TAG
Security Annual
2024
SPECIAL REPRINT EDITION

AN OFFENSIVE APPROACH TO CONTINUOUS ATTACK SURFACE DISCOVERY

AN INTERVIEW WITH SEEMANT SEHGAL, FOUNDER & CEO, BREACHLOCK

THE STATES OF CYBERSECURITY

REDEFINING CYBERSECURITY:
FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY

TAG DISTINGUISHED VENDOR

breachlock

The need to reduce cyber risk has never been greater, and BreachLock has demonstrated excellence in this regard. The TAG analysts have selected BreachLock as a 2024 Distinguished Vendor, and such an award is based on merit. Enterprise teams using BreachLock's platform will experience world-class risk reduction—and nothing is more important in enterprise security today.

The Editors,
TAG Security Annual
www.tag-infosphere.com

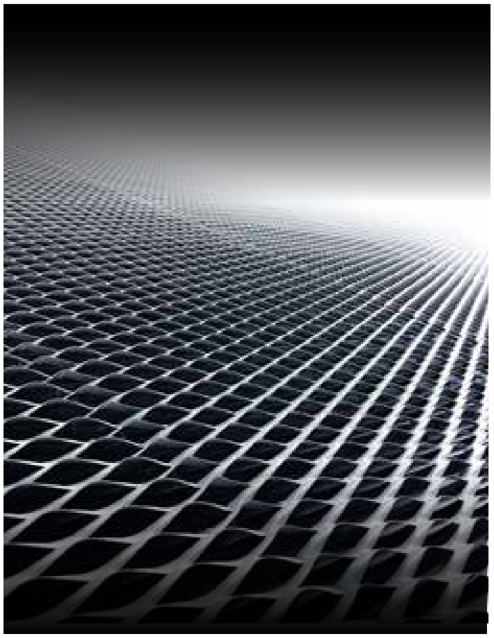
REPRINTED FROM THE TAG SECURITY ANNUAL

AN INTERVIEW WITH SEEMANT SEHGAL, FOUNDER & CEO, BREACHLOCK

AN OFFENSIVE APPROACH TO CONTINUOUS ATTACK SURFACE DISCOVERY

Enterprise security teams have come to understand the importance of continuously monitoring their attack surface before the next potential incident occurs. With an offensive security strategy for continuous attack surface discovery and penetration testing, BreachLock, a pioneering cybersecurity firm, offers a novel approach to protecting your threat landscape.

In this interview, we highlight BreachLock's unique methodologies, strategies, and experiences, offering insights into their offensive approach to identifying and mitigating potential vulnerabilities in an attack surface. Our goal is for readers to gain useful ideas on dealing with this increasing need to view exposed cyber assets.



TAG: Let’s start with you sharing a little about what led you to found BreachLock?

BREACHLOCK: After gaining experience at renowned global enterprises known for setting cybersecurity standards, I noticed a significant disparity in resource allocation between defensive and offensive security technologies. Upon analyzing the return on investment (ROI) from defensive versus offensive strategies, it became clear that offensive security consistently produced better results. For example, each penetration test identifies vulnerabilities and proactively addresses and closes potential entry points for hackers. So, I decided to delve into the reasons behind companies’relatively lower investment in penetration testing. Subsequent conversations ensued with multiple Chief Information Security Officers (CISOs) revealed an unmet need and gap in the market, with penetration testing methods proving inadequate for modern business requirements.

I identified four key shortcomings of traditional penetration testing: accuracy, agility, scalability, and cost-effectiveness. This stemmed from the fact that security tools operated on a point-in-time basis. Testing for vulnerabilities within systems was a singular event, typically conducted periodically or in response to impending audits or compliance requirements. The concept of continuous security was not yet conceived at that time. The existing offensive security landscape was driven by human intelligence only while the cyber criminals are far ahead of the game. They are using automated technology, and in some cases AI, to scrape the internet and find out who can bleed the most and the easiest. Now, this battle cannot be won without the use of technology.

That pivotal moment led me to dedicate myself to addressing these challenges, culminating in the establishment of BreachLock in 2019. My objective from the outset was to pioneer the world’s first full-stack Penetration Testing as a Service (PTaaS) solution, long before its widespread recognition or understanding. PTaaS was conceived to address the pressing demand for Offensive Security and a more continuous approach to safeguarding against an ever evolving and expanding attack surface.

Since its inception, BreachLock has undergone remarkable growth, significantly broadening our product portfolio and managed services to cater to the evolving needs of our clientele and the burgeoning market demand. Over the past five years, our client base has skyrocketed from under 100 to over 1000 across 30 countries with 100% YoY growth, marking an unprecedented trajectory. Our product suite has also evolved, now encompassing Application and Network Penetration Testing, API and Cloud

Our automated algorithms and supervised NLP-based AI models help to refine BreachLock's proprietary Pen Testing framework.

Penetration Testing, AI-driven Precision Pentesting, Attack Surface Management, and Red Teaming services.

TAG: What is it about BreachLock that has catapulted you from a PTaaS start-up to one of the global leaders in cybersecurity in a short span of five years? How have you managed your growth and success in such a short period of time?

BREACHLOCK: I think there are two key areas that are taken for granted by start-ups that ultimately make the difference to customers. That is the talent you hire and the customer service you provide.

