VENDOR VISION 2022

PRESENTED BY **EMA**™

EMA™

IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING

Table of Contents

Welcome to the inaugural edition of EMA's Vendor Vision!

VENDOR VISION 2022

PRESENTED BY **EMA**

If you are a veteran of the tech industry you have likely attended plenty of conferences, both large and small. It is really 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 help fix that. The EMA information security, risk, and compliance management team has selected 10 vendors that are a "must see" while attending the conference. These "visionaries" all 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

Appgate

https://www.appgate.com

Moscone South Expo Booth 0345

Network Security

Solution Name(s):
Appgate SDP

Appgate is the secure access company. We empower how people work and connect by providing solutions purpose-built on Zero Trust security principles. This people-defined security approach enables fast, simple, and secure connections from any device and location to workloads across any IT infrastructure in cloud, on-premises, and hybrid environments. Appgate helps organizations and government agencies worldwide start where they are, accelerate their Zero Trust journey, and plan for their future.

What Sets Them Apart:

Appgate's mission is to empower and protect how people work and connect by enabling any user on any device to securely access any application, use any network, and perform any transaction. We provide:

- Identity-centric and context-aware Zero Trust access solutions that ensure security and compliance across all environments, including on-premises, hybrid, and cloud-native
- A digital threat protection and risk-based authentication and comprehensive risk management tool designed to identify and eliminate attacks before they occur across social media, phishing attacks, bogus websites, and malicious mobile apps

One More Thing:

Appgate SDP is a Zero Trust access solution that aligns with the core principles of Zero Trust and independent reference architectures published by NIST (800-207) and the Cloud Security Alliance. Our dynamic and versatile software-defined perimeter architecture is a comprehensive ZTNA solution that goes well beyond remote users and web applications.

VENDOR VISION 2022

PRESENTED BY **EMA**™

The EMA Perspective:

Network security has always been a crowded market, with each and every vendor promising "the best" and "leading" protection of your networks and infrastructure. Appgate's approach is different. Microsegmented networks are nothing new, but the software-defined perimeter (SDP) implementation is arguably the cornerstone of any Zero Trust architecture. Appgate is the leader in SDP, and their visionary leadership coupled with their intuitive features from their very non-complicated installation means they are absolutely worth evaluating for any organization going on a Zero Trust journey.

Axonius

Moscone South Expo Booth 0943
Cybersecurity Asset Management, CAASM

AXONIUS

VENDOR VISION 2022

PRESENTED BY **EMA**™

Solution Name(s):
Axonius Cybersecurity Asset Management
Axonius SaaS Management

Axonius gives customers the confidence to control complexity by mitigating threats, navigating risk, automating response actions, and informing business-level strategy. With solutions for both cyber-asset attack surface management (CAASM) and SaaS management, Axonius is deployed in minutes and integrates with hundreds of data sources to provide a comprehensive asset inventory, uncover gaps, and automatically validate and enforce policies. Cited as one of the fastest-growing cybersecurity startups, with accolades from CNBC, Forbes, and Fortune, Axonius covers millions of assets, including devices and cloud assets, user accounts, and SaaS applications for customers around the world.

What Sets Them Apart:

Axonius is unique in the market because it connects to over 450 data sources to create an always up-to-date asset inventory, uncover gaps, and create automated response actions. Axonius does not scan, doesn't require an endpoint presence, and doesn't sniff network traffic. Instead, by connecting to what we call "adapters" (API connections to the tools customers already use), companies can deploy Axonius quickly and it can adapt to inevitable change.

One More Thing:

We are the fastest-growing cybersecurity company in history because Axonius solves a problem: letting customers easily understand what assets they have and whether they are managed and secured.

The EMA Perspective:

Axonius is a cybersecurity asset management solution that aggregates all of an organization's asset data, assess the data based on the environment or standard, and integrates with existing security infrastructure, all to improve organization's vulnerability management programs. Further, users can utilize the Enforcement Center to take over 80 recommended or custom actions to prevent vulnerabilities from propagating and increasing enterprise risk. Organizations looking to significantly improve their cybersecurity and risk posture through asset management would do well to evaluate and adopt a solution like Axonius.

Coalfire

https://www.coalfire.com
Presenting on June 9
Application Security

Solution Name(s):
Coalfire Application Security

The world's leading organizations – the top 5 cloud service providers, 8 of the top 10 SaaS businesses, and 3 of the top 5 in financial services, healthcare, and ecommerce – rely on Coalfire to strengthen their security postures and secure their digital transformations. As the largest global firm dedicated to cybersecurity, Coalfire delivers a full lifecycle of solutions through professional services, technology platforms, and managed services to help organizations solve their toughest cyber challenges. With more than 20 years of proven cybersecurity leadership, Coalfire combines extensive cloud expertise, advanced technology, and innovative approaches that fuel success.

