featured customers

Breach & Attack Simulation Software Category

WINTER 2024
Customer Success Report





Breach & Attack Simulation Software Category

Breach and Attack Simulation (BAS) software helps to test an organization's cybersecurity defenses by simulating real-world cyber threats and attacks in a controlled environment. It allows companies to assess the effectiveness of their security measures and identify vulnerabilities in their systems. By simulating realistic attack scenarios, organizations can identify weaknesses in their defenses, assess the response capabilities of their security teams, and prioritize remediation efforts.

Benefits of adopting such software include enhanced cybersecurity preparedness and regulatory compliance. BAS software aids in compliance by providing evidence of regular security testing, a requirement in various industry regulations. Overall, adopting BAS software strengthens an organization's cybersecurity posture, improves incident response preparedness, and reduces the risk of successful cyber attacks.

Customer Success Report Ranking Methodology

The FeaturedCustomers Customer Success ranking is based on data from our customer reference platform, market presence, web presence, & social presence as well as additional data aggregated from online sources and media properties. Our ranking engine applies an algorithm to all data collected to calculate the final Customer Success Report rankings.

The overall Customer Success ranking is a weighted average based on 3 parts:

CONTENT SCORE

- Total # of vendor generated customer references (case studies, success stories, testimonials, and customer videos)
- Customer reference rating score
- Year-over-year change in amount of customer references on FeaturedCustomers platform
- Total # of profile views on FeaturedCustomers platform
- Total # of customer reference views on FeaturedCustomers platform

MARKET PRESENCE SCORE

- Social media followers including LinkedIn, Twitter, & Facebook
- Vendor momentum based on web traffic and search trends
- Organic SEO key term rankings
- Company presence including # of press mentions

COMPANY SCORE

- Total # of employees (based on social media and public resources)
- Year-over-year change in # of employees over past 12 months
- Glassdoor ranking
- Venture capital raised

Award Levels



MARKET LEADER

Vendor on FeaturedCustomers.com with substantial customer base & market share. Leaders have the highest ratio of customer success content, content quality score, and social media presence relative to company size.



TOP PERFORMER

Vendor on FeaturedCustomers.com with significant market presence and resources and enough customer reference content to validate their vision. Top Performer's products are highly rated by its customers but have not achieved the customer base and scale of a Market Leader.



RISING STAR

Vendor on FeaturedCustomers.com that does not have the market presence of Market Leaders or Top Performers, but understands where the market is going and has disruptive technology. Rising Stars have been around long enough to establish momentum and a minimum amount of customer reference content along with a growing social presence.

2024 Customer Success Awards

Check out this list of the highest rated Breach & Attack Simulation Software based on the FeaturedCustomers Customer Success Report.



BISHOPFOX NetSPI™ PENTERA



ATTACKIQ bugcrowd Crowdsourced Security CYCOGNITO

Cymulate FIREMON PICUS

SafeBreach Synack XM Cyber



HORIZON3.ai
~~TRUST~~ BUT VERIFY

* Companies listed in alphabetical order



2024

BREACH & ATTACK SIMULATION SOFTWARE

MARKET LEADER

featured customers



ABOUT BISHOP FOX

BISHOPFOX

Bishop Fox is recognized as the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. Enterprises have been told that breaches are inevitable. But they don't accept that. They focus on offensive security because they believe securing modern organizations requires a "forward defense" approach that proactively uncovers and eliminates exposures before they are exploited.

49 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"The Bishop Fox assessment really helped us evolve our security processes. We grew quickly from a small organization, quadrupling over a year, and the guidance we received from Bishop Fox helped us prioritize certain areas and quickly get a phased security enhancement plan in place. This assessment was a great step forward in evolving our program to scale to our needs for the coming year."

DAN BLAKE
CHIEF TECHNOLOGY OFFICER, ASPIRE

"At Sonos, the hardware is a key component to the overall security posture. So having a partner that is comfortable with hardware-based penetration tests was very important to us. I've worked with a number of different vendors, but when it came time to figure out who to use for Sonos, I ultimately knew Bishop Fox was the best fit for us."

JIM HONG
DIRECTOR OF PRODUCT MANAGEMENT, SONOS

"Bishop Fox has demonstrated throughout the years that they're experts in our technology stack and have an ability to help us understand where we might be vulnerable before the adversaries have a chance to effect that value for our customers."

CARL KUBALSKY
BUSINESS INFORMATION SECURITY OFFICER, JOHN DEERE

"The Bishop Fox security consultants have brought critically interesting insights on the security of our systems, which has enabled us to improve them in very actionable ways."

