TAG Cyber

SecurityAnnual

2ND QUARTER 2021

MARKET OUTLOOK & INDUSTRY INSIGHTS

WELCOME TO THE 2021 TAG CYBER SECURITY ANNUAL – 2ND QUARTER EDITION

We are pleased to offer our peers, customers, colleagues, and friends in the cyber security community this volume of original articles, analyst reports, and yes – more original cartoons. The goal of our Quarterly is to inform, challenge, and entertain our readers. We hope you find the cyber security material helpful in your day-to-day work as practitioners, managers, vendors, educators, researchers, government officials, and investors.

While it's only been a few months since the publication of our first Quarterly, we see many changes in the cyber security community and even more broadly in the business world. While the Q2 2020 ushered in some dramatic changes in business operations and working environments, Q2 2021 is continuing many of those changes while introducing yet another challenge: hybrid working environments.

Why is this such a big deal for cyber security?

In the rush to accommodate a mass exodus from the office to work-from-home, security teams made concessions—at first—to grant access to home and remote workers, allowing them to do their jobs as well and as easily as possible. Baselines were then established (albeit ones that were abnormal) to understand new work-from-home habits, devices, and access needs. For nearly a year, the abnormal became the norm.

And during this time, executives saw that this flexible work environment was good for many more people than expected. It benefitted workers and businesses, alike. Now, then, as we see the light at the end of the pandemic tunnel, businesses are strategizing on their new operating plans, looking to incorporate more flexible options for a greater percentage of their workforce.

But the constant, continuous change precipitated by the allowance of both work-from-home and remote work introduces new security challenges. The mixed use of personal and work devices for work purposes, unmanaged devices touching corporate resources, perpetually shifting user locations and thus use of various connectivity options, and more all lead to the need for fine-grained control of access rights, highly-tuned behavioral monitoring, hardened data and application protection, increased device hygiene, improved cloud configuration management, and on and on the list goes.

Cyber security has never been for the faint of heart, nor the complacent. But in 2021, we have to work through myriad, fast-moving challenges at once, without dropping the ball on security while supporting a hybrid work environment that allows employees, contractors, and partners to work seamlessly, wherever and however they need or want to work.

And of course cyber attackers know that security defenders' attentions and resources are spread thin. The SolarWinds attack and its ongoing, far-reaching repercussions continue as we write this second quarter Quarterly. Microsoft experienced a severe attack against its Exchange server, impacting thousands of customers. Molson Coors was shut down temporarily after a cyber attack. Buffalo, New York public schools suffered the same fate. A water treatment plant in Florida was compromised due to a remote access vulnerability and the attacker was able to temporarily (and fortunately minimally) adjust the amount of lye added to the water. IBM Security reports a near-50% increase in attacks against vulnerabilities in industrial control systems over the past year. And more concerning attacks and incidents will occur between this writing and its publication in a month.

Continued

INTRODUCTION

Continued

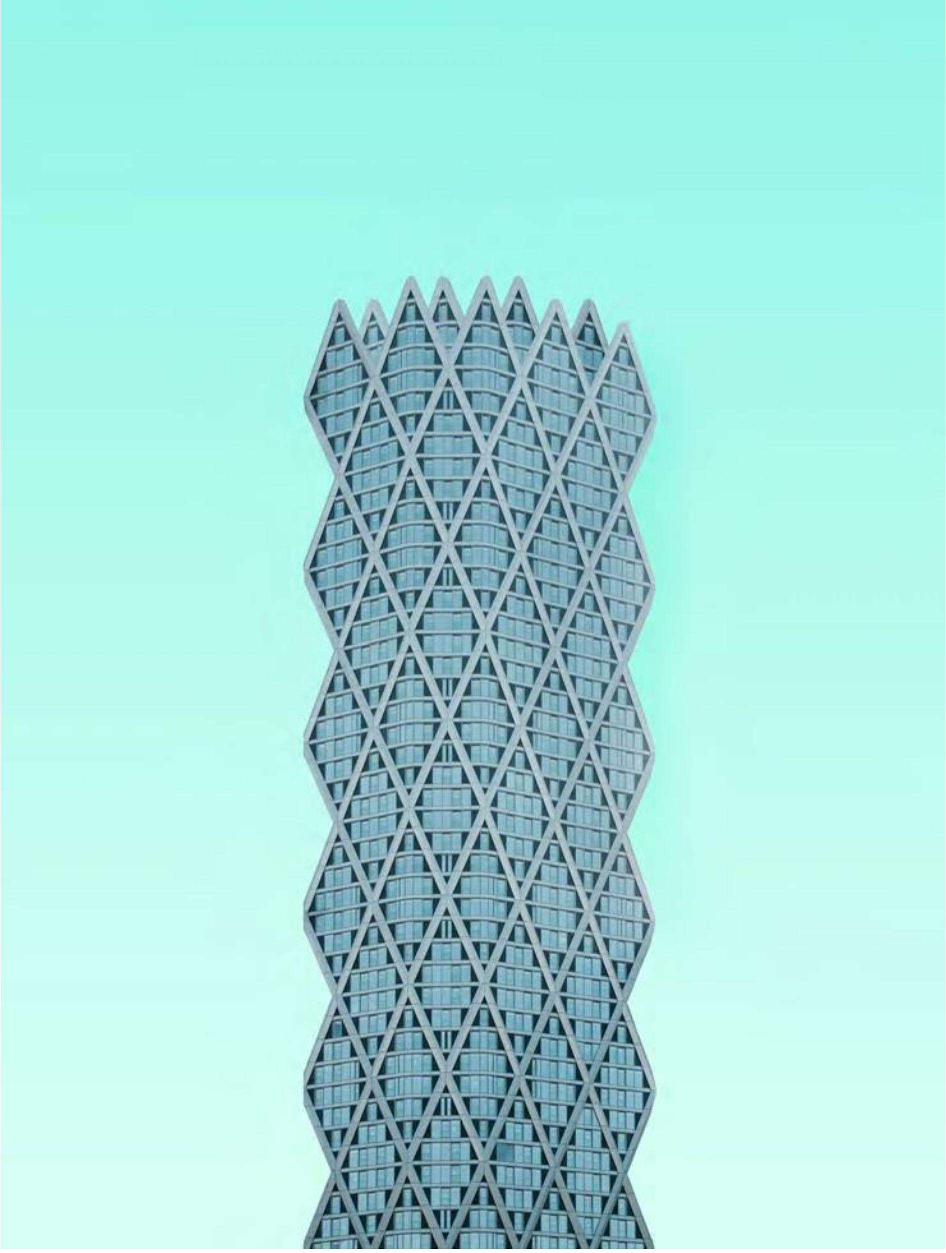
Enterprise security teams understand the scope of the problem and are now working on strategies and adopting technologies that can handle modern threats. Zero trust principles and data- and application-centric approaches are being adopted at the world's leading organizations, and vendors are rising to the challenges. But the road is long and there's much work still to do.