What Sets Them Apart:

Coalfire's end-to-end services span the complete software development lifecycle (SDLC), enabling operational efficiencies, consistency, and speed to market. Its application vulnerability platform, ThreadFix, manages, reduces, and reports on cloud-native application security risks. Coalfire's AppSec and cloud security technical experts support the leading cloud service providers and more than 500 successful projects each year. Its thought leadership drives AppSec innovation, including more than 10 years of Black Hat training, AppSec research reports, and speaking engagements.

One More Thing:

While cybersecurity is a priority for enterprises worldwide, requirements differ greatly from one industry to the next. Coalfire understands industry nuances and works with leading organizations in the cloud and technology, financial services, government, healthcare, and retail markets.

VENDOR VISION 2022

PRESENTED BY EMA

The EMA Perspective:

With a record high of 20,139 new vulnerabilities reported to the National Vulnerability Database in 2021, application security is now more important than ever. Unfortunately, many developers only look at security as an afterthought tacked on toward the end of the software development lifecycle. However, by implementing security at the end of each cycle, delays in go-to-market are ultimately created while correcting security vulnerabilities. Organizations looking to strengthen the security of their cloud applications and improve lifecycle turnaround would do well to implement Coalfire's application security solutions.

CyberGRX

https://www.cybergrx.com

Moscone South Expo Booth 3424
Third-Party Cyber-Risk Management

Solution Name(s):
CyberGRX Exchange

CyberGRX standardizes third-party cyber-risk management, making it possible to gain insights, prioritize risks, and make smarter decisions across your entire vendor ecosystem. Driven by sophisticated data analytics and automation, real-world attack scenarios, and real-time threat intelligence, CyberGRX provides customers with comprehensive and ongoing analysis of their vendor portfolio. Third-party organizations can effectively manage their cyber-risk reputation by proactively utilizing the CyberGRX Exchange to complete and share a single assessment with multiple upstream customers.

What Sets Them Apart:

Where competitors offer limited visibility, outside-in scanning, and "exchange" capability with only data gathering and storage capabilities, the Exchange has the largest standardized database of company cyber-risk profiles available. With Predictive Risk Insights, CyberGRX has the ability to provide cybersecurity reputation data on almost any company in the world. CyberGRX provides customers with threat profiles for high-value vulnerabilities in order to deliver real-time insights around recent cyber events to help quickly identify potential risks and prioritize follow-up activities.

One More Thing:

We wrote the book on third-party cyber-risk management. Attendees can get a free copy of Third-Party Cyber Risk for Dummies at our booth. This guide helps define how to build an effective TPCRM program, focusing on an evolution from collection of current static assessment to data-driven decisions and near-real time cyber-risk intelligence to reduce third-party risk.

The EMA Perspective:

With over 80% of the top 500 companies requested by customers already on its Exchange, such as Google, AWS, ADP, Cisco, and Iron Mountain, CyberGRX allows companies to have unmatched depth and breadth of actionable cyber-risk data. 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.

F5

Moscone North Expo Booth 5771
Application Security, Fraud & Risk

Solution Name(s):
F5 Distributed Cloud WAAP

F5 is a multi-cloud application security and delivery company that enables our customers—which include the world's largest enterprises, financial institutions, service providers, and governments—to bring extraordinary digital experiences to life.

What Sets Them Apart:

F5 gives the world's largest businesses, service providers, governments, and consumer brands the freedom to securely deliver every app, anywhere—with confidence. F5 delivers cloud and security application services that enable organizations to embrace the infrastructure they choose without sacrificing speed, control, and secure experiences.

One More Thing:

F5 is an established, trusted brand that has protected many of the world's leading brands and the communities they serve for 20+ years. F5's transformation from a hardware vendor to a software and SaaS provider is well underway with the launch of F5 Distributed Cloud Services: a SaaS-enabled platform of services for networking, security, performance, and edge compute built for modern distributed applications and workloads.

VENDOR VISION 2022

PRESENTED BY **EMA**

The EMA Perspective:

Organizations want a complete security solution, one that is easy to integrate into their existing environment, works with their existing tools, and will be easy to manage. Most 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 has 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.

Horizon3.ai

https://www.horizon3.ai/

Moscone North Expo Booth 4402
Network Security

HORIZON3.ai

VENDOR VISION 2022
PRESENTED BY **EMA**™

Solution Name(s): NodeZero

Horizon3.ai's mission is to help you find and fix attack vectors before attackers can exploit them. NodeZero, our autonomous penetration testing solution, enables organizations to continuously assess the security posture of their enterprise, including external, identity, on-prem, IoT, and cloud attack surfaces. Like APTs, ransomware, and other threat actors, our algorithms discover and fingerprint your attack surface, identifying the ways exploitable vulnerabilities, misconfigurations, harvested credentials, and dangerous product defaults can be chained together to facilitate a compromise. NodeZero is a true self-service SaaS offering that is safe to run in production and requires no persistent or credentialed agents.