ADRIEN VAN DEN BRANDEN
CO-FOUNDER & CHIEF EXECUTIVE OFFICER, CANYON

TRUSTED BY

CANYON illumio RELTIO SONOS JOHN DEERE



ABOUT NETSPI

NetSPI™

NetSPI delivers application and network security solutions to enterprise organizations, globally. Their security testing experts and proprietary technology platform empower organizations to scale and operationalize their security testing programs. Contact them today to learn how they can help you catapult the sophistication of your programs and improve your organizations' security posture.

65 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"We engaged NetSPI to support us in a variety of data security and penetration testing services ranging from our infrastructure all the way to our mobile apps. We store patient data and hold confidential information from lab results and other personal data. It's of utmost importance to keep this entrusted data safe while it's in our stewardship. We particularly appreciate the flexibility of working with NetSPI and their ease of identifying areas of risk."

MARK EPSTEIN
VICE PRESIDENT, RXMX

"prior to deploying NetSPI CVM, we relied on a collection of manual processes to manage our vulnerability data. There was no worlcfiow capability and the process required a tremendous amount of manual effort. The NetSPI CVM solution allowed us to streamline the process, providing a one-stop shop fox our vulnerability triage pfocesses."

JONATHAN KLEIN
CISO, BROADRIDGE INFORMATION SECURITY GROUP

"The quality of NetSPI's deliverables also stood out to me. I liked that the pricing model is functional elements and that they conduct an extensive walk-through of the application before the engagement. And the fact that remediation testing is included in NetSPI's pricing is huge. That is not something you commonly see from other penetration testing companies."

MISSION FEDERAL CREDIT UNION

"The NetSPI team is easy to work with. They gave all vulnerabilities to our team through a very easy process and the results were clear, making them easy to remediate. In addition, Resolve™ is easy to access and communicate through."

JED GRISEL
CO-FOUNDER, AUDITORY IMPLANT INITIATIVE

TRUSTED BY

Carlson Wagonlit Travel · Medtronic · GRACO · hudl · GONG



ABOUT PENTERA

PENTERA

Pentera is the category leader for Automated Security Validation, allowing every organization to test with ease the integrity of all cybersecurity layers, unfolding true, current security exposures at any moment, at any scale. Thousands of security professionals and service providers around the world use Pentera to guide remediation and close security gaps before they are exploited.

49 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"Pentera to me is peace of mind. What it does is validation, it's what allows us to have solid objective evidence that we are protected. Running the platform gives us assurance that we didn't miss any patches, that our configurations are secure. We know that we have not only remediated vulnerabilities, but that they also can't be exploited."

PAUL ERNST
MANAGING DIRECTOR & CHIEF INFORMATION OFFICER, SANDLER CAPITAL MANAGEMENT

"Pentera enables Quality Assurance of our cyber controls, credentials, vulnerabilities and privileges. It's not enough to rely on the employees and my security systems. I recommend to all security professionals that they look into automating their risk validation practices at scale."

ERAN LIUZZI
CHIEF INFORMATION OFFICER, YIGAL ARNON & CO.

"Not only does Pentera help guide the team to the vulnerabilities that need to be corrected, it also provides the ability to confirm the effectiveness of security policies and remediation patches while reducing the costs."

BRETT WALMSLEY
CHIEF TECHNOLOGY OFFICER, ROYAL BOLTON HOSPITAL NHS FOUNDATION TRUST

"Pentera gives us the only option for an agentless, low-touch, fully automated solution that continuously assesses security readiness with unlimited scale and one-click operation."

FELIPE FRASQUILO
BUSINESS DEVELOPMENT MANAGER DATA CENTER AND CLOUD, IP TELECOM

TRUSTED BY

LuLu Exchange · WYNDHAM HOTEL GROUP · BREWDOG · IP TELECOM · SANDLER Capital Management



2024

BREACH & ATTACK SIMULATION SOFTWARE

TOP PERFORMER

featured customers



ABOUT ATTACKIQ

ATTACKIQ

AttackIQ was a leading independent vendor of breach and attack simulation solutions, built the industry's first Security Optimization Platform for continuous security control validation and improving security program effectiveness and efficiency. AttackIQ is trusted by leading organizations worldwide to plan security improvements and verify that cyberdefenses work as expected, aligned with the MITRE ATT&CK framework. The Company is committed to giving back to the cybersecurity community through its free AttackIQ Academy, open Preactive Security Exchange, and partnership with MITRE Engenuity Center for Threat-Informed...

