

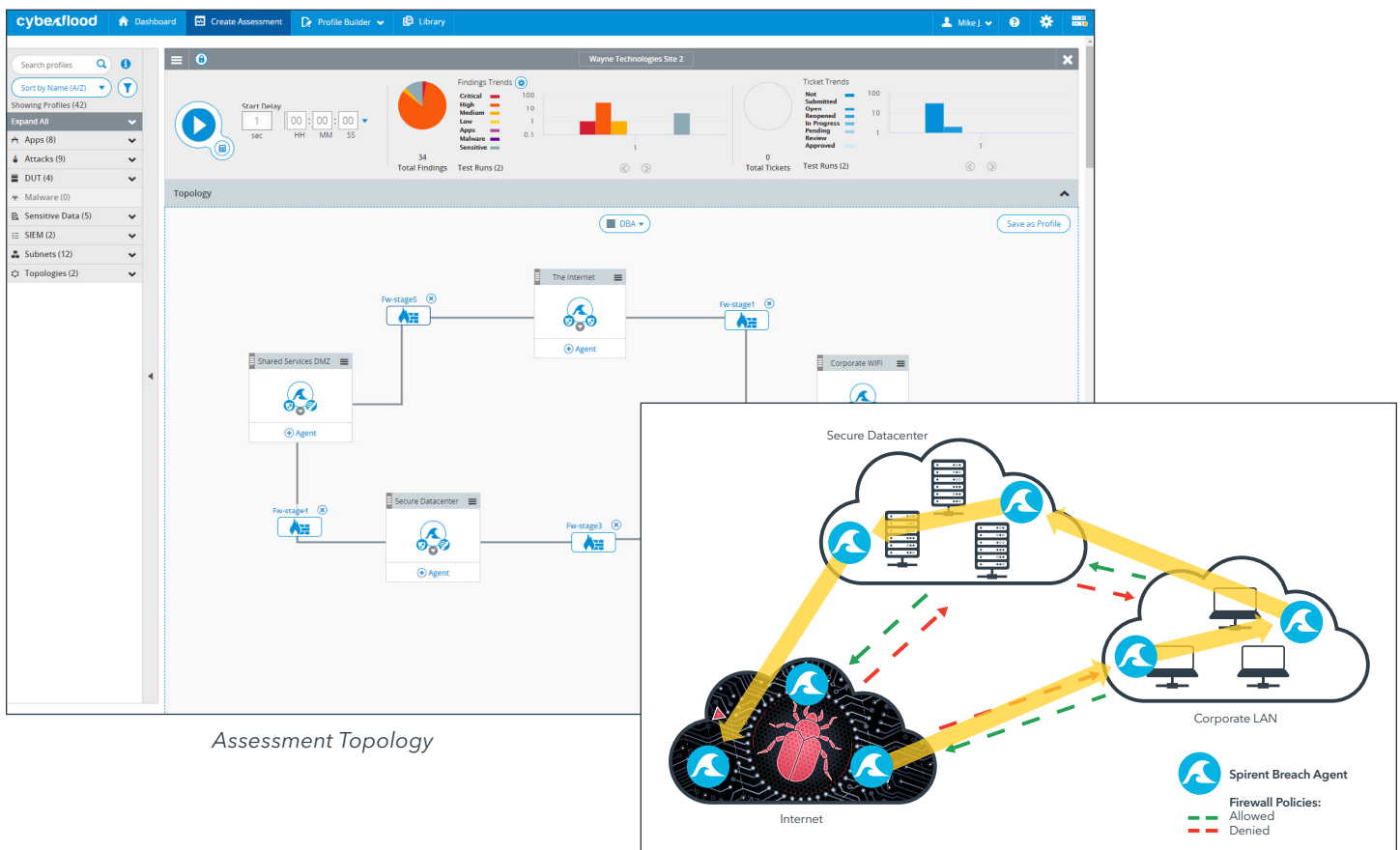
# Spirent **CyberFlood Data Breach Assessment**

## Hyper-Realistic, Continuous Assessment of Your Threat Landscape

Data Breach Assessment delivers accurate, automated, continuous and thorough assessment of live production network environments, using an always-up-to-date database of hyper-realistic attack, malware, data loss prevention, and applications scenarios to safely and accurately validate your security infrastructure and policies.

This powerful solution combines the concepts of Red Team penetration testing and Blue Team defensive testing and automates them into Purple Team assessments—and ties directly into your SIEM and incident response systems, giving you the best indication of how robust your security posture actually is. This enables your security operations teams to identify and address weaknesses in your security—before attackers do.

