CyberDB
The Cyber Research Databank

Automated breach simulation market

Facts and Emerging Vendors

October 10th, 2017

Contents

1. Introduction

Organizations are investing a significant amount of time and resources building, implementing, improving, and measuring security controls. This investment is expected to continue to increase sharply over the next few years. Gartner estimated a that the spend on information security globally rose well above $80 billion by the end of 2016, Until the end of 2020, the highest growth is expected to come from security testing, IT outsourcing and data loss prevention (DLP). But many professionals feel that the technology sprawl is hampering their efficiency more than it is helping them. The problem isn't lack of tools, it's that the industry is over-investing in a diversity of complex and unwieldy solutions. A typical med-large organization invests in at least 35 different security technologies and hundreds of devices which are potentially effective, but are trapped in silos that limit their capabilities.

In this paper, we focus on key drivers for this market, what are breach and attack simulation technologies, security testing techniques, tools and service offering from emerging vendors, and market overview.

2. Key drivers for the market

- A highly crowded security market generates confusion and makes the selection of security products and services challenging — leaving users unsure of the effectiveness of solutions once they are in place.

- Prioritizing security investment is the biggest challenge of many organizations because vulnerability assessment programs and penetration testing fail to connect risks with business metrics

- Assessing the efficacy of security services is frequently a guessing game with little empirical evidence available to inform decision making and facilitate risk management.

- With digital business, a growing number of solutions rely on APIs, but the market has struggled to offer one single solution to answer all API-security-oriented problems.

3. What are breach and attack simulation technologies

A secure network architecture should follow a defense-in-depth philosophy and be designed with multiple layers of preventive controls. While preventive controls are ideal, detective controls are a must. There is no way to prevent every attack and sometimes preventive controls fail. Even though a firewall is preventing certain traffic from entering the network, if unauthorized traffic is somehow able to subvert these preventive controls it will not be identified if logs are not being collected and reviewed in order to detect an attack. For this reason, it is essential that a comprehensive defense-in-depth architecture include detective controls designed to monitor and alert on anomalous activity.

Detecting intrusions into a network is not accomplished by deploying a single piece of technology. Establishing a well-defined breach and attack simulations exercise program allows organizations the ability to identify malicious or anomalous traffic on the network and determine how the analyst should respond to this kind of traffic (Critical Security Control: 20). When performing this kind of test, it is important to create traffic which mimics current attack methods.

New services have emerged that help organizations to do just that – assessing the effectiveness of security procedures, infrastructure, vulnerabilities and techniques by using breach and attack simulation platform. Such simulations test the vulnerability of your organization for e.g., ransomware attacks, (spear) phishing and whaling attacks, or clicking on malicious banners and links on websites.