68 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"Check Point is delighted to be part of AttackIQ's Preactive Security Exchange (PSE). Customers continue to consolidate their security approach with Check Point Infinity Architecture to prevent zero-day and fifth-generation cyberattacks. Leveraging the MITRE ATT&CK Framework with comprehensive capability for continuous and targeted validation of security posture, AttackIQ objectively showcases Check Point's prevention capabilities of their comprehensive Infinity Architecture."

JASON MIN
HEAD OF BUSINESS DEVELOPMENT, CHECKPOINT SOFTWARE TECHNOLOGIES

"Securonix values its partnership with AttackIQ and is delighted to be a part of AttackIQ's Preactive Security Exchange (PSE). Both companies are deeply committed to the MITRE ATT&CK Framework, both organisations improve security operations exponentially through analytics, intelligence and automation. Our MSSP's and Reseller partners requested this integration, and we are happy to deliver it."

SACHIN NAYYAR
CHIEF EXECUTIVE OFFICER, SECURONIX

"We are proud to count AttackIQ as a Microsoft Intelligent Security Association partner. We're pleased to now be part of their PSE as both our companies continuously work on ways that joint customers can realize greater ongoing value from both our products."

ROB LEFFERTS
CORPORATE VICE PRESIDENT, MICROSOFT

"AttackIQ also stands out because even as it emulates the adversary in its testing process, we can be confident that if we attack a client's production systems, we will not break their workflows. That is a problem for some pen testing tools."

GUILLEM RAJA
JUNIOR CYBERSECURITY TECHNICIAN, ESED

TRUSTED BY

SentinelOne · ISS · Attivo Networks · AmerisourceBergen · Check Point Software Technologies Ltd.



ABOUT BUGCROWD

bugcrowd
Crowdsourced Security

Bugcrowd delivers the ultimate in security assessment for the enterprise. The pioneer and innovator in crowdsourced security testing for the enterprise, Bugcrowd combines the power of more than 65,000 security researchers and its proprietary Crowdcontrol platform to surface critical software vulnerabilities, and level the cybersecurity playing field. Bugcrowd provides a range of public, private, and on-demand options that allow companies to commission a customized security testing program to fit their specific needs. Based in San Francisco, Bugcrowd is backed by Blackbird Ventures, Costanoa Ventures, Industry Ventures, Paladin Capital Group, Rally...

96 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"What is amazing about Bugcrowd — With all the security technology and process that we have in place at Motorola we always find bugs when product goes live. Bugcrowd has saved us close to $60 million, simply because we've avoided major data breaches in the eyes of our customers."

RICHARD RUSHING
CISO, MOTOROLA

"Bugcrowd has expanded our approach to vulnerability testing. Bugcrowd has provided us with a clearer understanding of the hackers' mentality, by bringing all the key parties together in a common, collaborative way. That is a key benefit that we've seen working with Bugcrowd."

SHIVAUN ALBRIGHT
CHIEF TECHNOLOGIST, HP

"Bugcrowd's Vulnerability Disclosure Program is one of the best value-for-money services that we have. The annual cost of the program is the same cost of one traditional penetration test and the VDP has given us around a 100-fold increase in actionable intelligence."

DAN MASLIN
CHIEF INFORMATION SECURITY OFFICER, MONASH UNIVERSITY

"We like Bugcrowd's approach. A structured format for reporting issues helps drive better quality bugs and filter out noise while the handling of bounty payments is a huge time savings for us. Having a third party help manage researchers will be very valuable."

DAVE FARROW
DIRECTOR OF ENGINEERING, BARRACUDA NETWORKS

TRUSTED BY

DigitalOcean · BIGCOMMERCE · Barracuda · aruba · ATLASSIAN



ABOUT CYCOGNITO

CYCOGNITO

CyCognito is believe all organizations should be able to protect themselves from even the most sophisticated attackers. That's why they created the first ever Shadow Risk Elimination platform, putting nation-state level cyber reconnaissance techniques into the hands of every organization. When their risks are no longer in the shadows, companies operate more confidently, safely and freely.

27 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"With the CyCognito platform we have greatly improved our attack surface visibility and enhanced our attack surface management workflows. The platform helps us operate smoothly and provides reduced risk, reduced complexity and increased visibility."

KEVIN KEALY
CHIEF INFORMATION SECURITY OFFICER, SCIENTIFIC GAMES

"CyCognito provides our company with cutting-edge technology enabling my team to have global visibility into all our web-facing assets in an easy-to-use interface, and it does so better than other attack surface management tools we've used."