What Sets Them Apart:

NodeZero is an on-demand, self-service SaaS platform that is safe to run in production and requires no persistent or credentialed agents. Our initial product focus is to give IT administrators and network engineers "security superpowers," enabling them to continuously assess their enterprise's security and compliance posture with the skills of a 20-year pen testing veteran at a fraction of the cost and effort.

One More Thing:

The future of cyber-warfare will run at machine speed – algorithm vs. algorithm – with humans by exception. It is time for organizations to approach network security with a wartime mindset, adopting a layered defense model, with purple teams in place that "train like they fight."

The EMA Perspective:

Sometimes, the best way to analyze the security of your organization is through the eyes of potential attackers. While traditional penetration testing can often be time-consuming and potentially disruptive, Horizon3.ai's approach to continuous penetration testing through APTaaS™ allows security practitioners to spend more time securing their network and less time analyzing it. Organizations that want to enhance their attack surface visibility while decreasing security team workload would do well to implement a solution like Horizon3.ai's NodeZero.

IBM

https://www.ibm.com/security

Moscone North Expo Booth 5759
Threat, SOAR, Data Security, Identity & Access
Management, Fraud, Security Services

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

We put security everywhere so your business can thrive anywhere. IBM Security works with you to help protect your business with an advanced and integrated portfolio of enterprise security products and services, infused with AI and a modern approach to your security strategy using Zero Trust principles, helping you thrive in the face of uncertainty. By aligning your security strategy to your business; integrating solutions designed to protect your digital users, assets, and data; and deploying technology to manage your defenses against growing threats, we help you manage and govern risk that supports today's hybrid cloud environments.

What Sets Them Apart:

Our breadth, depth, and integrated services offering.

One More Thing:

An IBM Zero Trust security strategy can help organizations increase their cyber-resiliency and manage the risks of a disconnected business environment while still allowing users access to the appropriate resources. It's a model that uses context to securely connect the right users to the right data at the right time under the right conditions while protecting your organization from cyber-threats. Integrating cloud into your existing enterprise security program is not just about adding a few more controls or point solutions. IBM Security® products and experts can help you integrate the appropriate controls, orchestrate workload deployment, and establish effective threat management.

The EMA Perspective:

Data privacy and security are hot topics in the security industry right now, second only to the buzz around Zero Trust. Many organizations have started to integrate data security as part of their overall security strategy, and vendors are catching up with how best to address the needs of their customers. Still, they don't want just any vendor. They are looking for leaders in the Zero Trust space, preferably a leader with a complete Zero Trust and data security solution. IBM is that leader: a proven leader in Zero Trust with data security solutions that are unmatched in the industry. With their multiple security offerings and solutions, organizations can literally transform their security strategy by partnering with the experts at IBM.

Infosec Institute

https://www.infosecinstitute.com
Moscone South Expo Booth 3324
Security Education and Skills Development

INFOSEC™

Solution Name(s):
Infosec Skills
Infosec IQ

Infosec's mission is to equip all organizations and individuals with the know-how and confidence to outsmart cyber-crime. As a leading cyber-security education provider, we help IT and security professionals advance their careers with skills development and certifications while empowering all employees with security awareness and privacy training to be cyber-safe at work and home. In 2021, Infosec helped millions of learners make the digital world safer by delivering 26 million minutes (49 years' worth!) of cybersecurity training. More than 70% of the Fortune 500 have relied on Infosec Skills to develop their security talent and teams, and more than 5 million learners worldwide are more cyber-resilient from Infosec IQ's security awareness and phishing training.

What Sets Them Apart:

The most successful security training and awareness programs—the ones that build proactive cyber-alert cultures—deliver the right training to the right people at the right time. While other solutions focus on technology, Infosec is helping businesses and organizations strengthen their security posture, reduce risk, and meet compliance by providing hands-on cyber-education for every role.

One More Thing:

The industry's need for hands-on, role-based security training is evident. This year, cyber-crime is estimated to be responsible for $6 trillion worth of damage to the global economy—a number expected to grow to $10.5 trillion by 2025. Infosec Institute works to fill that industry need through Infosec Skills and Infosec IQ.

VENDOR VISION 2022

PRESENTED BY **EMA**™

The EMA Perspective:

The human element has always been considered the weakest link in cybersecurity. While other vendors focus on augmenting the human element through technology, Infosec Institute seeks to strengthen the historically "weak link" and turn it into the strongest. Just like in education, security training is never "one size fits all" and needs to be custom-tailored toward an individual's roles and responsibilities. By combining security awareness training with workforce development, organizations can not only create a more resilient workforce, but also develop information security practitioners from within. Organizations looking to revolutionize and build their security culture would do well to adopt a solution like Infosec Institute.