In recent years, a recurring pattern has emerged within the cybersecurity sector: a succession of start-ups buoyed by investor enthusiasm who embarked on aggressive hiring sprees, often overcompensating employees to showcase rapid growth. This strategy, aimed at appeasing investors and projecting stability ultimately proved unsustainable. When investors clamored for substantial returns and consistent revenue growth, the unrealistic targets set forth by these companies culminated in inevitable staff reductions.

I had no desire to entangle my company in the complexities of managing millions in investor funds nor relinquishing the autonomy to steer it according to my vision. Consequently, I chose to bootstrap BreachLock during its inaugural year. Then came the unforeseen challenge of Covid in the following year, a period where I didn't even have the chance to meet my team face-to-face for the initial year and a half. Yet, amidst these obstacles, we surpassed the milestone of $1 million in revenue, witnessed expansion and growth, and this became part of our initial success story.

Our exceptional teams hail from diverse corners of the globe – the Netherlands, the U.K., Europe, India, and the United States – boasting unparalleled talent in the industry. Remarkably, our turnover rate remains below 5 percent, a rarity in today's landscape. Unlike many, BreachLock operates free from the constraints of heavy investment or the urgent demands of artificial growth strategies.

Secondly, our commitment extends to investment in innovative technology, sales, and customer service personnel. At BreachLock, we recognize the paramount importance of laying a robust foundation with our clients, dedicating ample time to establish clear, tangible metrics that truly reflect an organization's security performance. In today's landscape, clients seek more than just security solutions; they require the ability to articulate a genuine return on investment to their executives and boards.

So, our dedicated project managers immerse themselves in understanding the challenges of meeting both security and business needs within an organization, subsequently tailoring recommendations for the optimal tools and processes. Moreover, our customer service team sets an exemplary standard, consistently surpassing expectations to ensure seamless client onboarding, establishment of baselines and benchmarks, and implementation of regular business reviews. This unwavering commitment guarantees an unparalleled buying experience for our clientele.

Lastly, in 2023 there was a noticeable uptick as enterprises sought to overhaul their security strategies, gravitating towards a proactive and unified approach. They questioned the redundancy of paying for overlapping features and functionalities. Fast forward to 2024, and our response was clear: the launch of Attack Surface Discovery and Penetration Testing. We consolidated all our tools and services into a single, seamlessly integrated platform empowering enterprise with the scale, agility, and adaptability of comprehensive security solutions. Our unified platform combines human expertise, AI, and automation to identify risks and validate findings with concrete evidence, ensuring a fortified defense against cyber threats. By scrutinizing the entirety of the attack surface, we enable enterprises to preemptively thwart the next cyber breach before it materializes.

TAG: Can you please share an overview of your product portfolio and what you mean exactly by continuous attack surface discovery?

BREACHLOCK: From sophisticated malware to targeted attacks, security professionals are seeking new ways to enhance their defenses, and security automation and integration have emerged as powerful allies.

The significance of automated integration has grown substantially in response to the surge of data originating from purpose-built applications, proprietary systems, work management systems, and cloud or mobile-based applications, making it a potential playground for malicious attackers.

But as the potential points of vulnerability increase within the digital landscape, the expanding attack surface has given noticeable rise to more advanced targeting techniques used by attackers. The deployment of automated security testing and integration processes is based on a growing need for continuous discovery of the attack surface to ensure assets and systems are protected on an ongoing basis.

Continuous attack surface discovery is the ongoing assessment and monitoring of security controls and configurations as well as potential vulnerabilities across the attack surface.

In addition, technology continues to evolve to meet the changing needs of enterprises, offering more adaptable and innovative solutions, such as IoT, API, cloud, and SaaS security testing and services. It also includes AI and machine learning algorithms that are integrated into security platforms to truly benefit the customer by accelerating vulnerability identification, and the discovery of patterns and anomalies associated with potential attacker entry points.

Thus, we are seeing a more continuous and proactive approach to cyber security to effectively managing the escalating volume of digital assets, data, and the inherent vulnerabilities that come with them.

TAG: How does continuous attack surface discovery benefit from taking an offensive approach? Is being proactive a major component of the approach?

BREACHLOCK: Yes, a proactive or offensive approach is at the center of attack surface discovery. Continuous attack surface discovery is the ongoing assessment and monitoring of security controls and configurations as well as potential vulnerabilities across the attack surface. This approach relies heavily on security automation, continuous monitoring, and integration as a key enabler.

The idea of continuously monitoring the attack surface is born, once again, out of necessity. And with the rise of automation and integrated security tools, this notion is no longer a wish, but a very viable method of an ongoing and proactive cyber security process focused on identifying and monitoring potential attacker entry points in an enterprise's digital environment. This approach involves the constant assessment and analysis of assets, networks, and systems to detect new or changing attack surfaces for weaknesses and exposures.

Integrating disparate or siloed tools allows for such benefits as the sharing of common or overlapping security testing features and functionalities, seamless data exchange, real-time time threat discovery, and accumulative threat intelligence from testing results for efficient incident response.

TAG: What steps do you recommend enterprise teams take to build a continuous process for attack surface discovery? How should such process align with the goals of an organization and the tools they select?

