White Paper

Data Breach Assessment

Continuous, Accurate, Automated Assessment of Security Vulnerabilities

Introduction

There has been a steady rise in the number of data breaches over the past few years. The costs of a breach are also on an upward spiral. In 2019 more than 5,200 data breaches occurred1, exposing more than eight billion records. The total hard-dollar costs of a data breach averaged $3.92 million[2]—not including opportunity costs such as delayed strategic initiatives, missed market windows, GDPR and other compliance violations, or a tarnished reputation for the company.

Why do enterprises of all types and sizes, in every industry sector and every geography, continue to fall victim to data breach attacks? Why do attacks continue to succeed despite advancements in security technology and ever-increasing security budgets? Business leaders and security teams alike find these questions increasingly vexing, and clearly a more effective solution is urgently needed—one that isn't based on reactive strategies.

This paper cites the key reasons data breaches still succeed and provides an overview of a new approach that has proven extremely effective in allowing organizations to continually assess and validate their security posture: CyberFlood Data Breach Assessment.

Data Breach Assessment

Continuous, Accurate, Automated Assessment of Security Vulnerabilities

Limitations of Traditional Security Assessments

Assessing the security posture of an organization typically involves three traditional approaches. Each provides important capabilities, but even a combination of the three continues to fall short of delivering the comprehensive coverage required to protect against data breaches:

- **Pentesting (Red team assessments):** These assessments are specific to a point in time and typically do not recur often enough to provide true visibility into the ever-changing threat landscape. They also require human interaction, which can lead to delays and errors in the actual assessment.
- **Defensive approach (Blue team assessments):** While they add value to pentesting, defensive assessments can only be run in conjunction with Red Team assessments, which means they are still not frequent enough and can be very costly.
- **Hybrid approach (Purple team assessments):** Purple Team combines the offensive strategies of Red teams and defensive aspects of Blue teams to mimic the complexity of the real world but cannot provide a complete or continuous vision of the threat landscape.
- **Commercial simulation-based products:** These solutions replay previously captured traffic, sometimes in the form of a packet capture, leading to unrealistic assessments, a false sense of security, and potentially false positive results.

Advantages of an Emulation-based Approach

CyberFlood Data Breach Assessment combines and enhances the traditional approaches described above while also adding new capabilities, enabling security operations teams to identify and address weaknesses in security before attackers do.

Unlike other "Breach and Attack Simulation" (BAS) solutions, CyberFlood Data Breach Assessment is based on full stack emulation of attacks and other assessment traffic rather than simulation that may employ basic packet transfer. The distinction is that emulation replicates attack scenarios precisely, from the ground up, using real attack vectors. Simulation only "resembles" such a scenario and will not necessarily provide an accurate view of security coverage. Solutions that leverage simulation techniques (such as pcap replay) can potentially lead to incorrect results and a false sense of security.

Attacks, malware and other malicious content come in many forms and to circumvent security counter measures hackers use evasions techniques to mask or obfuscate content to avoid detection. This means one attack can instantly become many variants that are more difficult to mitigate. Assessing with evasions techniques can change the outcome of the results providing more visibility allowing you to harden your security defenses. In addition, with over 85%* of internet traffic encrypted it is imperative to asses attacks, malware and applications scenarios through security solutions over TLS encrypted flows, which places further pressures on security solutions ability to identify malicious traffic.

Using emulation, security teams can safely assess the organization's security posture with real attacks, malware, and data loss prevention (DLP) scenarios on the live production network, eliminating the false positives of simulated attacks. They can emulate attack propagation and pivoting behavior to get a more accurate assessment of complex security countermeasures, which in turn enables them to fine-tune security policies—more frequently and more completely.

Simply put, they can validate all techniques across all attack vectors, including exploits and malware, to confirm the organization's security solutions and prevent policies from being easily by passed.

**Google Encryption Transparency Report Jan 2020.*

CyberFlood Data Breach Assessment: Core Capabilities

CyberFlood Data Breach Assessment is emulation-based and proactively provides accurate, continuous, thorough, and automated assessment of the organization's security posture. It expands on the proven capabilities of CyberFlood, a test solution that generates realistic application traffic and attacks to test the performance, scalability and security of today's application-aware network infrastructures. CyberFlood Data Breach Assessment delivers the following capabilities:

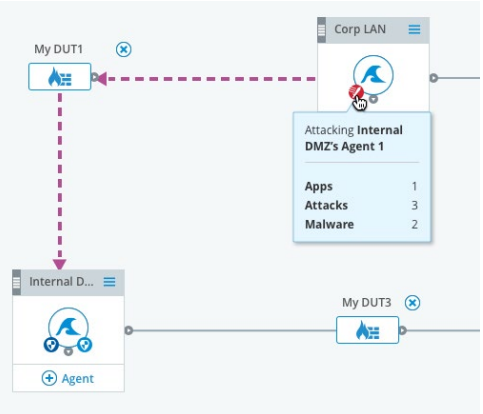
Accuracy through tens of thousands of continuously updated threat scenarios

The solution leverages a wide range of constantly updated threat intelligence feeds, including:

- **Applications** ranging from Netflix to Salesforce to Skype, allowing security teams to validate app ID policies
- **Attacks & exploits** targeting known vulnerabilities, enabling teams to verify IDS/IPS security coverage
- **Malware threats** including near zero-day scenarios, so teams can verify malware prevention capabilities
- **Application, attacks and malware over TLS**, validate inspection policies for scenarios that are hidden via encryption
- **Sensitive Data** emulation, including corporate intellectual property and customer protected data, allowing teams to ensure critical data does not escape your organization's filters and advanced networks data loss prevention policies

Comprehensive, automated assessment capabilities—from the security perimeter to the endpoint

CyberFlood Data Breach Assessment creates thorough assessments between lightweight Spirent CyberFlood Virtual (CFV) Agents at critical intersections within the network infrastructure. It defines a network topology, including network zone details, allowing teams to find security issues and gauge security efficacy. CFV agents can be installed on desktop hypervisors for Windows™ or Macintosh™ to allow assessment points to be easily deployed in branch offices or specific network segment locations.



CyberFlood Data Breach Assessment can leverage knowledge of zones to tailor its executed exploits and malware to your environment.

The solution automatically analyzes logs and correlates them to the assessment's security events, and submits issues discovered into the most popular incident tracking systems such as ServiceNow, JIRA, and ZenDesk. This gives teams a complete, end-to-end assessment including traceability from issue detection to resolution.

In additional to assessing inline security devices such as a next generation firewalls, IDS/IPS and other solutions CyberFlood Data Breach Assessment can assess representative end points, such as Windows laptops/severs, to validate the last line of a network's defense capabilities of mitigating attacks. This provides a complete end-to-end holistic level of security posture visibility.

Data Breach Assessment

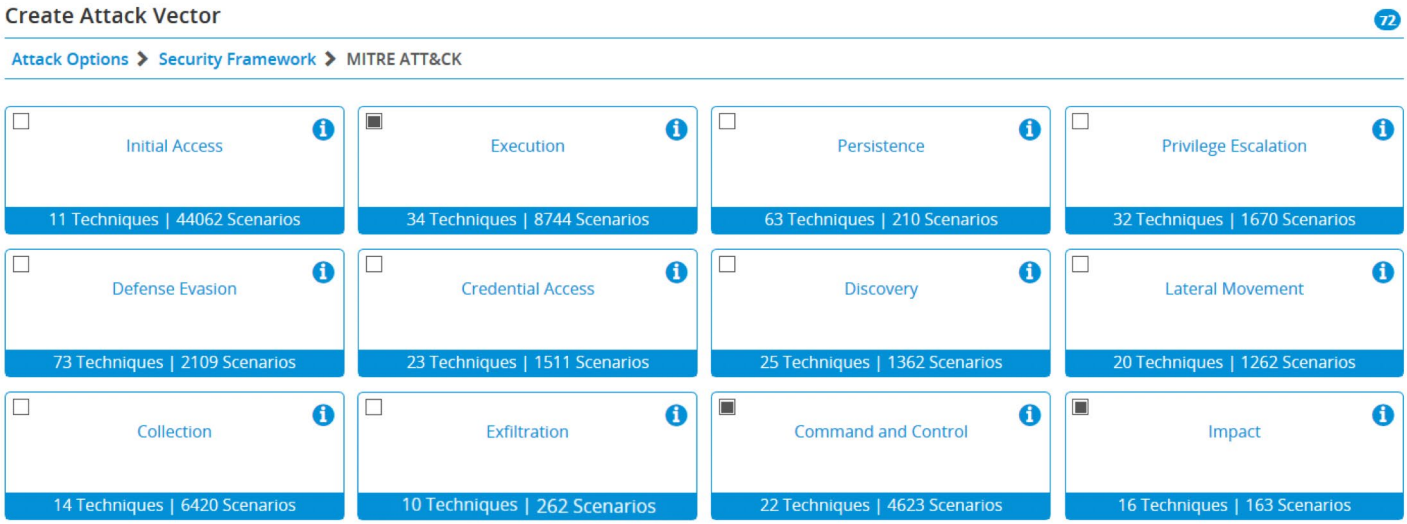
Continuous, Accurate, Automated Assessment of Security Vulnerabilities

Active monitoring assesses security impact, limits impact on users

With CyberFlood Data Breach Assessment, security teams can generate legitimate, hyper-realistic emulated traffic for the same services they are protecting, enabling teams to assess the impacts of security in real time.