We at TAG Cyber are working furiously with enterprises and vendors to connect needs and capabilities, and we know we're only a fraction of the puzzle. We're expanding our research services via a new research subscription that provides deeper insights and more detailed information, especially on commercial vendors—large and small, paying customers and not—for enterprises, and we're building a portfolio management tool for enterprise to better streamline their investments in security technology.

In this Q2 2021 Quarterly, you'll see TAG Cyber's continued commitment to frank, honest, and unbiased research about our industry. We hope you find some inspiration in the articles and reports, and we promise to continue pushing ourselves to provide guidance that is practical and useful.

We also encourage you to reach out; we wouldn't fulfill our promise of democratizing cyber security research if we weren't open to conversations with enterprises and vendors, regardless of their contractual status. We know you, the practitioners, have great insights that we don't always experience firsthand anymore, and we welcome your thoughts and ideas.

For now, enjoy the second edition of the TAG Cyber Quarterly. Read, learn, and laugh (at our cartoons), then go forth and secure!



FEATURED PHOTOGRAPER
Simone Hutsch / Unsplash

- LEAD AUTHORS – Ed Amoroso, Katie Teitler
- RESEARCH AND CONTENT – Adam LeWinter , David Hechler, Shawn Hopkins, Liam Baglivo, Stan Quintana, Andy McCool, Jennifer Bayuk, Matt Amoroso
- MEDIA AND DESIGN – Lester Goodman, Miles McDonald, Rich Powell

TAG Cyber LLC
P.O. Box 260, Sparta, New Jersey 07871

This publication may be freely reproduced, freely quoted, freely distributed, or freely transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system without need to request permission from the publisher, so long as the content is neither changed nor attributed to a different source.

Security experts and practitioners must recognize that best practices, technologies, and information about the cyber security industry and its participants will always be changing. Such experts and practitioners must therefore rely on their experience, expertise, and knowledge with respect to interpretation and application of the opinions, information, advice, and recommendations contained and described herein.

Neither the authors of this document nor TAG Cyber LLC assume any liability for any injury and/or damage to persons or organizations as a matter of products liability, negligence or otherwise, or from any use or operation of any products, vendors, methods, instructions, recommendations, or ideas contained in any aspect of the 2021 TAG Cyber Security Annual volumes.

The opinions, information, advice, and recommendations expressed in this publication are not representations of fact, and are subject to change without notice. TAG Cyber LLC reserves the right to change its policies or explanations of its policies at any time without notice.

The opinions expressed in this document are that of the TAG Cyber Analysts, and in no way reflect that of its Distinguished Vendors.

April 15, 2021

TAG Cyber

SecurityAnnual

2ND QUARTER 2021

CONTENTS

5 STEPS TO TURN YOUR MSP INTO AN MSSP

KATIE TEITLER

Managed service providers (MSPs) serve a critical function for businesses worldwide. With an estimated market size around the USD$200 billion mark,[i] there is an obvious need for outsourced IT and operations support. More and more, however, companies cannot decouple security from IT, hence, the existence of managed security service providers (MSSPs). It's fair to say that a business could not use an MSSP without either running its own internal IT department or through partnership with an MSP. The reverse, however, is not true. Any business can have an IT function without a security function.