BREACHLOCK: Gaining a human perspective is always important when it comes to security testing. Automation may miss small nuances related to identified vulnerabilities and human testing and analysis can further investigate the depth of criticality providing additional context, when needed. However, automation and integration also play critical roles in supporting continuous attack surface discovery through:

AUTOMATED SCANNING AND TESTING:

Automation enables the deployment of security tests at regular intervals or in real-time. Tools such as automated pentesting and continuous attack surface discovery systematically assess the digital landscape, exploiting or identifying new assets, configurations, or vulnerabilities. Automated scans can cover a wide range of systems, applications, and network components, providing a more comprehensive view of the attack surface.

DATA AGGREGATION AND CORRELATION:

Integration allows the aggregation of data from various sources, including internal security tools, threat intelligence feeds, and third-party databases. By correlating this diverse information, security teams can gain a more accurate and holistic understanding of the attack surface. This integrated data can reveal potential threats, vulnerabilities, and areas requiring attention.

REAL-TIME MONITORING AND ALERTS:

Automated processes can continuously monitor the digital environment in real-time. Integration with other continuous security testing tools enables the immediate identification of changes or anomalies that might indicate a new attack surface or emerging threat. Automated alerts can promptly notify security teams, allowing for swift response and mitigation.

ADAPTIVE SECURITY MEASURES:

As mentioned above, threat intelligence and automated systems enable enterprises to adjust, updated, or patch security controls based on the evolving threat landscape and/or identified vulnerability. This adaptability ensures that security measures align with the current attack surface, providing a more resilient defense against emerging threats.

TAG: How specifically does your platform work? How is it designed and how does it integrate with your offensive security solutions? What makes your platform different from your competition?

BREACHLOCK: The BreachLock Platform offers AI-powered, machine-based technology and a standardized, and a proprietary built-in framework to accelerate prioritization and remediation to enable greater testing accuracy across the entire security ecosystem.

Security providers must acknowledge that well-trained AI/ML models depend on substantial data for effective security solutions.

Our AI technology can analyze vast amounts of data in real-time to identify complex patterns and anomalies impossible to detect solely with manual methods to help predict an exploit before it happens. The power of our standardized built-in framework delivers predictability, consistency, and accurate results to establish benchmarks and measure the progress of your security posture over time.

BreachLock has been providing continuous security testing for over five years now. Having conducted hundreds of thousands of penetration tests, ASM scans, and automated testing for customers across different industries, our data contains comprehensive intelligence on vulnerabilities, exploits, threats, and remediation best practices. It is impossible for any human to assimilate and process this amount of data to make real-time inferences or intelligent decisions regarding their security ecosystem. Because every target for every hacker is different every time.

BreachLock has deployed AI technology driven by the power of Natural Language Processing (NLP) to identify patterns and anomalies in mere seconds to find unique attack paths, and Tactics, Techniques and Procedures (TTPs) to make faster, more accurate and scalable decisions.

All of this leads to data-driven, evidence-based results based on real data and Proof of Concepts (POCs) which BreachLock makes available and visible within its platform to provide the necessary context for every asset tested and associated vulnerability discovered.

Security providers must acknowledge that well-trained AI/ML models depend on substantial data for effective security solutions. At BreachLock we are all about evidence-driven results that are derived based on expansive data and threat intelligence that BreachLock has accumulated and aggregated across customer and industries for the past five years to make faster and more accurate security decisions.

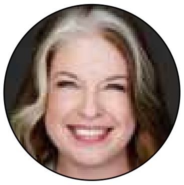
Lastly, BreachLock has developed a proprietary, uniformed framework tailored to ensure reliable, consistent, and precise outcomes. This framework not only sets benchmarks but also evaluates the advancement of our clients' security posture over time. Such a systematic approach guarantees consistent results, offering a clearer insight into cyber resilience. This, in turn, facilitates a pragmatic, metric-oriented ROI analysis that can be effectively communicated to executive teams and board members.

TAG: What future advances do you see in terms of cyber security innovation? BreachLock already offers a unique AI/ML technology, so what's next?

BREACHLOCK: The future of cybersecurity holds exciting development but will be a never-ending battle as attackers and attack methods continue to be more sophisticated and clandestine. Certainly, I hope to see a more proactive strategies when it comes to securing our defenses through continuous attack surface discovery but a few things that come to mind are:

- **Real-time Surveillance:** CSM tools will continue to play a crucial role by providing near-real-time surveillance and analysis of an environment to flag potential security threats. These tools should be integral to modern cybersecurity frameworks
- **UBA:** Leveraging behavior analytics to monitor the attack surface using AI technology to identify potentially malicious or anomalous actions.
- **Predictive Analysis:** The use of ML and AI, which BreachLock is already using, is the future of CSM and will shift enterprises and security teams from reactive to proactive intelligence, enhancing an organization's ability to manage risks.
- **Mandatory Regulatory Compliance:** We are already seeing Increasing regulation requiring the use of CSM tools as a requirement for regulatory compliance and I expect that to become more stringent., helping organizations stay updated with evolving cybersecurity laws and regulations.
- **Zero Trust:** Organizations will increasingly adopt a zero-trust approach, emphasizing continuous monitoring, verification, and validation of user identities and device access through automated technology.
- **Software Development Lifecycle:** Prioritizing security in software development will be integrated into the software development process from the outset, ensuring robust protection throughout the product lifecycle.