Lumu

https://lumu.io/

Moscone North Expo Booth 4315
Network Detection and Response, SOC Operations

Solution Name(s):
Lumu Free, Lumu Insights, Lumu Defender

Founded on the belief that all companies, regardless of their size or vertical, can operate cybersecurity proficiently, Lumu is focused on helping organizations illuminate threats and isolate confirmed instances of compromise. Applying principles of continuous compromise assessment, Lumu has built a powerful closed-loop, self-learning solution that helps security teams accelerate compromise detection, gain real-time visibility across their infrastructure, and close the breach detection gap from months to minutes.

What Sets Them Apart:

- Comprehensive cybersecurity operation at any level
- Extensive network metadata sources
- Response automation capabilities for any existing security stack
- Ease of deployment and quick time to value
- Actionable intelligence for automated response purposes

One More Thing:

Lumu offers cybersecurity to organizations regardless of their size or vertical. We have differentiated solutions that meet the needs of different industries. Lumu provides rich incident context, helping organizations identify if there was malicious activity across their network, which IoC it's associated with, when it happened, which devices were affected, and information on the automated attack response efforts.

The EMA Perspective:

Lumu founder and CEO Ricardo Villadiego finds unsolved problems and assembles a team to tackle that problem simply and directly: that is the approach he takes with Lumu. Lumu never claims (nor does it try) to solve all of your security problems. Instead, it does what it does: finds where you have significant security vulnerabilities and makes recommendations on how best to solve them. As an industry, security vendors need to continue to improve their efforts to educate their users—how security works, why things are a risk, and how best to solve those problems. Lumu does this and does it in ways that security practitioners and executives can understand and utilize.

Yubico

Moscone South Expo Booth 3300
Identity and Access Management

yubico

Solution Name(s):
FIDO2

Yubico, the inventor of the YubiKey, makes secure login easy and available for everyone. Since the company was founded in 2007, it has been a leader in setting global standards for secure access to computers, mobile devices, servers, browsers, and internet accounts. Yubico is a creator and core contributor to the FIDO2, WebAuthn, and FIDO Universal 2nd Factor (U2F) open authentication standards and is a pioneer in delivering modern, hardware-based authentication security at scale. Yubico's technology enables secure authentication, encryption, and code signing and is used and loved by many of the world's largest organizations and millions of customers in more than 160 countries.

What Sets Them Apart:

Yubico is the core inventor and contributor to new open authentication standards—FIDO U2F, FIDO2, and WebAuthn—that are supported by many leading browsers, operating systems, and services. As a result, other vendors have produced security keys that support these same open standards, including Google Titan. YubiKeys are the only multi-protocol security keys that support six different authentication standards on one device and accommodates legacy systems while enabling modern authentication.

One More Thing:

Since they were founded, Yubico has remained steadfast in its simple yet powerful mission: to make the internet safer for everyone by making logins secure, easy, and available for all. Today, the YubiKey is used by millions of people in over 160 countries and is loved by leading internet companies including Google and Facebook.

VENDOR VISION 2022

PRESENTED BY **EMA**

The EMA Perspective:

As the security industry moves away from password authentication and focuses on multifactor authentication and Zero Trust, the industry must adopt new authentication methods. These methods must be reliable, secure, and efficient. Yubico is not only a thought leader in the identity and access management space, but is setting the industry standard for authentication protocols and methods. Organizations looking to enhance their identity and access management security with phishing-resistant MFA tools would do well to look further at Yubico's solutions and authentication protocol standards.

Honorable Mentions

Banyan Security	Zero Trust Network Access (ZTNA)	South Expo Booth 2058
Digital Guardian	Enterprise Data Protection	South Expo Booth 0927
GlobalSign	Public Key Infrastructure (PKI)	South Expo Booth 3224
Juniper	Network Security/SASE	North Expo Booth 6071
Noetic Cyber	Cyber Asset Management	ESE South Level ESE 05
Onapsis	Business-Critical Application Security	North Expo Booth 4434
Ordr	Cyber Attack Surface Management	North Expo Booth 4304
Perimeter81	Zero Trust Network Access (ZTNA)	South Expo Booth 1849
Procilon	Identity Management	North Expo Booth 5671
Ridge Security	Offensive Security	North Expo Booth 4218
Salt Security	API Security	South Expo Booth 1835
Security Compass	Risk Assessment & Threat Modeling	North Expo Booth 4600
ThreatX	Web Application & API Security	South Expo Booth 3205
Torq	Automation & Orchestration	North Expo Booth 4404
Wabbi	Application Security	North Expo Booth 4503
XMCyber	Attack Surface & Vuln Management	North Expo Booth 4328