For the record, this is not recommended.

Clear bias aside, cyber security is intimately intermingled with all digital use and has become a top-line business priority for many organizations. A breach could bring devastating impacts to revenue, customer retention, future growth, reputation, and more. For this reason, many MSPs partner with MSSPs to offer customers the option of enhanced and dedicated security services. Yet, the estimated MSSP market valuation is ~USD$30 billion,[ii] just a small fraction of the greater MSP market.

Why? Are companies, in particular, small and medium-sized businesses, just not deploying security technology? In some cases, the answer is yes. What we've found in our work with these smaller businesses via our Cyber Corps service is that it's easy for them to be overwhelmed with the idea of adding security. They know it's an important business decision, but they neither have the time nor internal resources to evaluate what they need. Oftentimes they rely on their MSP to make security recommendations, then they fear the cost of implementation and are thus stuck in a cycle of analysis paralysis.

Part of the problem is the business model; MSPs often rely on external MSSPs to deliver security expertise. This means that the MSP contracts with the MSSP on its own accord, offers security as a value-add to its customers, and passes along a cost plus a markup to the end customer. As a result, the customer pays a higher price for security services, but contracting on their own could be confusing,

THE OPPORTUNITY FOR ENHANCED SERVICES AND INCREASED REVENUE ISATTRACTIVE TO THE MSP, AND IT BENEFITS THE END USER MARKET IN A VERY POSITIVE WAY.

plus there is no guarantee that their MSP would be able to integrate with whichever MSSP they choose. It's a circumlocutive cycle that hurts smaller businesses.

Partnering with a standalone MSSP is often not the answer, either, because most MSSPs have built their practice around the accepted current model and don't or won't offer some of the more basic IT functionality needed by these smaller businesses. It is easier, however, for an MSP to transform itself into a full MSSP, complete with basic IT services, by adding in-house capability. Over the last few years, we've at TAG Cyber have seen this transformation occur within a not-insignificant segment of the market. The opportunity for enhanced services and increased revenue is attractive to the MSP, and it benefits the end user market in a very positive way.

Enterprising MSPs that want to take advantage of the need and opportunity can start with a few basic steps.

1. Strategy: Unless your business is flush with capital (and kudos to you if it is) it will be impossible to incorporate full lifecycle security into your offerings immediately. Start by taking stock of what services you offer now, who your clients are, if there is a common thread to their security needs—e.g., they're all missing endpoint security or data protection—and how you can build or buy those capabilities first.

2. Technology: Select the technology or capability you want to offer, then determine if its preferable to build, buy, or borrow (i.e., have a partnership agreement with a provider). Think carefully about the cost implications of each choice and the long-term impact on your business. While partnership agreements may be the easiest to execute, you will pay a higher price, and therefore have to charge a higher price, than if the technology is in-house.

3. Staffing and Training: How will you accommodate 24x7x365 technical support (and potentially response capabilities when a security incident is discovered)? Can you hire and train enough security experts? Can you provide the ongoing skills advancement needed to keep pace with security demands? If the decision is to use third-party technology in your MSSP, how/when will the vendor supply training, for deployment as well as upgrades/updates?

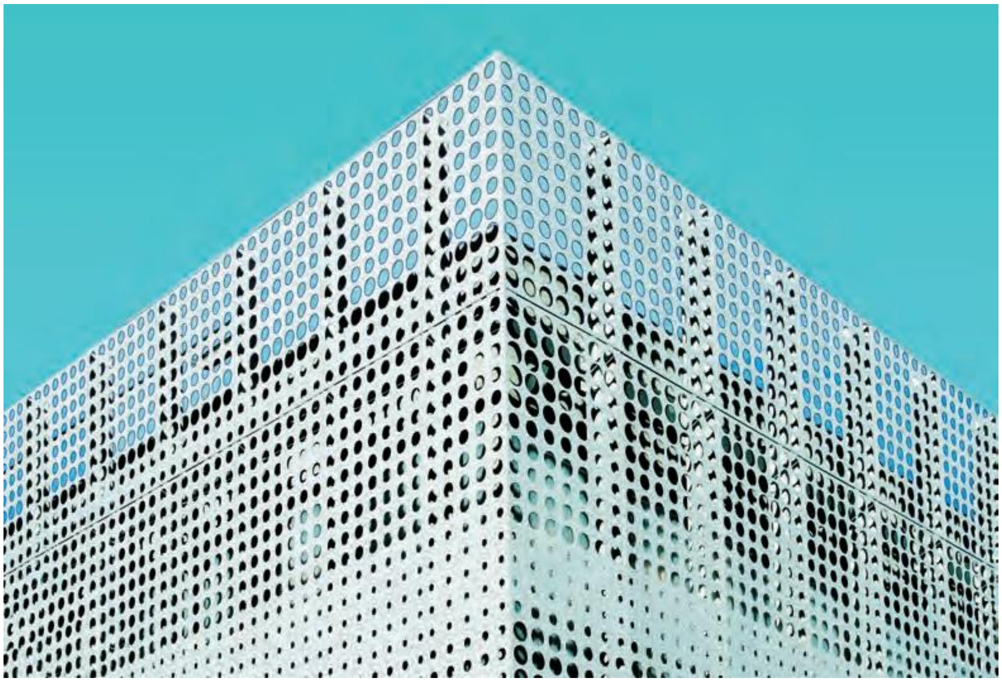
"I thought we could use some cyber expertise on our board."