THE STATES OF CYBERSECURITY



JOANNA BURKEY, SENIOR ANALYST, TAG

To get a real picture of the state of any given topic, it's common best practice to ask the experts. And there certainly are plenty of experts in cybersecurity to ask these days. In fact, just reference the other articles in this publication. But what about topics that are so far-reaching, so broad that they have a consistent and direct effect on an audience far larger than only experts? Cybersecurity is, without a doubt, one of these topics. It is difficult if not impossible to find anyone that is not in some way affected by this topic, so let's look at the state of cybersecurity from a few additional points of view.

We hear frequently that "perception is reality." And for three groups of people in particular, their perception of cybersecurity—and more importantly, their reactions in response—have a tangible and daily impact. These groups are: company employees, company officers and directors, and everyday citizens. The understanding of cybersecurity, and how understanding guides the actions of each of these groups, can have an outsize effect on the success or failure of cyberattacks that are in motion at any given time. So what is the prevailing zeitgeist amongst these particular populations? And is there a single one, or multiple, co-existing mindsets?

COMPANY EMPLOYEES

Let's start with the company employee, quite often and truly referred to as the most important company resource. It's certainly inarguable that the actions of an enterprise's individual employees are one of the most important factors on the scope and impact of a potential cybersecurity incident. Knowing this, CISOs for years have attempted to create a more "cyber savvy" workforce through a variety of tools: cybersecurity training, phishing tests, tabletop simulations (just to name a few).

IT IS OBVIOUS TO ALL THAT ALLOWING AN UNAUTHORIZED, BADGELESS INDIVIDUAL INTO A SECURE BUILDING IS A THREAT, BUT TRANSLATING THIS EQUIVALENT INTO THE DIGITAL WORLD IS EXTREMELY DIFFICULT FOR ANYONE WHO IS NOT A TECHNOLOGIST.

So why are we still in a place where most employees don't feel particularly empowered or educated? In fact, the emotion they express most often about cybersecurity is that it is "frustrating." Frustrating in all senses—either the employee has to contend with technology intended to make them safer, but that instead just gets in the way, or the employee is relied upon to make good cybersecurity decisions without having any particular cybersecurity expertise. This situation can also be frustrating for the CISO. If it's so straightforward for employees to understand that letting someone tailgate into a building is bad practice, then why isn't there the same intuitive understanding of the ills of password sharing?

Technology has moved so fast, and, driven by digital transformation, taken over so many of our ways of working, that we now have large numbers of company employees who understand how to use the technology but not actually how the technology works behind the scenes. It is obvious to all that allowing an unauthorized, badgeless individual into a secure building is a threat, but translating this equivalent into the digital world is extremely difficult for anyone who is not a technologist. As the pace of technology adoption, and the exponential curve of digital complexity increase, it is becoming more and more critical to consider the employee experience. Too often, technology is adding complexity and creating impediments to the employee function. This has an adverse effect not only on security but also on employee productivity overall.

OFFICERS AND DIRECTORS

Moving on to a smaller subset of the broader employee population, let's look at the C-suite and, by extension, the board of directors. The high-level strategic decisions made by company leaders have the potential to dramatically influence the cybersecurity posture of any given enterprise. This fact is well understood. For some years now it has been impossible to avoid discussing cybersecurity and its criticality in the boardroom and at the CEO level. What has been more elusive is how to translate that criticality into appropriate action and oversight.

Board directors and C-suite members are no strangers to risk discussions. It's not overly dramatic to say that risk discussions are literally the lifeblood of what the senior executives discuss and decide on every day. However, these risk discussions usually occur in a common, business-centric lexicon and relate to well-known topics such as the net present value (NPV) of a new project. Technology, and cybersecurity in particular, often bring their own jargon that can be difficult to put into analogous business terms. On the surface, the analogies between maintaining a fleet of company cars and maintaining a fleet of firewalls—software upgrades are like oil changes!—are obvious to practitioners but not obvious at all to business experts, who generally comprise the majority of board and C-level roles.

The outcome of this disconnect is the perception that cybersecurity is a new, strange animal when in reality it is business risk and opportunity in a different form. Without tech leaders and CISOs who can make that translation, the members of the C-suite and the board will continue to struggle to understand cybersecurity in relatable terms, impacting their ability to make optimum strategic decisions.