ALEX SCHUCHMAN
CHIEF INFORMATION SECURITY OFFICER, COLGATE-PALMOLIVE

"Whatever you do, you need some kind of transparency, some kind of information about how your outward-facing landscape looks to hackers. I would recommend CyCognito because it's easy to use."

DANIEL MAIER-JOHNSON
CISO, ASKLEPIOS

"The CyCognito platform helps me figure out how to distill an overwhelming amount of information and determine what is a risk for our business."

MEGAN BELL
CHIEF PRIVACY AND SECURITY OFFICER, HUMAN API

TRUSTED BY

SCIENTIFIC GAMES · KAISER PERMANENTE · HUMAN API · Berlitz · axel springer



ABOUT CYMULATE

Cymulate

Cymulate is a SaaS-based breach and attack simulation platform that makes it simple to know and optimize your security posture any time, all the time, and empowers companies to safeguard their business-critical assets. Cymulate challenges your security controls by initiating thousands of attack simulations, showing you exactly where you're exposed and how to fix it making security continuous, fast, and part of every-day activities.

99 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"We rely heavily in security service providers (SSPs) and technology to protect our company. In the past we assumed that we were protected, but in reality, our assumptions were incorrect. Cymulate enables us to collaborate with our SSPs to improve our security, and they have embraced this because it improves the services they provide to all their customers."

RENE FRANCIS LARES
IT MANAGER, YX ENERGY

"Cymulate provides us with the insights to close gaps and optimize the controls we already have in our security stack—we don't need to waste time or money looking for new tools to improve our security."

LIAD PICHON
DIRECTOR OF CYBERSECURITY, BLUESNAP

"I use many security solutions, but Cymulate is a must if you want to ensure your organization is safe from cyber threats. It's easy to use, intuitive, and the customer support is unparalleled."

ARIEL KASHIR
CISO, HERTZ

"I would recommend Cymulate because of its ease of use, it can quickly provide you a window into how vulnerable or how protected your organization is against external threats."

JORGE RUÃO
HEAD OF SECURITY OPERATIONS, EURONEXT

TRUSTED BY

CaixaBank · Raiffeisen Bank International · Nemours Children's Health System · Telit · Hertz



ABOUT FIREMON

FireMon is the only real-time security policy management solution built for today's complex multi-vendor, enterprise environments. Supporting the latest firewall and policy enforcement technologies spanning on-premises networks to the cloud, only FireMon delivers visibility and control across the entire IT landscape to automate policy changes, meet compliance standards, and minimize policy-related risk. Since creating the first-ever policy management solution in 2004, FireMon has helped more than 1,700 enterprises in nearly 70 countries secure their networks. FireMon leads the way with solutions that extend and integrate policy management with...

61 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"With FireMon tracking compliance for us, we were able to shrink our overall audit time by two-thirds of our original schedule. Additionally, we were able to clean and push out almost 300 rules that had not been reviewed in over three years."

PATRICK STOEHR
MANAGER, DATA NETWORK SERVICES, CONVEY HEALTH SOLUTIONS

"FireMon is very well suited for an enterprise with any number of firewalls and types. It is scalable, and can be installed as a single appliance, or distributed infrastructure, with as many data collectors as needed."

KEN SHARP
CYBERSECURITY / FIREWALL ANALYST, DUPONT

"FireMon Security Manager is well suited for a dynamic environment that includes firewalls from multiple types of manufacturers with a large amount of firewall changes."

JAMIE HUDSON
INFORMATION SYSTEMS AUDITOR, LEGALSHIELD

"Change control is the key to every security audit, FireMon allows us and auditors to research all changes done. It's a must-have tool for the security department."

JEFF REESE
CYBER SECURITY ENGINEER, AERA ENERGY LLC

TRUSTED BY

LegalShield · Alkami · AERA · convey · DUPONT



ABOUT PICUS SECURITY

PICUS

Picus Security, the leading security validation company, gives organizations a clear picture of their cyber risk based on business context. Picus transforms security practices by correlating, prioritizing, and validating exposures across siloed findings so teams can focus on critical gaps and high-impact fixes. With Picus, security teams can quickly take action with one-click mitigations to stop more threats with less effort.

31 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"The Picus Platform is an easy to use solution that helps us ensure our defenses keep pace with evolving threats. The security scores and insights it provides help us to assess the effectiveness of our controls and identify ways to better protect our assets and customer data. The results we've seen, as well as the high level of support and guidance we receive from Picus' Customer Success Team, were key factors in our decision to recently renew our..."