4. Integrations: There is no doubt that some overlap exists between traditional IT and security technology. Today, many tools integrate via API, thus allowing operations staff simpler management and visibility. However, some legacy tools are harder to integrate, and some tech ecosystems just don't work well with others. Make sure that whatever tech you use, you aren't grappling with multiple, disparate systems and data streams, increasing the burden on your workforce and thus ratcheting up the potential forerror.

5. Pricing: One of the biggest advantages of the service provider model is economy of scale. The ability to use a centralized set of technology and staff across multiple customers allows for competitive pricing, but the tendency is to charge a premium for the security expertise brought to the table. Consider your target market before pricing your service out of reach. There is nothing wrong with charging premiums for expert-level work, but if the idea is to support smaller businesses, realize that the reason they're not already running a security program and security tools is because it's unaffordable to do so.

In short, upgrading your MSP to an MSSP is a great business opportunity. However, doing so requires more than just buying some new technology, deploying it, and offering it to existing customers. Develop a strategic, step-by-step plan, based on the needs of your current customers (and likely many others) that will help you grow, expand, and provide the necessary security capability so many businesses are lacking today.

i bit.ly/3bZ0ouK
ii bit.ly/3qU4zMM



AN INTERVIEW WITH CANDID WUEST, VP OF CYBER PROTECTION RESEARCH, ACRONIS

A HOLISTIC APPROACH TO INFRASTRUCTURE, DATA, AND DEVICE CYBER PROTECTION

The Holy Grail of cyber security is full lifecycle management. Workloads must be protected from the instant a user or system is connected, a piece of data is created, or a new tool is made operational, all the way through to data destruction or removal and instances when a compromise or breach occurs.

Most enterprises use disparate tools, techniques, and processes for each lifecycle stage. It's why there's an abundance of security vendor technologies available on the commercial market. And vendors have gotten savvy; most recognize the requirement for inter-technology compatibility. Thus, even if a vendor builds and sells a capability to address only one lifecycle stage, it often integrates with other best-of-breed technologies to give customers holistic visibility, orchestration, and governance.

Acronis, a well-known data backup and recovery provider, has pivoted on their strategy and technology. We recently spoke with Candid Wuest, VP of Cyber Protection Research at Acronis, about the philosophy of cyber protection and how it enables businesses to comprehensively protect their data and systems.

TAG Cyber: Traditionally, data protection and backup were separate and distinct IT functions from cyber security. Why is this an outdated approach?

ACRONIS: Cyber threats have evolved over the past few years and will continue to do so into the future. We've seen that attackers are combining different methods to compromise machines, steal data, or otherwise disrupt businesses. It is therefore vital to take a holistic approach to protection, one that can cover the whole organization—infrastructure, devices, and data—in all situations. For example, imagine a targeted ransomware attack, which nowadays often tries to delete existing backups as well as steal sensitive information before encrypting critical workloads or files. To protect against such a multi-pronged attack, you need to break the silos of backup and cyber security. For ransomware attacks, this means you need to protect the backups from tampering in order to ensure that you can recover a clean copy, should there be a compromise.

TAG Cyber: Why and how did Acronis decide to expand the range of products and services you offer?

ACRONIS: Over five years ago, Acronis began observing more and more of our customers suffering from sophisticated ransomware attacks, destroying their backups and fast recovery capabilities. On this premise, Acronis developed a threat-agnostic data protection technology called Active Protection, which monitors any data interaction on a system and uses artificial intelligence to separate legitimate activities from malicious ones. Since Acronis has granular data backups, we can restore

With some of these attacks yielding millions of dollars in ransom, there’s no reason for threat actors to stop.

damaged or encrypted data in the event of a compromise. All of this functionality is provided from within a single agent, allowing the system to automatically restore without the need for user interaction. For example, if a previously unknown ransomware variant manages to encrypt a handful of files, the heuristic will automatically detect this tampering, stop the process, and restore any modified files.