AVERAGE CITIZENS

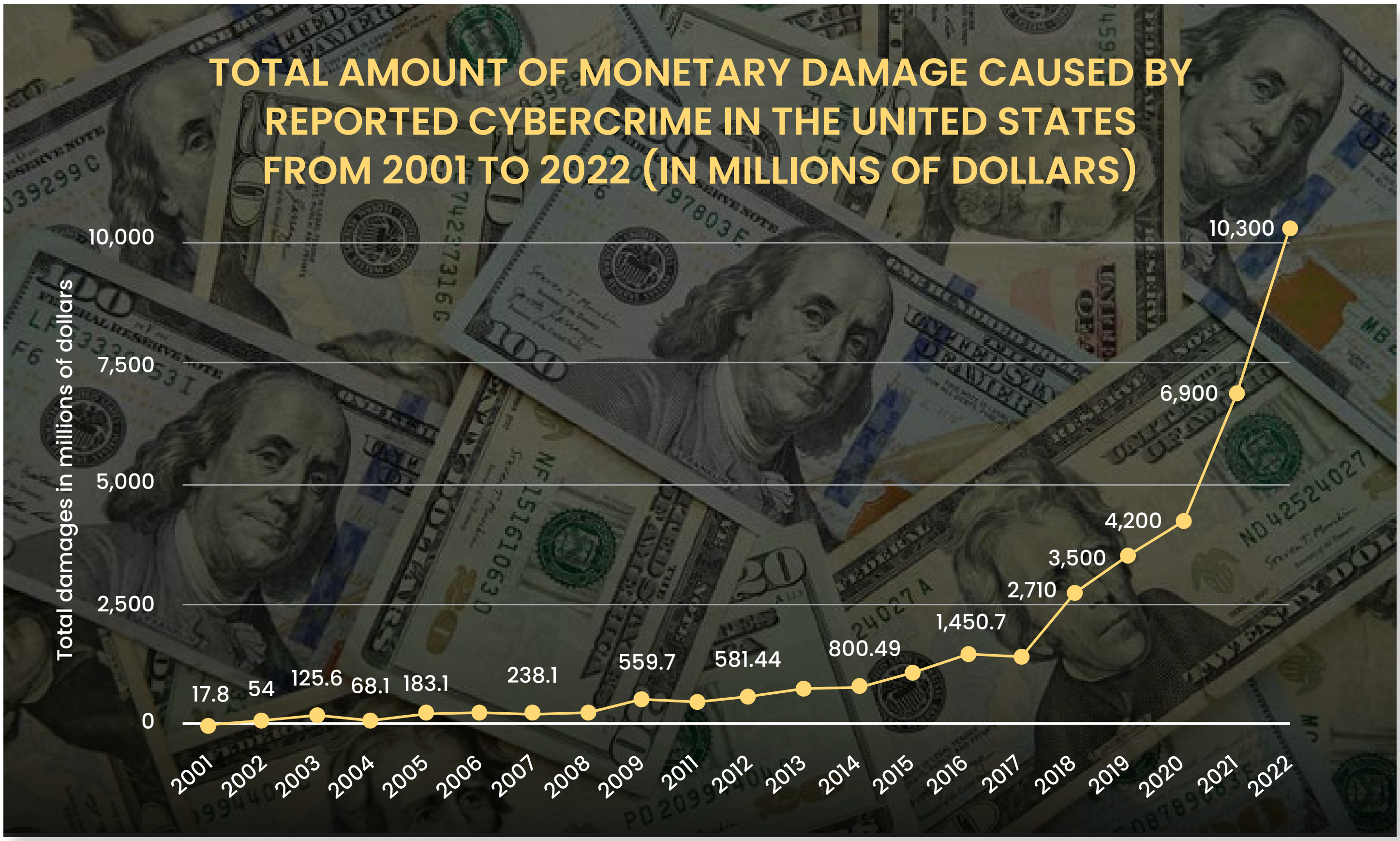
Now broadening the aperture, do we see similar states of mind in everyday citizens? Just as there's a disconnect between the 3D world and the digital world for the everyday worker, and between "business as usual" and cybersecurity for senior executives, we see people across society grapple with how to identify cyber threats and avoid joining the line of global victims. A similar analogy to the office tailgating example comes to mind. It is easy to understand how locking a door protects the house, or how putting a seat belt on protects the passenger in a car. It is extremely challenging for most people to intuitively understand what the equivalents are in the digital world to these basic protections.

The state of mind this has engendered is one of confusion, fear, and helplessness. When so much of life is digital, as it today, the effects of a cyberattack can be fundamentally destabilizing, if not life-threatening. The ability of average citizens to conceptually understand the digital tools that surround them, and then use that understanding to guide appropriate action, is not at the level needed for a "cyber-savvy" society. This can manifest, at one end of the spectrum, in extreme avoidance and mistrust of the digital ecosystem; and at the other end, in a complete reliance on the producers of technology to protect their user base.

THE BOTTOM LINE

In conclusion, there is no single "state of cybersecurity"—unless we want to posit that the state is one of fragmentation, with more opacity than clarity. Each population discussed here struggles to make parallels between their world as they know it, and how to avoid and/or mitigate cybersecurity threats.

While cybersecurity experts define and implement enterprise strategies, ultimately the bottom-line impact of cybersecurity on the lives of everyday people depends as much on those same people as it does on the experts. The ability to make good choices while living and working in the digital world will continue to require better conceptual models for understanding—and an increased focus on developing frictionless guardrails in the digital medium.



TOTAL AMOUNT OF MONETARY DAMAGE CAUSED BY REPORTED CYBERCRIME IN THE UNITED STATES FROM 2001 TO 2022 (IN MILLIONS OF DOLLARS)

Source: Statista 2024

REDEFINING CYBERSECURITY

FROM DEFENSIVE MEASURES TO A STRATEGIC BUSINESS STRATEGY

DAVID NEUMAN, SENIOR ANALYST, TAG

In 2022, the monetary damage caused by cybercrime reported to the United States' Internet Crime Complaint Center (IC3) reached a historic peak of $10.3 billion, which represented a year-over-year increase of around 50%. This is despite 2023 global spending on cybersecurity and risk management reaching $181.1 billion. It's projected to rise to $215 billion in 2024. Given these numbers, why aren't we seeing a reduction in the cyber threat or in the material damage to businesses?

