merits your attention and consideration. Don't get lost in the vaporware of the pretend XDR providers and spend some time at the conference learning more about Anomali.

Armis

https://www.armis.com
Moscone South Expo Booth 1127
CAASM and Vulnerability Management

Solution Name(s): Armis Asset Intelligence & Security Platform

Armis, a leading asset visibility and security company, provides the industry's first unified asset intelligence platform designed to address the new extended attack surface that connected assets create. Fortune 100 companies trust Armis's real-time and continuous protection to see with full context all managed and unmanaged assets across IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G. Armis provides passive cyber asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in California.

What Sets Them Apart

The Armis Asset Intelligence & Security Platform offers unparalleled insights into all connected assets, wired and wireless, within and surrounding OT networks. Armis discovers, classifies, and profiles, offering rich contextual insights into every asset—including SCADA, PLCs, DCS, IIoT, IoT, IoMT, and IT—and the interconnected support devices that keep organizations operational. Armis interoperates seamlessly with the existing tech toolset to immediately focus attention on critical events and to prevent their expansion, mitigate their effects, and resolve them quickly.

One More Thing

By monitoring all assets and their transactions and dependencies, Armis delivers true insights into the cyber asset attack surface found within the entire enterprise.

VENDOR VISION 2023
PRESENTED BY EMA

The EMA Perspective:

While connected assets greatly help with productivity, efficiency, and profitability, these assets also introduce new risks to the enterprise. Armis has a vision of the future of cybersecurity utilizing an asset-centric approach. Through this approach, better visibility and context can achieve superior protection of the organization from cyber threats.

When it comes to detecting cyber threats, visibility is key. Armis provides enhanced visibility to the enterprise by improving current tools instead of replacing them.

CyberGRX

https://www.cybergrx.com
Moscone South Expo Booth 4432
Third-Party Cyber Risk Management

Solution Name(s): CyberGRX Exchange

CyberGRX is the world's first and largest third-party risk Exchange, equipping organizations with unparalleled cyber risk intelligence. Powered by 13,000 attested assessments, 225,000 company profiles, data on 425 of the 500 most requested vendors, and 100% standardized data, CyberGRX provides third-party threat intelligence, predictive risk insights, outside-in scanning and scoring, and a portfolio-wide view of security gaps. As a result, cybersecurity professionals can plan appropriately, make decisions confidently, and sleep soundly.

What Sets Them Apart

CyberGRX is the only risk management platform in the world that includes comprehensive data on over 225,000 third parties. Security practitioners no longer have to chase vendors or wait for assessment data. Leveraging CyberGRX's sophisticated data analytics, predictive risk intelligence, real-world attack scenarios, and real-time threat intelligence, CISOs can make data-informed decisions faster and prioritize risks more effectively. CyberGRX uses this data to give customers the ability to eliminate the sole reliance on "point in time" third-party risk assessments or single vendor assessments. CyberGRX's platform is dynamic and scalable to a real-time and prioritized view of critical risks as business and threat landscapes evolve.

One More Thing

In Q1 2023, CyberGRX added new features to the Exchange. They announced the availability of a Predictive Data tool to the Exchange platform's Attack Scenario Analytics feature, which allows organizations to pinpoint outliers that will require further assessments to ensure they meet their security standards. Upon uncovering risk, CyberGRX can also provide a path forward with remediation by leveraging MITRE techniques to create kill chains and use cases. Additionally, they added Portfolio Risk Findings, which gives customers visibility into their riskiest vendors based on customized risk views that are continuously monitored based on the domain cyber hygiene and industry intelligence gleaned from technology partners. CyberGRX is also integrating with other software and risk management providers to further streamline third-party cyber risk programs.

VENDOR VISION 2023
PRESENTED BY EMA

The EMA Perspective

We have been following IT regulatory and compliance trends for over 20 years and one thing is certain: the regulatory controls and vendor due diligence requirements have always increased and will continue to increase. The CyberGRX Exchange is a game-changer for companies looking to decrease their spending on risk management and compliance. Combined with predictive assessment results, CyberGRX truly allows organizations to shine a light on third-party security blind spots. Organizations looking to better prioritize risks and make smarter decisions would do well to implement a solution like CyberGRX Exchange.

Dynatrace

https://www.dynatrace.com
Moscone South Expo Booth 1261
Application Security

Solution Name(s): Dynatrace Application Security

Dynatrace (NYSE: DT) exists to make the world's software work perfectly. Their unified software intelligence platform combines deep observability and continuous runtime application security with the most advanced AIOps to provide answers and intelligent automation from data at enormous scale. This enables innovators to modernize and automate cloud operations, deliver software faster and more securely, and ensure flawless digital experiences. That is why the world's largest organizations trust the Dynatrace® platform to accelerate digital transformation.