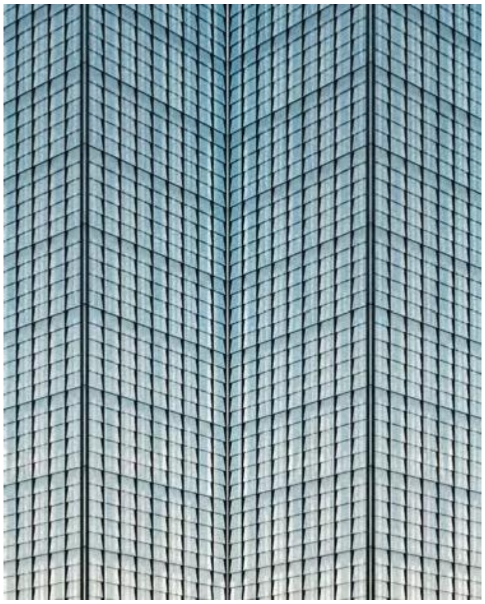
TAG Cyber: Why is Acronis’ legacy as a backup and recovery provider an important underpinning of Acronis Cyber Protect, your new solution?

ACRONIS: Building on the success of the integrated Active Protection and backup, Acronis decided that an adequate cyber protection solution needs to be built across even more domains. For example, it’s important to address the five vectors of cyber protection—availability, accessibility, privacy, authenticity, and security (SAPAS)—which cover the full lifecycle of data. This is why Acronis integrated backup and a full next-generation security solution into a single agent, which has become Acronis Cyber Protect. This includes cloud-based reputation, signature-based antivirus, and AI-based pre-execution scanning. On top of this, the behavior of every running process is analyzed in real time, allowing cyber analysts to react to unknown threats at any stage. In addition, URL filtering prevents users from reaching malicious websites such as phishing websites, minimizing the risk of further attacks.

To cover all five stages of the NIST cybersecurity framework, the Acronis Cyber Protect solution also includes vulnerability assessment, patch management, and exploit prevention functionalities, which help prevent attacks from succeeding in the first place. At the other end of the NIST framework, in the “recover” phase, our forensic data backups allow a thorough root-cause analysis that provides richer data than traditional EDR.

TAG Cyber: What are some of the bigger or more recent threat trends you’re seeing?

ACRONIS: One of the biggest threats against organizations of all sizes is targeted ransomware. Modern ransomware attacks not only encrypt data, but also steal sensitive information and disrupt business operations with distributed denial of service (DDoS) attacks. These attacks will continue to grow in number—cyber criminals are increasingly automating their attacks and even starting to use AI to increase their success rate. With some of these attacks yielding millions of dollars in ransom, there’s no reason for threat actors to stop. This means that there is a need for integrated and automated solutions that can handle the full scope of these attacks.



Another threat that has increased drastically during the COVID-19 pandemic is phishing attacks, leading to a rise in compromised credentials. In February 2021 alone, we observed over 700,000 malicious requests. User awareness training programs can be as good as they come, but they are never 100% effective; there will always be at least one user who clicks on an enticing or confusing link, and therefore enterprises need a technical solution to protect against phishing.

TAG Cyber: What types of clients are onboarding to Acronis Cyber Protect?

ACRONIS: There are two answers to this question. First, Acronis' go-to-market strategy is primarily channel-focused, enabling service providers of all sizes and types (MSPs, telcos, hosting companies, etc.) to offer cyber protection services to their end customers. We have an existing partner network of over 50,000 channel partners worldwide, and we're encouraging them to build new cyber protection services by leveraging our Acronis Cyber Protect Cloud platform. Installed via one agent and managed through one central console, our service provider platform integrates cyber security, data protection, and endpoint management in a single solution that protects endpoints, systems, and data. The essential capabilities include full-image and file-level backup and recovery for workloads on more than 20 platforms; an advanced AI-based behavioral detection engine that stops malware, ransomware, and zero-day attacks on client endpoints; and centralized management that integrates with remote monitoring and management and professional services automation systems.

Vulnerability assessments, file sync and share, blockchain-based notarization, and disaster recovery are also included and available as add-ons.

Our second (but equally important) target market is the ultimate end user. Service providers primarily cater to the small and medium business (SMB) market. SMBs generally do not have the resources or expertise to handle their basic IT environments, let alone triage cyber threats, so they rely quite heavily on service providers to do this for them. Ultimately, Acronis' solutions are being consumed primarily by SMBs but they are being delivered by service providers.

TAG CYBER

DISTINGUISHED VENDORS

2Q 2021

Working with cyber security vendors is our passion. It's what we do every day. Following is a list of the Distinguished Vendors we've worked with this past three months. They are the cream of the crop in their area – and we can vouch for their expertise. While we never create quadrants or waves that rank and sort vendors (which is ridiculous), we are 100% eager to celebrate good technology and solutions when we find them. And the vendors below certainly have met that criteria.

1KOSMOS BlockID

1Kosmos offers next-gen passwordless authentication digital identity proofing with advanced biometrics. The company's innovative approach leverages blockchain, and provides a mobile app experience that allows businesses to verify employee and customer identity without the typical friction or vulnerability of traditional authentication.

accurics™

Accurics enables self-healing cloud native infrastructure by codifying security throughout the software development lifecycle. The company's products programmatically detect, monitor, and mitigate risks in Infrastructure as Code to reduce customers' attack surfaces and prevent cloud posture drift before infrastructure is provisioned.