As industries grapple with the escalating digital complexity, sophistication of cyber threats, and the cost of defeating them, the traditional stance on cybersecurity—primarily focused on defensive technical operations and compliance—is proving to be ineffective. It is imperative to have a strategic pivot towards viewing cybersecurity through the prism of business enablement and risk management.

This change is driven by the need to safeguard assets and business operations and harness cybersecurity as a catalyst for competitive differentiation in the marketplace. It highlights the pressing need for cybersecurity to evolve in purpose from a defensive, technical posture to a proactive strategy that aligns with and propels business objectives. Moreover, it emphasizes the necessity for technologies and processes that are both adaptive and swift, mirroring the pace of business innovation. Through this lens, we gain clarity on why cybersecurity must transcend its traditional boundaries and be reimagined as a core component of business strategy, enabling organizations to navigate the digital age with confidence and strategic advantage.

> **IF YOUR SECURITY BUDGET IS BASED ON CONTINUING INCREASES THAT ARE TIED PURELY TO ADDITIONAL COSTS FOR MORE TECHNOLOGY PLATFORMS VERSUS BUSINESS OUTCOMES, THEN YOU ARE LIKELY NOT PROVIDING A COMPETITIVE ADVANTAGE.**

THE LEGACY MINDSET: A BUSINESS STRATEGY DISASTER

For too long, the prevailing approach to cybersecurity has been reactive. Too often products and services are designed with functionality as the primary focus, and security is bolted on as an afterthought. This leads to weaknesses attackers can exploit, resulting in costly redesigns, reputational damage, and potential fines for noncompliance.

“Security by design” means baking security into the development process from the outset. The alternative can lead to disaster. For example, a software company releases a new product with exciting features but fails to incorporate security. The product is riddled with vulnerabilities, leading to a major data breach that erodes customer trust and forces costly remedial efforts. We saw this recently in the attack against Microsoft Exchange Online. As reported by the DHS Cyber Safety Review Board, the breach was attributed to Chinese espionage and advanced threat actors who accessed U.S. government agencies involved in sensitive diplomatic issues with China. This suggests the problem affects enterprises and companies of all sizes. We can all do better.

Many organizations rely on static security architectures that are ill-equipped to handle the dynamic nature of today’s business environments. An enterprise that relies on a rigid security architecture, if they have one at all, will struggle to adapt to the rapid adoption of cloud services and artificial intelligence, among other digital imperatives. This creates security blind spots, exposing the organization to new attack vectors and slowing growth.

If your security program or IT and product platforms have not adopted this approach under the guidance of experienced experts, then you are likely accepting significant business risk. On the other hand, if your company’s architectures are flexible and can evolve alongside changes in technology, business processes, and the threat landscape, cyber resiliency can be a competitive advantage.

CYBER LEADERS AS BUSINESS LEADERS

Cybersecurity leaders often lack the business acumen needed to effectively communicate risks and justify security investments to business partners and corporate leaders. This disconnect can lead to underinvestment in cybersecurity and a failure to align security initiatives with broader business objectives. It's crucial to bridge this gap between technical experts and business leaders to have a deep understanding of business strategy.

TAG Infosphere tracks over 4,700 cybersecurity vendors in a taxonomy of 20 categories. In a recent conversation with a chief information security officer (CISO) of a large enterprise, I asked, "How many of these taxonomy categories do you have a a technology in? His response was, "All of them. In fact, I have as many as three technologies for some of them." We agreed that more tools do not mean better security and don't necessarily equal business enablement. Many CISOs are trapped in sustaining these large security ecosystems, making it difficult for them to adapt to business demands and contribute to the growth the company is trying to achieve.

1. APPLICATION SECURITY
2. ATTACK SURFACE MANAGEMENT
3. AUTHENTICATION
4. CLOUD SECURITY
5. DATA SECURITY
6. EMAIL SECURITY
7. ENCRYPTION AND PKI
8. ENDPOINT SECURITY
9. ENTERPRISE IT INFRASTRUCTURE
10. GOVERNANCE, RISK, AND COMPLIANCE (GRC)
11. IDENTITY AND ACCESS MANAGEMENT (IAM)
12. SECURITY OPERATIONS AND RESPONSE
13. MANAGED SECURITY SERVICES
14. MOBILE SECURITY
15. NETWORK SECURITY
16. OPERATIONAL TECHNOLOGY SECURITY
17. SECURITY PROFESSIONAL SERVICES
18. SOFTWARE LIFECYCLE SECURITY
19. THREAT AND VULNERABILITY MANAGEMENT
20. WEB SECURITY

TAG Cyber Taxonomy

If your security budget is based on continuing increases that are tied purely to additional costs for more technology platforms versus business outcomes, then you are likely not providing a competitive advantage. Nor are you addressing the business risks for your organization. As indicated above, many security programs have duplicative technologies performing highly similar functions. This means higher complexity, costs, and a demand for highly skilled people. The result may be the equivalent of a two-mile freight train going five miles an hour, unable to move or change at the speed of the business.

We are seeing rightsizing in the cybersecurity technology market, which indicates that many security organizations, especially those in large enterprises, are rationalizing their existing portfolios instead of buying more technology solutions. That is a step in the right direction. Still, the rationale must include more than the technological capability and extend to ensuring that the solutions map a path to business outcomes, and that talent development and growth are part of it.