Figure 1. Hype Cycle for Threat-Facing Technologies, 2017
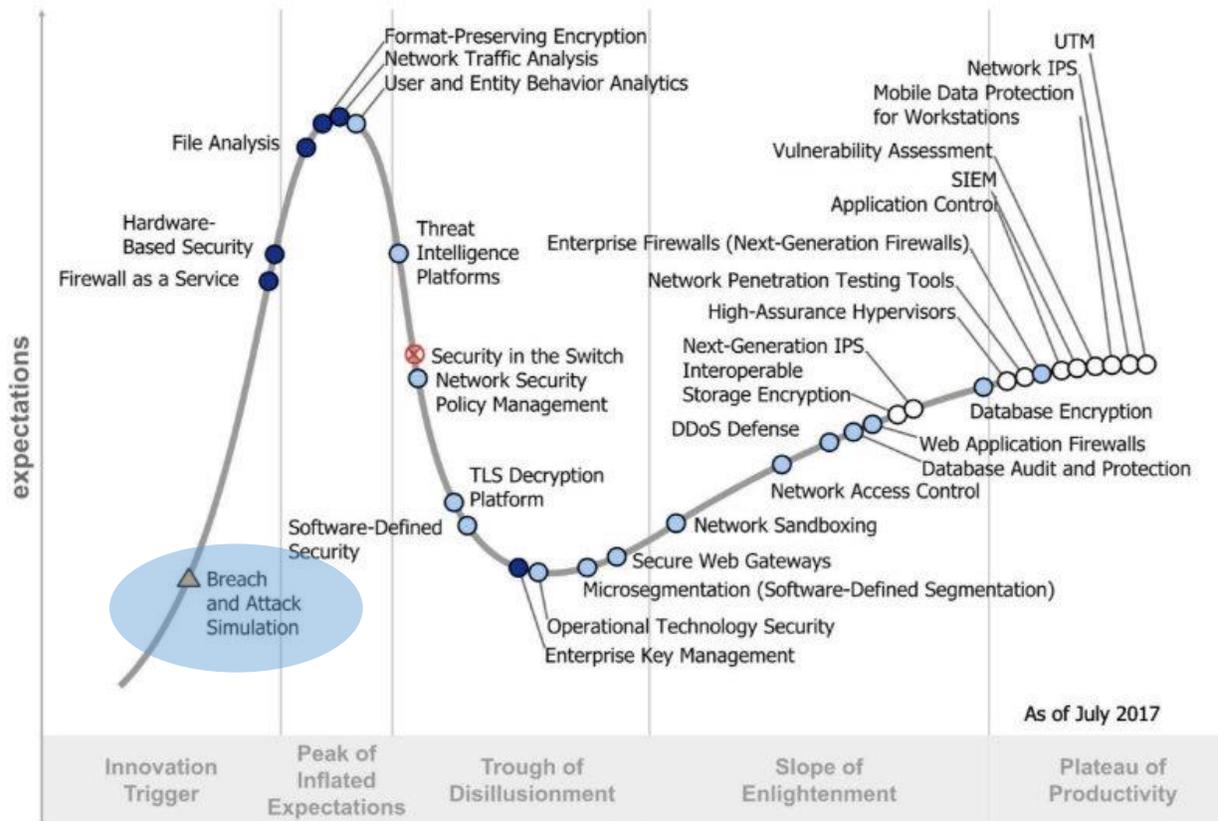
Gartner's Hype Cycle for Threat-Facing Technologies, 2017

These platforms allow organizations to run continuous, on demand cybersecurity simulations at any time without affecting their systems. As a Software-as-a-Service (SaaS) breach and attack platform, it simulates multi-vector, internal or external attacks by targeting the latest vulnerabilities, including those that are in the wild. These simulated attacks expose vulnerability gaps which allows the organization to determine if its security architecture provides the right protection and if its configurations are properly implemented. Overall, breach and attack simulation platforms have become a powerful tool in the arsenal of the organization's security team.

As noted on Gartner's Hype Cycle for Threat-Facing Technologies, 2017 (image 1). "*The ability to provide continuous testing at limited risk is the key advantage of Breach and Attach Simulation (BAS) technologies, which are used to alert IT and business stakeholders about existing gaps in the security posture, or validate that security infrastructure, configuration settings and prevention technologies are operating as intended*".

4. Security testing techniques, tools and service offering from vendors

Other than established and cross-solutions vendors such as Rpaid7 and Qualys, the following emerging vendors offer notable service offering:

1. AttackIQ
2. Cronus
3. Cymulate
4. eSecureVisio
5. SafeBreach
6. Mazebolt
7. ThreatCare
8. Whitehax
9. Verodin

AttackIQ (www.attackiq.com)

San Diego, California based AttackIQ has built a library of over 1,500 distinct attacks that includes contributions from a community of elite security practitioners. Their pre-defined templates called 'FireDrill' allows organizations to test whether their security program (people, process and technology) can prevent or detect attacks that mimic actual cyberattack techniques. The AttackIQ platform automates security assessment by allowing security personnel to either create scenarios or leverage the curated library of existing attack scenarios to continuously attack their environment and expose weaknesses to the security architecture. Scenarios can be made to account for situational differences, such as a laptop connected to the corporate network or used in a public Wi-Fi setting. On-premises deployments are possible if required by client organization.

Security firms are embracing AttackIQ because the platform allows them to validate their product and service claims against a client's actual infrastructure — and not in a simulated environment.

Cronus Cyber (https://cronus-cyber.com/)

Headquartered in Haifa, Israel Cronus Cyber technologies listed on Cybersecurity 500 – hottest cyber company in 2017. Cronus has developed machine based automated pen-testing solution called CyBot. Their attack patch scenario based suite mimic the common patterns of a normal

hacker, allowing companies to simulate penetration scenarios, host's detected vulnerabilities details and recommended remediation. The CyBot has one core engine CyBot Pro, plus two additional management consoles. One for Enterprises and one for MSSPs.