Acronis

Acronis Cyber Protect helps businesses integrate cyber security, data protection, endpoint management, and backup and recovery to prevent breaches and ransomware. Acronis offers a one agent, one management interface platform, making cyber protection across your infrastructure and endpoints easy and effective.

AGARI©

Through applied science, the Agari Identity Graph™ delivers business context to every email risk decision. Agari ensures outbound email from the enterprise cannot be spoofed, increasing deliverability and preserving brand integrity, and protects the workforce from devastating inbound BEC, VEC, spearphishing, and account takeover-based attacks.

TAG CYBER DISTINGUISHED VENDORS

2Q 2021

ATTACKIQ

AttackIQ, the leading vendor of breach and attack simulation solutions, built the first Security Optimization Platform for continuous security control validation. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyber defenses work as expected, aligned with the MITRE ATT&CK framework.

avanade

Avanade was founded as a joint venture between Microsoft Corporation and Accenture LLP. The company's solutions include artificial intelligence, business analytics, cloud, application services, digital transformation, modern workplace, security services, technology, and managed services. Avanade helps clients transform business and drive competitive advantage through digital innovation.

axis security

Axis Security simply and securely connects users to any application through one centrally managed service. The Axis Application Access Cloud replaces disparate and complicated secure access technologies such as VPNs, VDI and inline cloud access security broker services using a single zero trust platform.

AXONIUS

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with nearly 300 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

Balbix®

Balbix was founded to help companies automate cyber security posture and reduce the ever-growing attack surface. The company's BreachControl™ platform uses proprietary algorithms to discover, prioritize, and mitigate unseen risks and vulnerabilities at high velocity, without infinite budgets or large, skilled security teams.

CLOUD RANGE

Cloud Range cyber range training allows SOC analysts and incident responders to test and improve attack detection, response, and remediation capabilities within a safe environment. With virtual access or on-site training, users prepare for hyper-realistic attacks against their network and infrastructure and become better defenders.

TAG CYBER DISTINGUISHED VENDORS

2Q 2021

CloudPassage

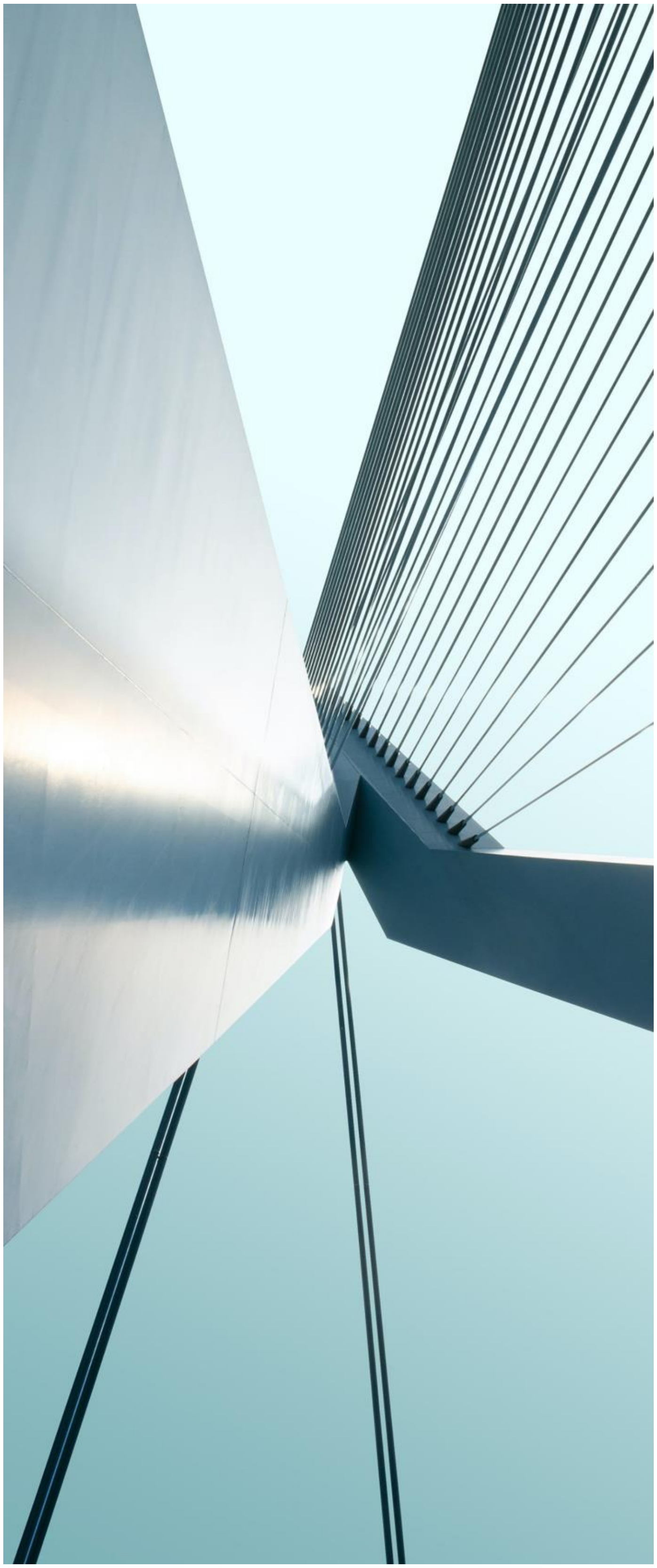
CloudPassage's Software-as-a-Service product is CloudPassage Halo, a unified cloud security platform that automates security and compliance controls across servers, containers, and IaaS resources in any public, private, hybrid, and multi-cloud environment. Halo's extensive automation capabilities streamline and accelerate.