THE PATH FORWARD: CYBER RESILIENCY AND TRUST AS STRATEGIC ENABLERS

If your organization is considering a real pivot, there are some things you should consider. No two organizations are identical, and there are no easy buttons, so it's impractical to suggest a common playbook. But some focus areas are a good starting point.

1. ESTABLISH SHORT AND LONG-TERM PLANNING.

Many organizations claim to do strategy when what they are doing is planning—for their own teams and business units. In some cases, this is understandable. It may be because the organization lacks a comprehensive strategy. But in most cases the security organization is unaware of the business objectives and how they fit in. This isn't a company problem; it's a security problem. If you are doing any strategy or planning and have no direct insight or influence in what the business is doing, you are likely creating disruptions instead of enablement.

Your strategy should always begin with the business ambitions and desired outcomes. A series of questions arises from those insights. Are you positioned, with existing capabilities and services, to enable the outcomes the business seeks—near- and long-term? If you are not, can you adjust or rationalize your portfolio? Last, do you have the right skills and leadership to work with other business stakeholders? If the answer to any of these questions is no, you should consider fundamental changes to your strategy.

If your answer to these questions is yes, start influencing the messaging among external stakeholders that cyber resiliency and trust are differentiators. It may sound like a play on words, but you may be able to stop focusing on security and instead change your company's value generation story as part of product and service delivery.

2. SET RISK EXPECTATIONS AND SPEAK CLEARLY.

The security community has far too many cliches and tag lines the business doesn't understand and can't relate to. "Defense in depth is key to our cybersecurity strategy." "Zero trust is the future of security." "We must stay vigilant against advanced persistent threats." These make it hard for others you need for support to understand what you do and why it's important. Additionally, security teams all too often talk about what they do and not the business or the market they serve. Instead of spending time explaining advanced persistent cyber threats, try putting your concerns in terms of potential business disruption and what that could mean to your customers or business partners. Spend time spreading awareness of the risks in your market. Let your customers know what you do and why, and how your approach differentiates you from your competitors.

What you don't do is sometimes just as important as what you do. The security team cannot accept business risk on its own because it doesn't own much of the business it is charged to protect. In addition, not every cyber risk requires a cyber solution. This means emphasizing that not all issues in the realm of cybersecurity can be effectively addressed solely through technological or security means. For example, cybersecurity risks can also arise from weaknesses in the supply chain, where third-party vendors or partners may inadvertently introduce risks into an organization's systems and networks.

While implementing cybersecurity measures within one's organization is important, it may not be sufficient to address supply chain risks that lead to operations disruption or that compromise product integrity. You're going to get attacked—embrace it and prepare for it. This is what it means to be resilient. There are risk tolerance guardrails the security team must help business stakeholders understand so that they can participate in remediation (and value generation), and, more importantly, so that they won't make incorrect assumptions about their risk exposure.

3. BUILD AN ADAPTIVE AND HIGH-PERFORMING TEAM.

A 2023 report from the International Information Systems Security Certification Consortium (ISC2) highlights a shortage of almost four million cybersecurity professionals globally. Frankly, I don't buy it. I'm not suggesting that ISC2 has done something wrong. Still, there is too much ambiguity in our jobs and the positions we need to fill. And our existing workforce lacks professional development. We also are addressing only our needs today and yesterday instead of focusing more attention on the organization we'll need to be tomorrow. To seize the opportunities of tomorrow, we must develop a workforce of innovative thinkers and creative doers, not just technical experts. This entails personal and professional skills, including the ability to communicate, understand how an organization is organized and operates, and build relationships. The skills are essential in building a resilient organization.

As an adjunct university professor who teaches cyber operations and threat hunting, I ask students about their career ambitions. They almost unilaterally say, "I want to work in cyber." When I ask for more specifics, they seem lost. Why is that? I believe we have produced a generation of security tool administrators when we need critical and analytical thinkers and problem solvers. The security industry needs to drive the demand for more of these thinkers and fewer holders of professional certifications, which have become an industry themselves.

Too often security team member development is relegated to technical competency training. I'm not suggesting this is wrong; it's just incomplete. If technical skills are all a person brings to the table by the time they are promoted into leadership positions, they will be disadvantaged, as will the organizations they belong to. We must build well-rounded teams to solve business risk problems and take advantage of opportunities beyond security and technology. If deliberate training, development, and career progression plans are discretionary budget items, companies will not recruit or retain the top talent needed to compete and succeed. People are vital to the effective execution of strategy.