This startup company has large networks of VARs and OEM partners including EMC, Asseco, BT and Ness with commercial partners in Europe and Asia.

Cymulate (www.cymulate.com)

Cymulate is a SaaS based breach and attack simulation platform using advanced technology to allows organization launch simulations of cyber-attacks against themselves, immediately providing them with vulnerabilities and mitigation procedures to close each gap.

The centralized platform allows security testing through multiple attack vectors such as Email, Browsing, Internal Network (Lateral Movement), Human awareness, Data Exfiltration, WAF, EDR and SOC Simulation. Fully-automated and diversified attacks allow for complete security testing anytime, providing organizations with a better understanding of their security posture while continuously improving it.

Cymulate was founded in 2016 by an elite team of former Israel Defense Forces intelligence officers and leading cyber researchers with world-class experience in offensive cyber solutions. Combining vast expertise in cyber simulation technology with extensive field experience to mimic the latest and most sophisticated cyber-attacks. Cymulate employs software-as-a-service applications to simulate the myriad tactics and strategies employed by hackers to attack network and endpoint security infrastructures. This startup headquartered in Israel

eSecureVisio (http://esecure.pl/en)

Founded in 2010 in Rzeszów, Poland, provide IT Governance, Risk management, and Compliance (GRC) solution equipped with an electronic documentation of IT systems, as well as integrated Incident Management, Threat Modelling, Security Auditing and Business Impact Analysis tools. SecureVisio can act as an independent IT GRC solution in an organization or as an intelligent platform to build a Security Operations Center (SOC).

SafeBreach (https://safebreach.com/)

SafeBreach founded in August 2014 and headquartered in Sunnyvale, CA, USA. Their research and development center is in Tel Aviv, Israel. The company is listed on Bloomberg 50 most promising startups in March 2017.

SafeBreach Continuous Security Validation Platform consists of two parts: The Orchestrator (cloud) and Breach Simulators (on-premises). The prices are depending upon no of simulators deployment.

Threatcare (www.threatcare.com)

Threatcare is cloud based SaaS platform that allows proactive cyber threats scanning and simulation solutions for different industry sectors and regulatory compliances. Their platform provides security product evaluation, continuous cyber security controls monitoring, on-demand simulations and security trainings.

The firm is Austin, USA based and founded in 2014.

Mazebolt (https://mazebolt.com)

Mazebolt provide services on DDoS simulations, Phishing awareness programs and Vulnerability scanning. Their SaaS based solution is operational over 70 countries and supporting 20 languages.

The Company headquartered is in Ramat Gan, Israel with international offices is in US, UK and France.

WhiteHaX (http://mvs2i.com/)

IronSDN, Corp. is a Silicon Valley start-up, provide security solution suit called 'WhiteHaX'. This suite is available in different versions such as WhiteHaX network for On-Prim Enterprise and local data-center network security infrastructure effectiveness verification. WhiteHaX End-point for Endpoint security solutions and policy control verification, WhiteHaX Lite for quick security verification of 3rd-party remotely connecting sites (Vendors/Partners/Contractors and remote users), WhiteHaX PVC for testing Private or Public Cloud deployed infrastructure, and WhiteHaX

MSSP or Managed Security Service Providers who perform Pen-testing, Ethical Hacking and other services.

The above solution can be used on premise or in the cloud and it is compatible with AWS, MS Azure, VMWare or OpenStack based public & private Clouds.

»VERODIN™
Security. Instrumented.
Verodin (www.verodin.com)

Verodin headquartered in Reston, VA, USA. Its SaaS based platform called Instrumented Security provides scanning and cyber-attack simulations on endpoint, network and cloud based real production environments. The software agents assume the roles of attacker and target and safely execute real attack behaviors with evidence based reporting. The solution also aggregates the resultant data into meaningful business intelligence dashboards.

The firm is back by leading investors such as Cisco Investments, BlackStone, Rally ventures, ClearSky Power and technology Funds.