Constella INTELLIGENCE

Constella Intelligence is a leading digital risk provider. Its solutions are powered by a combination of proprietary data, technology, and human expertise—including the largest breach data collection, with over 100 billion attributes and 45 billion curated identity records spanning 125 countries and 53 languages.

corelight

Corelight gives defenders unparalleled insight into networks to help protect the world's most critical organizations. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek, the widely-used network security technology.



TAG CYBER DISTINGUISHED VENDORS

2Q 2021

cybereason

Cybereason is the leader in future-ready attack protection. The company's Defense Platform unifies endpoint protection, security operations, security assessments, and threat hunting to help businesses outthink and outpace attackers. Cybereason is built to interrupt malicious operations, getting customers to mitigation and root cause analysis quicker.

eclypsium®

Eclypsium helps organizations manage and protect devices for their distributed workforce, data centers, and networks, down to the firmware and level. The Eclypsium platform provides security capabilities ranging from basic device health and patching at scale to protection from the most persistent and stealthiest threats.

endace

Endace's EndaceProbe Analytics Platform records a 100% accurate record of network activity, while simultaneously hosting third-party network security and performance solutions. The ability to integrate accurate network history into these solutions enables rapid investigation and resolution of network security and performance issues.

IBM

IBM Security is one of the largest security providers in the world. IBM's broad security portfolio includes a suite of capabilities across data, endpoints, identity and access, intelligence, and more. IBM security solutions let businesses "put security everywhere" and achieve zero trust across the enterprise.

INKY®

INKY prevents phishing using a unique method of computer vision and machine learning to stop attacks other email solutions can't see. The company's flagship product, INKY Phish Fence, uses proprietary techniques to block attacks before they reach user inboxes, avoiding costly compromises and financial loss.

HUMAN

Human is a cybersecurity company that protects enterprises and internet platforms from digital fraud and abuse. The company verifies 10 trillion+ interactions per week, protecting customers' sensitive data, reputation, compliance, bottom line and customer experience as they grow their digital business.

TAG CYBER DISTINGUISHED VENDORS

2021

kasada

Kasada provides the only online traffic integrity solution that accurately detects and defends against bot attacks across web, mobile and API channels. Kasada restores trust in the internet by foiling even the stealthiest cyber threats, from credential abuse to data scraping.

netskope

The Netskope security cloud provides unrivaled visibility and real-time data and threat protection when accessing cloud services, websites, and private apps. Netskope understands the cloud and delivers data-centric security, empowering organizations to balance security and speed and reimagine the perimeter.

NowSecure

NowSecure are the experts in mobile app security testing and services. Their platform provides comprehensive mobile app testing for security, compliance, and privacy risk vectors across 3rd party, custom, and business-critical mobile apps, with speed, accuracy, and efficiency.

OKERA

Okera provides secure data access and governance at scale. The Okera Dynamic Access Platform automatically defines, enforces, and audits data access policies at the fine-grained level using an intuitive zero-code interface. Okera ensures data privacy compliance and that the appropriate data access policies are configured.

prismo

Prismo Systems empowers enterprises to transform the way they secure users, assets, and applications with an active risk-based approach. The company's flagship product, the Prismo Transaction Graph, is a data lake purpose-built for security at enterprise scale, providing active cyber risk management.

SCYTHE

SCYTHE is an adversary emulation platform for enterprises and cyber security consultants. The company's platform allows red, blue, and purple teams to compile synthetic malware, test defenses against real-world adversarial campaigns, and assess their risk posture and cyber exposure across the enterprise.

TAG CYBER DISTINGUISHED VENDORS

2021

Security Risk Advisors (SRA) is a global consulting firm offering advisory services and a 24x7 CyberSOC. SRA's consultants provide specialty services that produce measurable security program improvement. Through a combination of strong technical acumen and strategic insight, SRA serves the Fortune 500 and Global 100.