What Sets Them Apart

Dynatrace unifies observability and security in the same platform with full topological and dependency mapping context. This enables causal AI to determine precisely where vulnerabilities exist and what the risk of each vulnerability is based on the applications and processes that may introduce an attack vector for the vulnerability. For example, a vulnerability in a running production environment that is adjacent to the internet and/or with access to sensitive data is higher risk than if the vulnerability is inaccessible.

One More Thing

When security vulnerabilities are introduced or detected in an environment, it is critical to instantly know the severity of each instance. Dynatrace is the only platform that identifies precisely where the vulnerabilities are, quantifies the risk associated with each vulnerability, prioritizes which vulnerabilities to remediate in which order, and automates the remediation process. This has immense value when Log4Shell-type issues occur.

The EMA Perspective

Nearly every company is, has, or will be embarking on a digital transformation journey at some point, whether that's app modernization, taking advantage of cloud-native capabilities, or updating to the latest security constructs and standards. Without observability, this journey will hit some potholes and possibly run full speed into a brick wall. Dynatrace is the map that the enterprise needs for their digital transformation journey. Dynatrace is the industry leader in observability, providing contextual, relevant environmental insights for practitioners and business leaders. Security professionals and dev teams are looking for the best (and easiest) way to gain visibility into application security and functions—and Dynatrace is the answer.

ELASTIC

https://www.elastic.co

Moscone North Expo Booth 5879

SIEM & Security Analytics, XDR, Endpoint, Cloud Security

Solution Name(s): Elastic Security

Elastic is a platform for search-powered solutions for enterprise search, observability, and security. They enhance search experiences, keep mission-critical applications running smoothly, and protect against cyber threats for over 19,000+ customers.

Founded in 2012, Elastic is a public company (NYSE: ESTC). Its customers include more than half of the Fortune 500. Delivered wherever data lives, in one cloud, across multiple clouds, or on-premises, Elastic enables its customers to achieve new levels of success at scale and on a single platform.

What Sets Them Apart

Elastic approaches security as a data problem. They excel at analyzing, visualizing, and allowing customers to search through data quickly to protect, investigate, and respond to security threats. Elastic Security intends to help modernize security operations for enterprise customers with a unified SIEM and security analytics, EDR, and cloud security solution.

One More Thing

Elastic is making huge strides in driving cloud security with our SIEM and security analytics capabilities. Elastic's cloud security innovation delivers more value and reduces risk for Elastic Security customers.

The EMA Perspective

With their focus on merging data visibility for cloud and on-premises security monitoring, Elastic provides a powerful tool for hybrid organizations to simplify workflows and improve productivity. Attackers know that visibility across hybrid environments has been challenging and utilize switching between environments to throw off analysts and increase dwell time. Elastic helps level the playing field, restoring critical security visibility to the enterprise. Cloud is the new endpoint, and while traditional security methods don't apply to cloud, we still need to protect those traditional endpoints as well. With Elastic Security, users can monitor the entire environment in a single pane of glass, helping modernize today's hybrid enterprise.

F5

https://www.f5.com
Moscone North Expo Booth 5435
Application Security, API Security

Solution Name(s): F5 Distributed Cloud WAAP

F5 is a multi-cloud application services and security company committed to bringing a better digital world to life. F5 partners with the world's largest, most advanced organizations to secure and optimize apps and APIs anywhere: on-premises, in the cloud, or at the edge. F5 enables organizations to provide exceptional, secure digital experiences for their customers and continuously stay ahead of threats.

What Sets Them Apart

F5 Distributed Cloud WAAP is a SaaS-based offering integrating F5's industry-leading web application firewall (WAF), bot mitigation, DDoS protection, and API protection capabilities into a single, easy-to-deploy solution that enables SecOps and DevOps teams to enforce consistent security policies wherever their applications are deployed. With the F5 Distributed Cloud WAAP, organizations can streamline the deployment and operation of modern containerized apps with cloud-native management, consistent security, and end-to-end observability—from the data center to the cloud and the edge. This solution brings together the best of F5 application security technologies, delivering flexible deployment options that support multiple applications, robust API security with behavioral analysis and anomaly detection, high-efficacy bot defense, protection that extends beyond traditional WAAP security, and a purpose-built platform to secure hybrid app environments

One More Thing

The momentum of F5's Distributed Cloud Services, introduced in 2022, has been accelerated by unified security management and bolstered by the recent announcement of Distributed Cloud App Infrastructure Protection (AIP). Crucially, F5 gives customers ultimate flexibility for protecting organizations' specialized apps and infrastructure. Specialized connectors simplify integration with leading cloud platforms, such as AWS, Salesforce, Adobe Commerce Cloud, and ForgeRock. Additionally, F5 Distributed Cloud Connector for BIG-IP 17.1 now delivers seamless access to enhanced bot defense, authentication intelligence, account protection, and client-side defense solutions, dramatically simplifying service deployment to improve user security and personalization.