The solution also identifies security policies that degrade performance without providing additional security coverage, so teams can make changes and verify the balance between performance and security continuously.

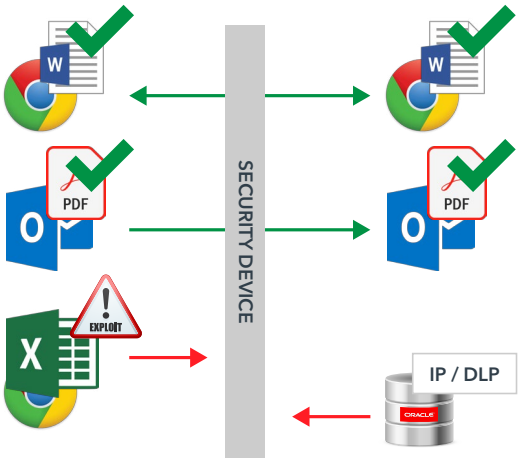
Reporting is extensive showcasing the net results of the security kill chain in action including standard CyberFlood reporting, MITRE ATT&CK framework support for both the creation and results of an assessment and NetSecOPEN assessment that can be configured in minutes.



Easily create assessments based on MITRE ATT&CK tactic vectors.

Secures communications without compromising them

CyberFlood Data Breach Assessment enables teams to verify that security solutions don't just block all files of that filetype but actually inspect them to stop the malicious ones without impact to the user's daily work.



CyberFlood Data Breach Assessment enables teams to verify data loss policies across filetypes and network vectors.

Actual files sets are created on-the-fly or users can upload representative files types for specific assessment needs. Teams can also validate that intellectual property and other sensitive file content, such as social security numbers and credit card numbers, does not leave the network.

Deployment and Use

CyberFlood Data Breach Assessment is specifically designed for ease of use and is intended for IT, security operations, and incident response teams with experience in network security, network operations and associated management tools and services. This section provides additional detail about the deployment process, features and functionality, and reporting capabilities.

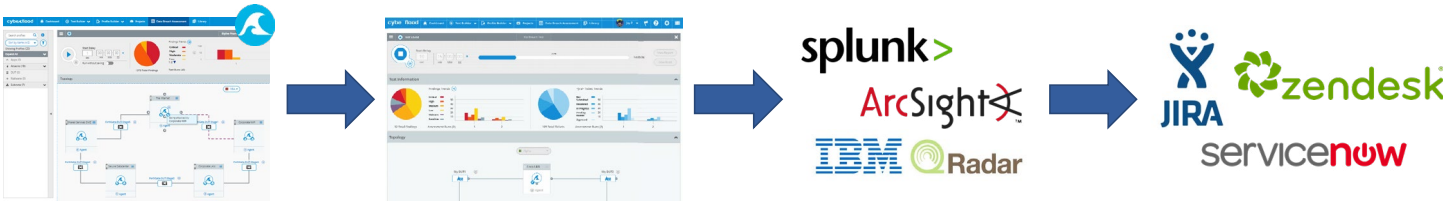
Implementation process and requirements

Customers will leverage Spirent's SecurityLabs team to ensure efficient and accurate installation and maximum customer satisfaction. It is not necessary for customers to engage with Spirent Professional Services; however, it is advisable that a systems administrator from the customer's organization participate in the installation process and provide proper credentials and authorization to the APIs of specific SIEM and IT systems.

For maximum benefit, CyberFlood Data Breach Assessment will need to interface with central logging services (e.g. SIEM). There is no specific integration required with firewalls or other devices assessment traffic will be running through. All management communication is done over encrypted channels to ensure that any content used in the assessment process cannot be used for any unauthorized purposes.

Test traffic: sources and call-flow

The malware samples and applications tested by CyberFlood Data Breach Assessment are fully emulated; they look and behave like malicious or legitimate traffic. However, when an assessment is executed only Spirent CyberFlood Virtual Agents are sent and targeted to complete the messaging exchange. No user's end system is compromised or infected. The workflow for assessing live networks is illustrated below.