Business leaders and security teams require a more effective solution for finding, fixing, and preventing data breach attacks. In 2018 more than 5,200 data breaches occurred, exposing more than eight billion records—at an average cost of \$3.86 million<sup>1</sup> per breach. CyberFlood Data Breach Assessment simplifies assessment of the organization’s security posture using an emulation-based approach. It goes beyond the capabilities of traditional Breach and Attack Simulation (BAS) solutions by combining and adding value to Red Team, Blue Team, and Purple Team assessments, and it draws on continuously updated threat intelligence and Spirent’s decades of expertise in testing and assessment.



1) Source: Ponemon Institute, 2018.

## Advantages of an Emulation-based Approach

CyberFlood Data Breach Assessment emulates attacks and other assessment traffic rather than relying on simulation. Emulation replicates attack scenarios precisely, using real attack vectors. Simulation, usually relying on simple pcap replay techniques, only “resembles” such scenarios and will not necessarily provide an accurate view of security coverage, potentially leading to incorrect results and a false sense of security.

Using hyper-realistic emulation, security teams can safely assess the organization’s security posture with real attacks, malware, applications, and sensitive data (for DLP assessment) on the live production network, eliminating the false positives of simulated attack and other scenarios. 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. They can validate all techniques across all attack vectors, including exploits and malware, to confirm the organization’s security solutions and policies cannot be easily bypassed.

**Results Summary**

**Findings**

- Critical  4
- High  2
- Medium  8
- Low  13
- Malware  5
- Sensitive  7

**Zones**

- Corp LAN
- Internal DMZ
- Guest WiFi

**Devices**

- My DUT1
- My DUT3

**Attack Plan Data**

☰ My DUT1

✖ Corp LAN: 5 Scenarios
 ➔
🔍 Internal DMZ
 🏠

🔍

Blocked (70) 60%  40% Not Blocked (70)

**Findings**

- Critical  0
- High  1
- Medium  0
- Low  0
- Malware  1
- Sensitive  1

Scenario Name (5)	Category/CVE ID	Start Time	Attacker IP	Target IP	First Reported	Issue Status	Severity	Result	Event	Actions
App name here	Microsoft	2019-01-21 T11:30	1.1.1.11	1.1.1.10	N/A	N/A	N/A	Blocked	Matched	☰
Attack name here	2012-0391	2019-01-21 T11:40	1.1.1.11	1.1.1.10	N/A	N/A	Critical	Blocked	Matched	☰
Attack name here	2012-0391	2019-01-21 T11:50	1.1.1.11	1.1.1.10	New	⚠ Not Submitted	High	Not Blocked	Not Matched	☰
Sensitive Data here	2012-0391	2019-01-21 T11:55	1.1.1.11	1.1.1.10	2019-01-21 T12:01	Open	Sensitive	Not Blocked	Not Matched	☰
Malware name here	Malware	2019-01-21 T12:01	1.1.1.11	1.1.1.10	2019-01-21 T01:34	⚠ Reopened	Malware	Not Blocked	Not Matched	☰

☰ My DUT2

✖ Guest WiFi: 5 Scenarios
 ➔
🔍 Internal DMZ
 🏠

🔍

Blocked (70) 60%  40% Not Blocked (70)

**Findings**

- Critical  0
- High  1
- Medium  0
- Low  0
- Malware  1
- Sensitive  1

Scenario Name (5)	Category/CVE ID	Start Time	Attacker IP	Target IP	First Reported	Issue Status	Severity	Result	Event	Actions
App name here	Microsoft	2019-01-21 T11:30	1.1.1.11	1.1.1.10	N/A	N/A	N/A	Blocked	Matched	☰
Attack name here	2012-0391	2019-01-21 T11:40	1.1.1.11	1.1.1.10	N/A	N/A	Critical	Blocked	Matched	☰
Attack name here	2012-0391	2019-01-21 T11:50	1.1.1.11	1.1.1.10	New	⚠ Not Submitted	High	Not Matched	Not Matched	☰
Sensitive Data here	2012-0391	2019-01-21 T11:55	1.1.1.11	1.1.1.10	2019-01-21 T12:01	Open	Sensitive	Not Matched	Not Matched	☰
Malware name here	Malware	2019-01-21 T12:01	1.1.1.11	1.1.1.10	2019-01-21 T01:34	⚠ Reopened	Malware	Running...	Running...	☰