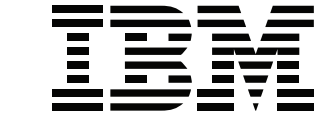
VENDOR VISION 2023
PRESENTED BY EMA

The EMA Perspective

Looking for API security? F5 invented it, improved it, and pushed the rest of the security world to pay attention to it. They are the leaders when it comes to cloud, application, and network security. Most security vendors are concentrating on providing point security solutions. While this is generally a great approach, organizations are inundated by dozens of point solutions to solve their security challenges. F5 takes a different, wholistic approach to security and is one of the few vendors that has the experience and portfolio to be able to effectively do it. F5 made strategic acquisitions and updates to core products to cement their leadership in the security space. When looking for network security, WAF/WAAF, and cloud security solutions, F5 is one of the best complete solutions to consider.

IBM Security

https://www.ibm.com/security
Moscone North Expo Booth 5658
Threat Detection and Response



Solution Name(s): QRadar, IBM Security Guardium, IBM Verify, IBM MaaS360, IBM X-Force

IBM Security helps secure the world's largest enterprises and governments with an integrated portfolio of security products and services infused with dynamic AI and automation capabilities. The portfolio, supported by world-renowned IBM Security X-Force® research, enables organizations to predict threats, protect data as it moves, and respond with speed and precision without holding back business innovation. With worldwide global security expertise spanning over 5,000 security experts, thousands of organizations trust IBM as their partner to assess, strategize, implement, and manage security transformations.

What Sets Them Apart

A strong differentiator is IBM's commitment to open and connected tooling, as showcased with its dedication to third-party integrations and shift to embracing community-based functionalities, such as the Grafana dashboarding plug-in available with the log management tool. IBM Security is an initial contributor to the OCA project, which is comprised of global, like-minded cybersecurity vendors, thought leaders, and users who are interested in fostering an open cybersecurity ecosystem and solving the interoperability problem.

One More Thing

The IBM Security suite of products has been strategically architected to simplify and unify the analyst experience. Each solution is purpose-built to assist the security analyst for faster alert detection and response workflows in fewer screens and minimal clicks. Featuring AI-powered automated investigation, analysts will spend less time evaluating and take action sooner. The suite brings together all core technologies needed for the modern Security Operations Center built on an open platform, with a wide partner ecosystem for flexibility and connections across IBM and third-party toolsets.

The EMA Perspective

Looking around the expo hall, you will find that the center square of your "buzzword bingo" sheet is likely something around detection and response or threat detection/hunting. Most of the vendors talking about threat detection and response only have a partial solution (if any). IBM is different. So many associate IBM with the goliath tech company of their parents, and while that may be true, that is only part of the story. IBM Security is *THE* leader in data security and threat detection. Companies looking for a complete solution for security considerations should pay a visit to IBM. QRadar, Guardium, and IBM's vast array of service offerings make IBM the trusted and experienced security partner that many companies are searching for.

Netenrich

https://netenrich.com

Moscone South Expo Booth 4241

Data Analytics for Secure Operations

Solution Name(s): Resolution Intelligence Cloud

Netenrich boosts the effectiveness of organizations' security and digital operations so they can avoid disruption and manage risk. Its Resolution Intelligence Cloud is a native-cloud data analytics platform for enterprises and services providers that need highly scalable, multitenant security operations and/or digital operations management. The platform uses Google Chronicle as its scalable, fast security data lake. Resolution Intelligence Cloud transforms security and operations data into intelligence that organizations can act on before critical issues occur. More than 3,000 customers and managed service providers rely on Netenrich to deliver secure operations at scale.

What Sets Them Apart

Unlike traditional point solution tools, Resolution Intelligence Cloud uses behavioral, anomaly, and situational analytics coupled with business-risk awareness to prioritize the security of critical assets. Resolution Intelligence Cloud is a new way to manage security and digital ops with the scale and speed of Google Chronicle built in. With real-time data analytics, machine learning, and automation, you can identify, track, and respond to threats quickly. You can also proactively find and fix vulnerabilities, dramatically increase SOC effectiveness and up-level the team, and improve performance and efficiencies of security systems and tools.