Build network topology including zone details

Run Data Breach Assessment to find security issues

Collect logs and correlate to security events generated

Populate found issues in external tracking system

CyberFlood Data Breach Assessment leverages Spirent Threat Research in enterprise production networks and assesses live networks from user login to end results.

Data Breach Assessment

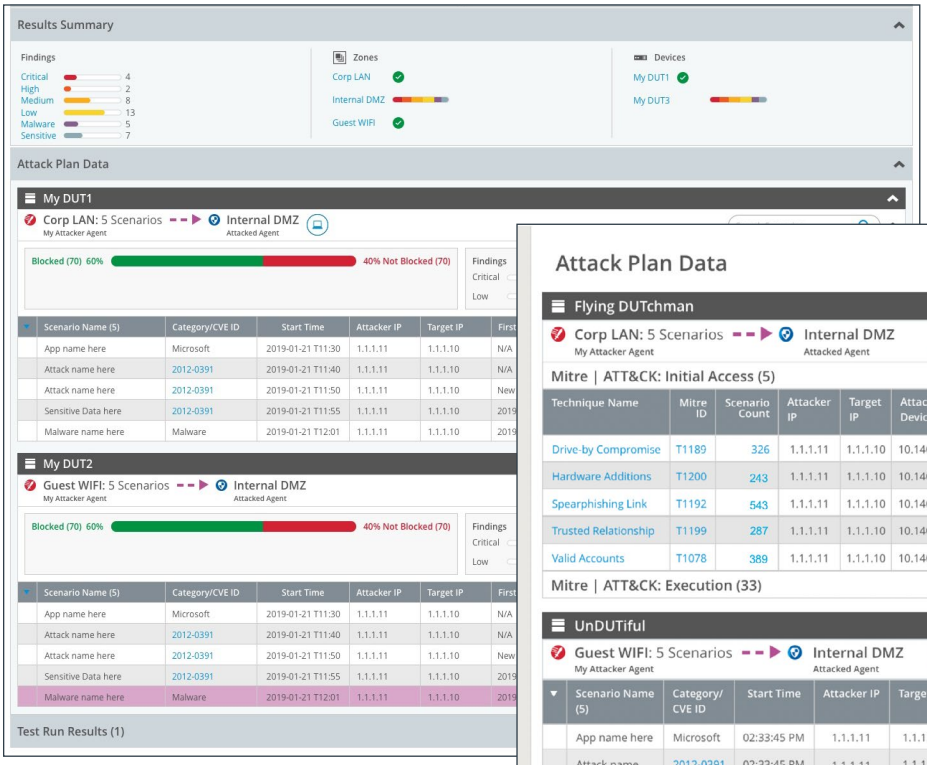
Continuous, Accurate, Automated Assessment of Security Vulnerabilities

CyberFlood Data Breach Assessment agents are similar to CyberFlood Virtual endpoints and are managed and updated the same way. They are easily installed on premises or on compatible cloud environments such as AWS and Azure, and customers can log in to an administration shell of these agents. The agents are given a range of IPs to work in an assessment and create message/call flows between them. This appears as actual traffic in the devices it passes through, thus stressing the inspection and policy engines of devices under test under real-time network traffic conditions. Since CyberFlood Data Breach Assessments are done in the live network, devices that have been servicing traffic for long periods are put under added pressure of deflect attack, malware and other policy validation; this can expose weaknesses in solutions that may start to falter or become erratic after excessive uptime.