**Test Run Results (1)**

Detailed Live Results

## Features and Benefits

- **Assessment based on reality:** Generates realistic security assessment traffic on the exact services the organization is protecting. Emulates attack propagation and pivoting behavior to provide an accurate assessment of complex security countermeasures, enabling teams to fine-tune security policies more frequently and more completely.
- **Continuously updated threat intelligence:** Leverages a wide range of constantly updated threat intelligence feeds, including with tens of thousands of relevant and zero-day scenarios:
  - **Applications:** including popular applications from Netflix to Salesforce to Skype, allowing security teams to validate app ID policies.
  - **Attacks & exploits:** targeting known and unknown vulnerabilities, enabling teams to verify IDS/IPS security coverage.
  - **Malware threats:** including near zero-day scenarios, so teams can verify malware prevention capabilities.
  - **Sensitive data emulation:** by automatically creating sensitive data file sets (or users can upload custom content) allows teams to ensure critical data does not escape your organization's filters and advanced networks data loss prevention policies.
  - **Secure team management:** Organize and control access to assessments, results, and data to be seen and used by selected members or groups. This protects sensitive results details and which individuals are allowed to create and execute assessments.
- **Comprehensive assessment of production networks:** Creates complete, automated assessments between lightweight Spirent CyberFlood Virtual (CFV) Agents at critical intersections within your network infrastructure.
  - **Defines a network topology,** including network zone details, allowing you to find security issues and gauge security efficacy. Automatically analyzes logs and correlates them to the assessment's security events and SIEM systems such as Splunk, Elasticsearch and others.
  - **Submits and tracks discovered issues** into popular issue tracking systems such as ServiceNow, JIRA, and ZenDesk.
  - **Automatically creates assessment profiles** with our exclusive reconnaissance mode to fingerprint and map network zone services and other information to create the most appropriate attack/malware set from our ever growing threat intelligence feed.
- **From assessment to remediation:** CyberFlood Data Breach Assessment provides complete end-to-end visibility, including traceability from issue detection to security device remediation guidance.
- **Limits the impact to users:** Identifies security policies that degrade performance without providing additional security coverage, so teams can make changes and verify performance and security continuously.
- **Draws on our experience:** The solution leverages many years of security content cultivated by Spirent's Threat Research and SecurityLabs teams.
- **Proven solution from a reliable partner:** Expands on the proven capabilities of CyberFlood, the powerful, easy-to-use test solution that tests the performance, scalability and security of application-aware network infrastructures.

## Key Differentiators

- First solution to use emulated assessment traffic that accurately recreates stateful attacks, malware, sensitive data, and application scenarios
- First solution to perform ongoing Data Loss Prevention (DLP) assessments
- Leverages advanced threat intelligence for realistic assessment with zero-day attack and malware scenarios
- Provides remediation guidance for specific platforms and services based on assessment event details
- Automatically creates assessment profiles from our database of tens of thousands of attack and malware scenarios based on fingerprinting network zone details
- Combines, expands and automates the value of Red, Blue, Purple teams
- Creates comprehensive assessments between lightweight Spirent CyberFlood Virtual (CFV) Agents at critical intersections within the network infrastructure
- Easily defines network topologies, including network zone details, allowing teams to find security issues and gauge security efficacy
- Evasion techniques can be used to further prove security solutions can detect attacks under the most adverse of conditions
- Associate data to logs, automatically analyze logs and correlates them to the assessment's security events and SIEM systems such as Splunk, Elasticsearch and others
- Spirent: agility and innovation of a start-up, resources of a major enterprise

For additional information about Spirent and the CyberFlood Data Breach Assessment, visit [www.spirent.com/go/cyberfloooddba](http://www.spirent.com/go/cyberfloooddba).

Contact us for more information, call your Spirent sales representative, email [spirentsecurity@spirent.com](mailto:spirentsecurity@spirent.com) or visit us on the web at [www.spirent.com/ContactSpirent](http://www.spirent.com/ContactSpirent).

---

### Contact Us

For more information, call your Spirent sales representative or visit us on the web at [www.spirent.com/ContactSpirent](http://www.spirent.com/ContactSpirent).

[www.spirent.com](http://www.spirent.com)

© 2019 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name "Spirent" and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice.

Americas 1-800-SPIRENT  
+1-800-774-7368 | [sales@spirent.com](mailto:sales@spirent.com)

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

Asia and the Pacific  
+86-10-8518-2539 | [salesasia@spirent.com](mailto:salesasia@spirent.com)