5. Market Overview

A key Gartner reveals that "The efficacy of commercial penetration testing is limited because tests require significant human involvement, and are of limited duration and frequency, often only performed annually." According to the Gartner "7 Top Security Predictions for 2017":

1) By 2020, 10% of penetration tests will be conducted by machine-learning-based smart machines, up from 0% in 2016.

2) By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

The Gartner article: Predicts 2017: Threat and vulnerability Management. (Nov 14, 2016, G00316869) predicted following figures:

- Total Cyber industry: $160B in 2020
- Penetration testing: $12B

Based on the above, CyberDB estimates the market the market for automated breach and penetration and simulation to reach the size of $1B by 2020. This includes internal developments and open-source tools.

Market Needs
- Businesses are becoming more and more global and complex, very difficult to test manually.
- The move towards cloud and virtualization makes for a continuously changing network, therefor current security solutions are not built for this environment.

- Regulation and penalization is becoming harsh on large enterprises.

- Security solutions do not take into account business processes

- Annual human PT makes infrequent and outdated PT reports, today a continuous test is needed to keep up with new attack methods

Market Challenges

- Breach and attack simulation technologies are relatively new, and this segment is frequently confused with vulnerability assessment tools. The adoption of scenario-based simulated attacks will require an engaged community.

- The breach and attack simulation technologies is in its infancy. This could be made difficult because of potential confusion around what attack simulation can offer compared to the benefits of vulnerability management and advanced penetration testing.

CyberDB
The Cyber Research Databank

6. Solution Offering of Selected Products

The table below is a competitive analysis for a selected list of vendors in this market.

For wider and deeper analysis, please **contact us**

Common Product Features *(Included in all products)*	Attack IQ	Cronus	Cymulate	SafeBreach	Verodin
Attack Scenario: **Persistence** **Privilege Escalation** **Lateral Movement** **Access to other Data Stores** **C&C** **Ex-filtration**	Agent software deployment for attacking on entire infrastructure with different scenario, over 1,500 distinct attacks	CyBot has one core engine: CyBot Pro, plus two additional management consoles. One for Enterprises and one for MSSPs.	Email, browsing, phishing, WAFs assessments and data ex-filtration, SOC simulations	cloud, network and endpoint simulators, more targeted attack scenarios	cloud, network and endpoint simulators, distributed deception platform

Validation Scenario (Technology Testing)	Test and retest of client network and cyber security measure changes Automated repeatability	Machine-Based Penetration Testing and retesting	Multi-vector validation	automated audit	Compliance verification included
• **Access/Routing /Availability** • **Data Loss Prevention (DLP)** • **Content/Web Filtering** • **Firewall** • **Network and Host IPS/IDS** • **AntiVirus (AV)** • **SIEM** • **SSL Certificates**					
Reporting & dashboards	Assessment / comparison reports	Assessment / comparison reports	Assessment / comparison reports	Assessment / comparison reports	Assessment / comparison reports

CyberDB
The Cyber Research Databank

Solution Model	SaaS platform, monthly subscription	SaaS, 3 BOTs for different clients, monthly subscription	SaaS, SME and Enterprise offering, yearly subscription	SaaS, SME and Enterprise offering, yearly subscription	SaaS, SME and Enterprise offering, yearly subscription

7. About CyberDB

CyberDB (www.cyberdb.co) is the leading global research databank for Cyber solutions and vendors.

CyberDB database includes over 1,400 vendors and 5,700 products, categorized into 8 main cyber categories and 146 sub-categories. The company publishes market researches and summaries on bi-weekly basis on cyber categories.

The database is being used by VC's, multinationals, CISO's and system integrators worldwide to help them navigate through the dynamic cyber landscape.

In addition, CyberDB offers its customers Consulting Services for Cyber Product Strategy, Cyber Technology Scouting and tailored Market researches.

CyberDB is established by the founders of Stratechy, strategy consulting practice that has been working with management teams of Hi-Tech vendors to shape their product strategy turn-around and design and execute their Go-To-Market plan

Among its customers, are NEC Corporation, Samsung, Rafael, Amdocs, Nice, Adallom (Microsoft), Brother, Cyberbit (Elbit) and S21Sec

Please contact CyberDB at **info@cyberDB.co** or visit us in **www.cyberdb.co**, on **Twitter** or **LinkedIn**