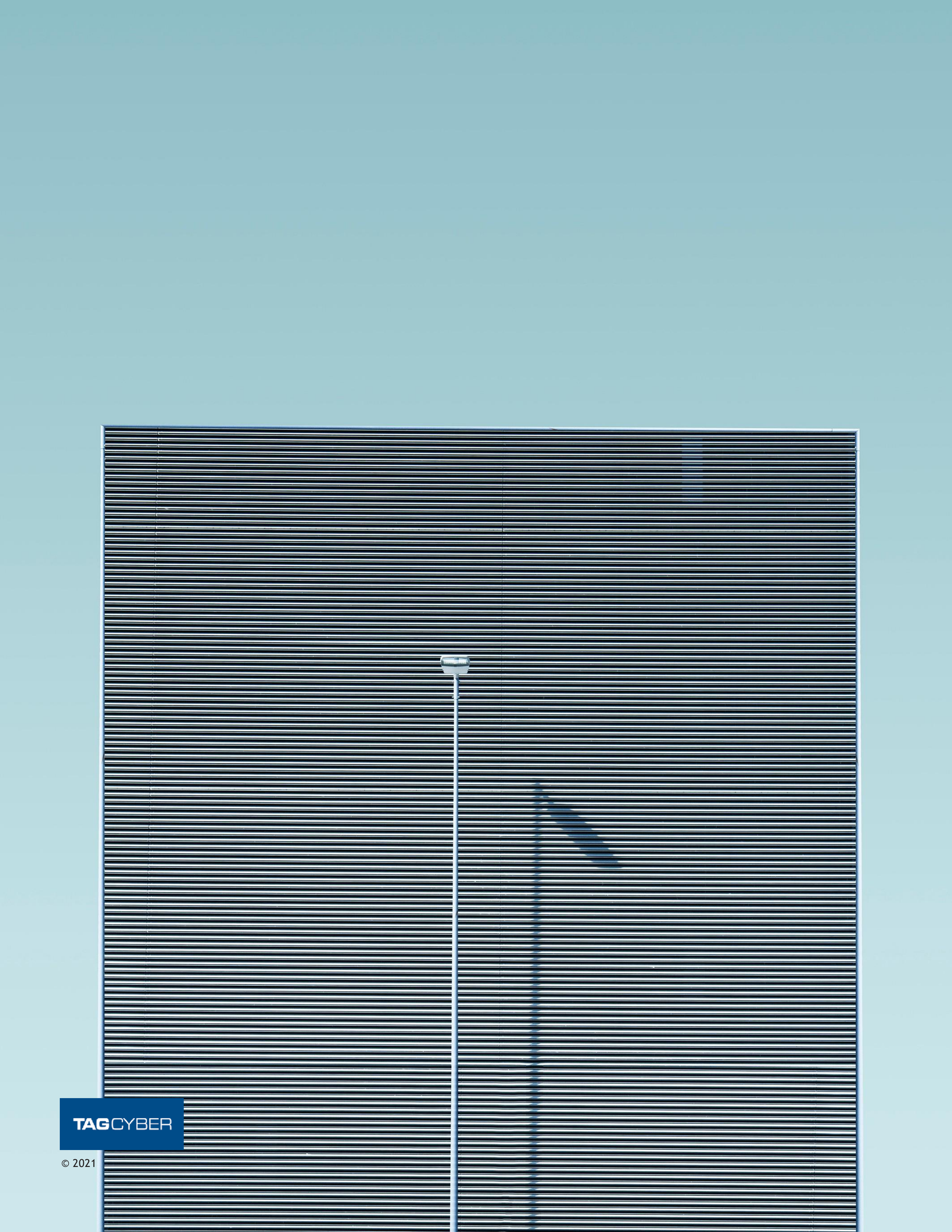
Semperis provides cyber preparedness, incident response, and disaster recovery solutions for enterprise directory services. Semperis' patented technology for Microsoft Active Directory protects over 40 million identities from cyberattacks, data breaches, and operational errors.

Sepio Systems offers the first hardware access control platform that provides visibility, control, and mitigation to zero trust, insider threat, BYOD, IT, OT, and IoT security programs. Sepio's hardware fingerprinting technology discovers all managed, unmanaged, and hidden devices that are invisible to other security tools.

ShardSecure offers total privacy, zero data sensitivity for data stored in the cloud or in on-prem environments. The company's proprietary Microshard™ technology shreds, mixes, and distributes data to eliminate its value on backend infrastructure, reducing the probability that attackers can exploit or steal sensitive data.

Siriux was founded to improve companies' SaaS deployments by identifying insecure or risky configurations that introduce unnecessary data and access exposure. Focused on the Microsoft Office product suite, Siriux offers quick scans and vulnerability assessments with tailored guidance for organizations' unique business requirements.

Trusona offers true passwordless multi-factor authentication, with a focus on digital identity. Trusona eliminates eight of the most common attack vectors—from credential stuffing to SIM swapping, phishing, and more—and uses biometric authentication and unique visual IDs to confirm users' identities without adding friction.



TAGCYBER