One More Thing

Digital ops and security share a common goal of keeping the business operating securely at optimal capacity. To succeed in this shared mission, you need to create a cohesive "digital + security" approach supported by a team that collaborates and optimizes the resources at hand—both human and machine.

VENDOR VISION 2023

PRESENTED BY EMA

The EMA Perspective

Through their scalable approach to cybersecurity data analytics, Netenrich provides a powerful toolset to optimize and enrich the usage of other tools within the enterprise. They have a vision of digital operations and security moving from traditional siloed models to a unified data processing experience. This approach can help keep organizations secure and operating smoothly. Helping ITOps and security teams work together is an extremely important goal for all organizations, and Netenrich's solution helps organizations achieve that collaboration.

Ordr

https://ordr.net
Moscone South Expo Booth 5314
Cyber Asset and Attack Surface Management

Solution Name(s): Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT devices. Ordr uses deep packet inspection and advanced machine learning to discover every device, map all communications, identify risk, profile behavior, and automate policies to stop active threats and improve security. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance, and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures.

What Sets Them Apart

Ordr uses deep packet inspection, API integrations, and application decoding techniques to automatically identify, classify, and gain granular context for all devices. Ordr learns all device behaviors, creates a baseline, and maps device communication patterns with the Ordr Device Flow Genome. By establishing these behavior baselines for each device, organizations can immediately identify and respond to any anomalies. Ordr makes it easy to protect every connected device, regardless of where it is and how it might be exposed.

One More Thing

No single tool can address all security requirements. Ordr has over 80 integrations and continues expanding and deepening integrations across the security and IT ecosystem. Data from various sources, including the network and external tools, provide rich input for analysis and are required for a comprehensive view of devices and risk.

VENDOR VISION 2023
PRESENTED BY EMA

The EMA Perspective

Traditional security practices have always been fragmented with endpoints and servers getting the most attention, while IoT, IoMT, and OT devices are traditionally neglected, sometimes intentionally, to prevent operational compatibility issues. Most traditional security solutions have always been agent-based, which is impossible for many non-traditional devices, or network-based without any account for context of connections. By implementing a learning component to their solution, Ordr enables security analysts to protect these devices, even if they're not an IoT expert. With more IoT devices becoming commonplace, this type of protection will be key for tomorrow's enterprise.

Security Journey

https://www.securityjourney.com
Moscone South Expo Booth 5529
Secure Coding Training

Solution Name(s): Application Security Education Platform

Three seasoned software engineers and security practitioners went on separate missions to reduce software vulnerabilities through effective training. These efforts created two industry-leading training solutions: HackEDU and Security Journey. The two application security training companies became one in the spring of 2022 when HackEDU acquired Security Journey and adopted the Security Journey name. Today, Security Journey offers robust application security education tools to help developers and the entire SDLC team recognize and understand vulnerabilities and threats and proactively mitigate these risks. The knowledge learners acquire in Security Journey's programs go beyond helping learners code more securely: it turns everyone in the SDLC into security champions. Organizations with teams of security champions develop a security-first mindset that allows them to deliver safer, more secure applications.

What Sets Them Apart

Security Journey trains developers and everyone in the SDLC on application security using a programmatic approach that increases knowledge as much as 85%.

One More Thing

Security Journey believes that over time, organizations will make application security a top priority to protect customer data and reduce organizational risk. Once organizations focus on proactively reducing application vulnerabilities, secure coding training will become a security staple, like code scanning and code reviews. Since Security Journey is one of the top three providers, they expect this will drive innovation and business growth for all secure coding training providers.

VENDOR VISION 2023
PRESENTED BY EMA

The EMA Perspective

Tools have their place, but it's important to invest in the human element for cybersecurity. Security Journey's vision is for organizations to proactively invest in their people to write better, more secure code. This proactive approach to reducing software vulnerabilities, and in the process reducing organizational risk, is quickly becoming just as important as code reviews and code-scanning tools.

After all, it's better to prevent vulnerabilities in the first place than try to fix them after software is already developed and deployed to production.

Honorable Mentions

Axonius	Cybersecurity Asset Management	South Expo Booth 0734
Coalfire	Information Security and Privacy Compliance	South Expo Booth 4219
Digital AI	Application Security	North Expo Booth 5424
Dragos	ICS/OT Cybersecurity	North Expo Booth 5214
Gigamon	Network and Cloud Security and Compliance	South Expo Booth 2227

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals, and IT vendors at **www.enterprisemanagement.com**. You can also follow EMA on **Twitter** or **LinkedIn**.

2770 Arapahoe Road, Ste 132 - 544, Lafayette, CO 80026 +1 303.543.9500 **www.enterprisemanagement.com**

4262.033023