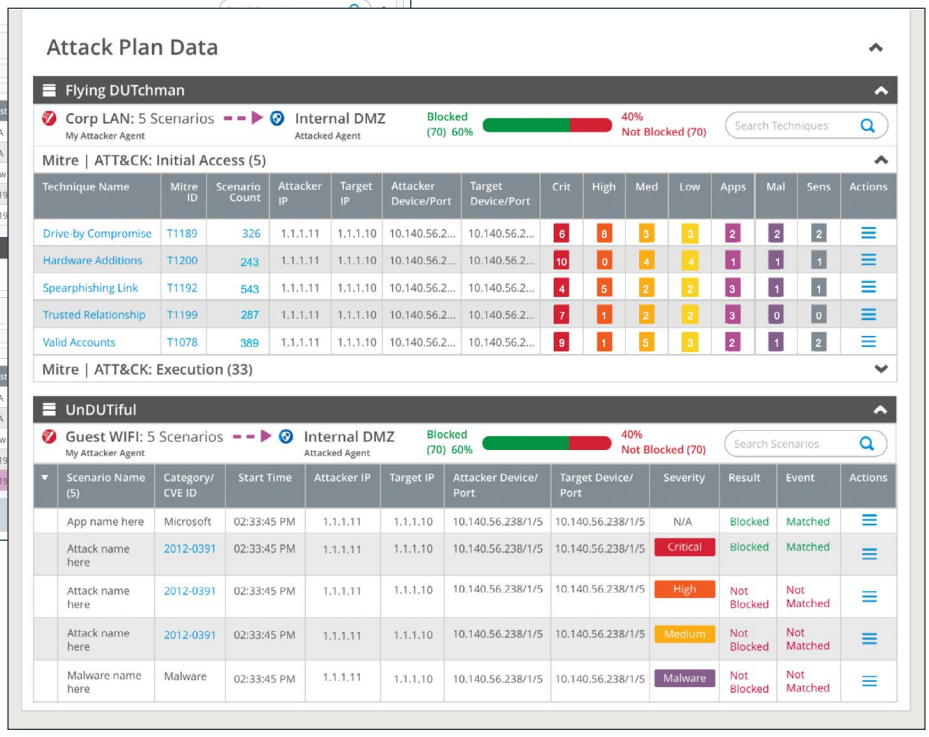
CyberFlood Data Breach Assessment also allows assessments to be scheduled at specific times and days. Security mitigation effectiveness may be impacted when the network is under busy time of the day or shift changes.

Attack malware and other traffic samples are stored in the TestCloud database. Depending on the severity, a zero-day attack or malware sample can be added to TestCloud and made available within hours. As an example, WannaCry and Petya samples were added within 24 hours after their discovery.

If a customer has the pcap of a specific attack or malware they want tested, they can import it into CyberFlood Data Breach Assessment for on-the-wire stateful recreation, or request that Spirent prioritize the request to be added to the database. TestCloud content is published on monthly basis; however, CyberFlood Data Breach Assessment checks for updates every 15 minutes and any content published outside of normal schedules will be downloaded and made available for immediate use in an assessment.



Detailed Live Results



MITRE ATT&CK Framework Reporting

Network discovery and log analysis

For network discovery, CyberFlood Data Breach Assessment uses industry-standard methods to identify listening IPs, the operating systems using those IPs, and the services and applications those operating systems are hosting to create assessment cases that are best fit for the network zones that CyberFlood Virtual agents are deployed in.

CyberFlood Data Breach Assessment analyzes security events from the device logs sent to the SIEM participating in the assessment. It performs assessment of traffic malware, attacks, application DLP fingerprinting (IP + Port address, time stamp, device ID) to correlate events in SIEM logs.

Results and reporting

All assessment data and results are stored on the CyberFlood Data Breach Assessment controller, which has user access policy setup by the account administrator, so test results are protected from general visibility. Assessment reports can be exported as PDF files; however, emails are used as notification only (CyberFlood Data Breach Assessment will not automatically send end-of-assessment results). In additional, CyberFlood Data Breach Assessment does not lock users into a specific framework and supports MITRE ATT&CK and NetSecOPEN frameworks providing maximum reporting flexibility.

Remediation

CyberFlood Data Breach Assessment provides valuable visibility on security holes and vulnerabilities. When an attack gets through a device's counter measures Data Breach Assessment can provide specific guidance for a growing list of compatible solutions to quickly update device policy settings and remediate found issues.

Licensing

CyberFlood Data Breach Assessment is available only as a subscription offering. There is a one-year minimum, with reduced pricing if multiple years are purchased up front. Packaged options are available for a variety of implementation scenarios and scales of assessments. Licenses are installed and managed on the CyberFlood Data Breach Assessment controller.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

Conclusion

CyberFlood Data Breach Assessment is designed to simplify and streamline assessment of security vulnerabilities and provide users with information to harden network security policies. By harnessing an emulation approach and providing continuous, accurate assessment, it enables security teams to find the holes in protections before attackers do. It also provides clarity and confidence in the enterprise's security posture, and by extracting complexity from data breach assessments it unburdens teams of very time-consuming activities so they can focus on addressing holes in the threat landscape.

For additional information about Spirent and the CyberFlood Data Breach Assessment, visit www.spirent.com/go/cyberflooddba.

Contact us for more information, call your Spirent sales representative, email spirentsecurity@spirent.com or visit us on the web at www.spirent.com/ContactSpirent.

1 Source: Dark Reading
2 Source: Ponemon Institute.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

US Government & Defense
info@spirentfederal.com | spirentfederal.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com