ELIF SEVEN
SENIOR TEAM LEAD, MIGROS

"Using Picus, we can conduct risk analysis about possible attacks for their impact on people, processes, and technology layers. We obtained the capability of pinpointing if a technology we deployed currently does not detect and prevent a new threat. This insight allows us to mobilize the relevant stakeholders to eliminate the associated risk immediately."

ANIL KUŞ
INFORMATION SECURITY RISK MANAGER, ISTANBUL GRAND AIRPORT

"Our decision to choose Picus stems from the urgent need to stay ahead of rapidly evolving threats. It provides us with real-time insights into active threats and allows us to assess our defense capabilities and validate our remediations effectively."

JD BROWN
CHIEF INFORMATION OFFICER, PRIME INSURANCE COMPANY

"By using Picus, SOC professionals are more aware of infrastructure management and conversely, SecOps become more involved in cyber defense activities."

ENGIN KARAGÜLMEZ
INFORMATION SECURITY MANAGER, TURKISH AIRLINES

TRUSTED BY

iGA · MIGROS · ukrtelecom better starts today · TURKCELL · TURKISH AIRLINES



ABOUT SAFEBREACH

SafeBreach

SafeBreach is a cybersecurity company based in Sunnyvale, California and Tel Aviv, Israel. The company has developed a platform that simulates hacker breach methods, running continuous "war games" to identify breach scenarios across network systems. Their mission is to innovate the way the industry validates security risks from static to continuous, from theoretical to practical.

46 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"Tools like SafeBreach provide a continuous picture of how well you're protecting yourself. Vulnerability scanners miss the mark, penetration testing doesn't go far enough, and compliance tools only provide an isolated, often subjective snapshot of your security posture. SafeBreach, however, provides continuous insight while accurately replicating real-world attack scenarios."

TAL ARAD
CHIEF INFORMATION SECURITY OFFICER, CARLSBERG

"SafeBreach constantly challenges my security controls to ensure they are working as expected and improves the quality of the findings of my red teams. It enhances security by identifying potential outbound channels for data, and makes our red teams more efficient and effective by focusing them on the right issues."

SHAHAR BEN-HADOR
CHIEF INFORMATION SECURITY OFFICER, IMPERVA

"With cyberattacks, the key thing to understand is that only when the data gets out does it become an actual breach. This is where the brilliance of SafeBreach comes in. By giving you an actionable inventory of egress methods so data cannot be exfiltrated, SafeBreach prevents the final step in the kill chain."

JOE WHITE
SENIOR SECURITY ARCHITECT, CREDIT KARMA

"A human pen tester can't attack your entire system all the time, but attack simulations can be programmed to run continuously. SafeBreach helps us identify risks and issues before a breach actually occurs."

JIMMY SANDERS
HEAD OF INFORMATION SECURITY, NETFLIX DVD

TRUSTED BY

HUSCH BLACKWELL · experian · PayPal · creditkarma · imperva



ABOUT SYNACK

Synack

Synack is a security company revolutionizing how enterprises view cybersecurity through a hacker's eyes. Synack's hacker powered security platform arms clients with hundreds of the world's most skilled, highly vetted ethical hackers who provide a truly adversarial perspective of clients' IT environments. Synack's confidential client base is comprised of some of the largest F500/G500 enterprise organizations across banking and financial services, healthcare, consumer goods and retail, manufacturing, technology and the U.S. Federal Government.

28 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"As part of a technology-driven insurance company, Security needs to keep up with fast iterations and deployment cycles at Allianz Direct. Traditional, point-in-time pentests are no longer viable in our agile delivery approach. Continuous pentest programs like the one from Synack are the only way to securely deliver customer value at the pace we want."

ANTON GÖBEL
INFORMATION SECURITY OFFICER, ALLIANZ DIRECT

"EllisDon utilizes leading technology and leverages data to create a sustainable competitive advantage. That needs to be protected. Synack not only uncovers our unknown vulnerabilities, but they also provide us with valuable security data that tells us more about our security posture and how it changes over time."

GARY SMITH
VP ENTERPRISE TECH RELATIONS, ELLISDON

"We now have greater confidence in our security because Synack showed us vulnerabilities that matter, found by their crowdsourced group of 500+ researchers, then told us what we needed to improve and how to fix it."

CASEY LEE
DIRECTOR, IT SECURITY, NOV

"Synack struck us as the most professional, the most responsive, the best designed and had the best functioning product. We didn't feel quite the same comfort with other providers as we did with Synack."