4. WORK TO ACHIEVE OPERATIONAL EXCELLENCE.

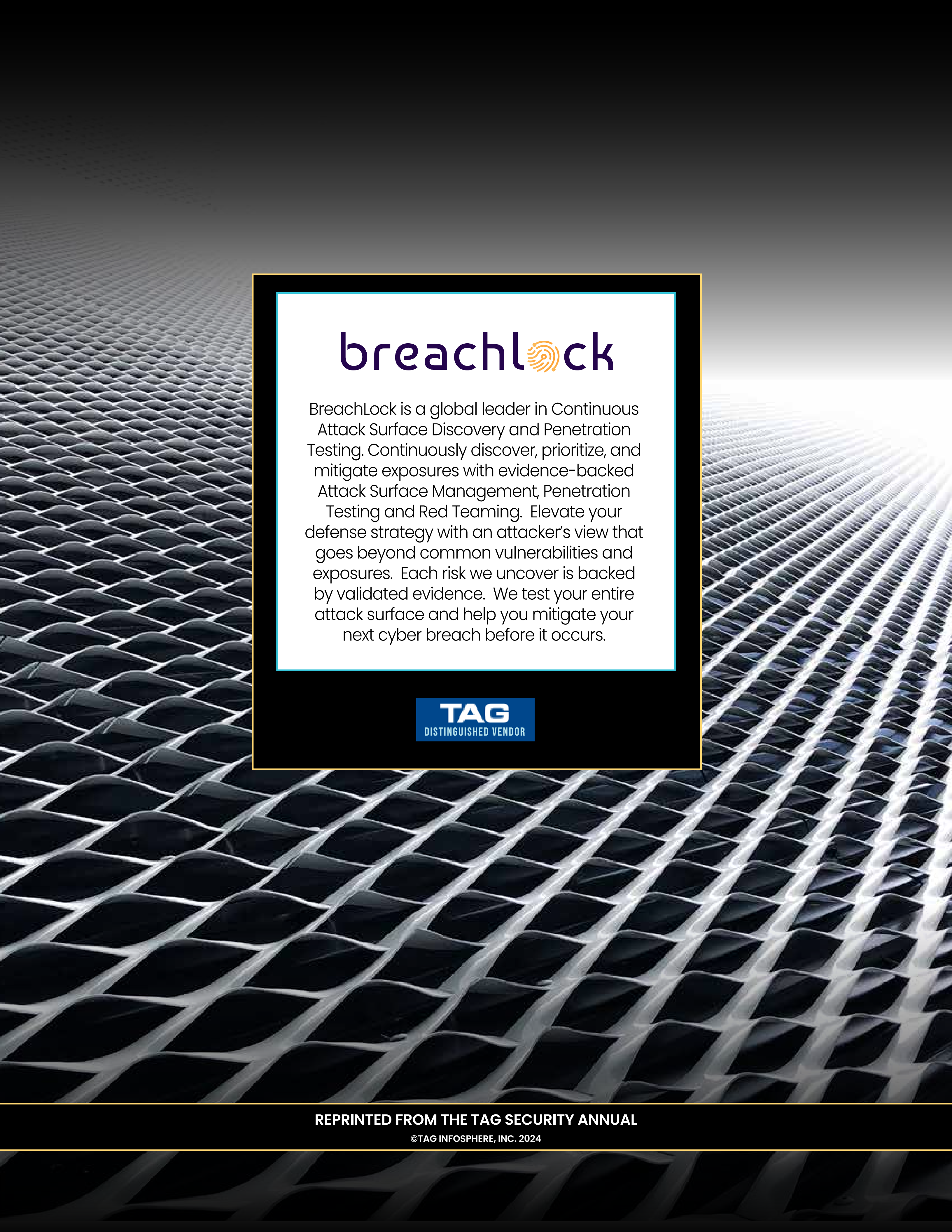
Organizations must transcend procedural efficiency and evolve into dynamic learning entities, constantly honing their defenses against ever-shifting threats. Embracing a learning organization mindset, they foster curiosity, innovation, and a relentless pursuit of improvement throughout their organization.

This approach entails more than just investing in technical prowess; it's about cultivating a collective intelligence that thrives on feedback, reflection, and shared knowledge. By promoting ongoing training, encouraging experimentation, and institutionalizing robust incident response processes, organizations equip themselves to navigate the complexities of modern cybersecurity with agility and resilience. Moreover, they recognize that cyber resiliency is not a static discipline but a fluid landscape where adaptability and innovation are paramount.

Ultimately, by prioritizing a culture of continuous improvement, organizations elevate their capabilities from reactive measures to proactive planning. They leverage each encounter with cyber threats as an opportunity for growth, distilling insights from successes and failures alike. Through this commitment to learning and evolution, organizations fortify their posture against cyber exploitation, safeguarding their digital assets and resilience in an increasingly hostile digital landscape.

FINAL THOUGHTS

The consequences of outdated approaches are significant. Companies find themselves locked in a never-ending arms race against cybercriminals and nation-state threat actors, constantly pouring resources into upgrading defensive technology. This leads to bloated cybersecurity budgets that drain resources from more value-adding initiatives. In addition, the reactive nature of legacy security models often results in a material impact on companies and their customers. According to IBM's report on the Cost of a Data Breach 2023, the average is $4.45 million. The reputational damage can be even more devastating, eroding customer trust and hindering long-term growth.



breachlock

BreachLock is a global leader in Continuous Attack Surface Discovery and Penetration Testing. Continuously discover, prioritize, and mitigate exposures with evidence-backed Attack Surface Management, Penetration Testing and Red Teaming. Elevate your defense strategy with an attacker's view that goes beyond common vulnerabilities and exposures. Each risk we uncover is backed by validated evidence. We test your entire attack surface and help you mitigate your next cyber breach before it occurs.

TAG
DISTINGUISHED VENDOR

REPRINTED FROM THE TAG SECURITY ANNUAL