JOSEPH DALLAGO
CEO & CO-FOUNDER, RAIN FINANCIAL

TRUSTED BY

Rain · Freshfields · EllisDon · CBI HEALTH GROUP · Allianz Direct



ABOUT XM CYBER

XM Cyber

XM Cyber is the global leader in cyber attack path management The XM Cyber platform enables companies to rapidly respond to cyber risks affecting their business-sensitive systems by continuously finding new exposures, including exploitable vulnerabilities and credentials, misconfigurations, and user activities. XM Cyber constantly simulates and prioritizes the attack paths putting mission-critical systems at risk, providing context-sensitive remediation options.

28 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"Because it offers continuous, automated protection, security issues that would normally take dozens of manual steps to discover are surfaced almost instantaneously. We have historically been compelled to focus pen tests on non-critical areas of infrastructure, as the risk of collateral damage-related downtime was too great. Thanks to XM Cyber's automated testing, this problem was solved, and protection was extended across the entire infrastructure."

JENS MEIER
CHIEF EXECUTIVE OFFICER, HAMBURG PORT AUTHORITY

"I've never seen a tool that visually delivers as much diagnostic information on system technologies-and in a manner that is very easy to see and understand-as XM Cyber. We have immediate visibility into the state of network tools and potential misconfigurations and know what action to take."

MICHAEL BERRY
DIRECTOR OF INFORMATION SECURITY AND CISO, KETTERING HEALTH NETWORK

"Continuous control monitoring empowers us to have full visibility into our network. It is easier for us to manage our cybersecurity assets and understand what has gone wrong within minutes. We are also able to identify any security gaps in our network and this has helped us to ease our daily workload."

ROOTSECURITY

"Continuous control monitoring provides full visibility on the connected, critical infrastructure components and specific security assets, the continuous auditing reflects configuration and security gaps to be closed in a clear and easy to understand way."

PETER VAN LIERDE
CHIEF INFORMATION SECURITY OFFICER, SIBELGA

TRUSTED BY

SANS · HPA Hamburg Port Authority · Plymouth Rock assurance · :rootSECURITY · FC Bayern München e.V.



2024

BREACH & ATTACK SIMULATION SOFTWARE

RISING STAR

featured customers



ABOUT HORIZON3.AI

HORIZON3.ai
~~TRUST~~ BUT VERIFY

The NodeZero™ platform empowers organizations to continuously find, fix, and verify exploitable attack surfaces. It is the flagship product of Horizon3.ai, founded in 2019 by former industry and U.S. National Security veterans. Our mission is to help organizations see their networks through the eyes of the attacker and proactively fix problems that truly matter, improve the effectiveness of their security initiatives, and ensure that they are prepared to respond to real cyberattacks. Reduce your security risk by autonomously finding weaknesses in your network, knowing how to prioritize and fix them, and immediately verifying that your fixes work. NodeZero...

47 TOTAL CUSTOMER REFERENCES

VIEW ALL REFERENCES

FEATURED TESTIMONIALS

"NodeZero is a really great tool for both consultants and pentesters...because for us pentesters, we can use it [NodeZero] kind of like the grunts or infantry of the military...just send it in to go blow everything up and then we [pentesters] can be a scalpel, and really dig into and spend time on the areas where things are potentially bad."

JON ISAACSON
PRINCIPAL CONSULTANT, JTI CYBERSECURITY

"When there is a cyberattack on a PSAP, there is the potential for loss of life due to the caller not being able to get through to the 911 call center. Our job is to prevent that situation. We specialize in knowing the cyber threat actor's tactics, techniques, and procedures (TTPs) so we can protect organizations from those things."

BRIAN BECKWITH
CHIEF TECHNOLOGY OFFICER, INTUITUS

"NodeZero let me do a review of our settings and firewall. Not only did it identify vulnerabilities – it also provided proof showing that they were potentially exploitable and this was incredibly helpful."

SEAN MCKIM
MANAGER OF TECHNOLOGY, REGINA INTERNATIONAL AIRPORT

"NodeZero helps you discover problems you didn't know you had. The product itself is user friendly but the product is 65 or 70 percent of the equation – the team behind it makes it really valuable to me."

BRIAN CAMPBELL
CHIEF INFORMATION SECURITY OFFICER, CITY OF ST. PETERSBURG

TRUSTED BY

Intuitus · Airiam · Moravian University · DRI Desert Research Institute · st.petersburg www.stpete.org