Data Sheet

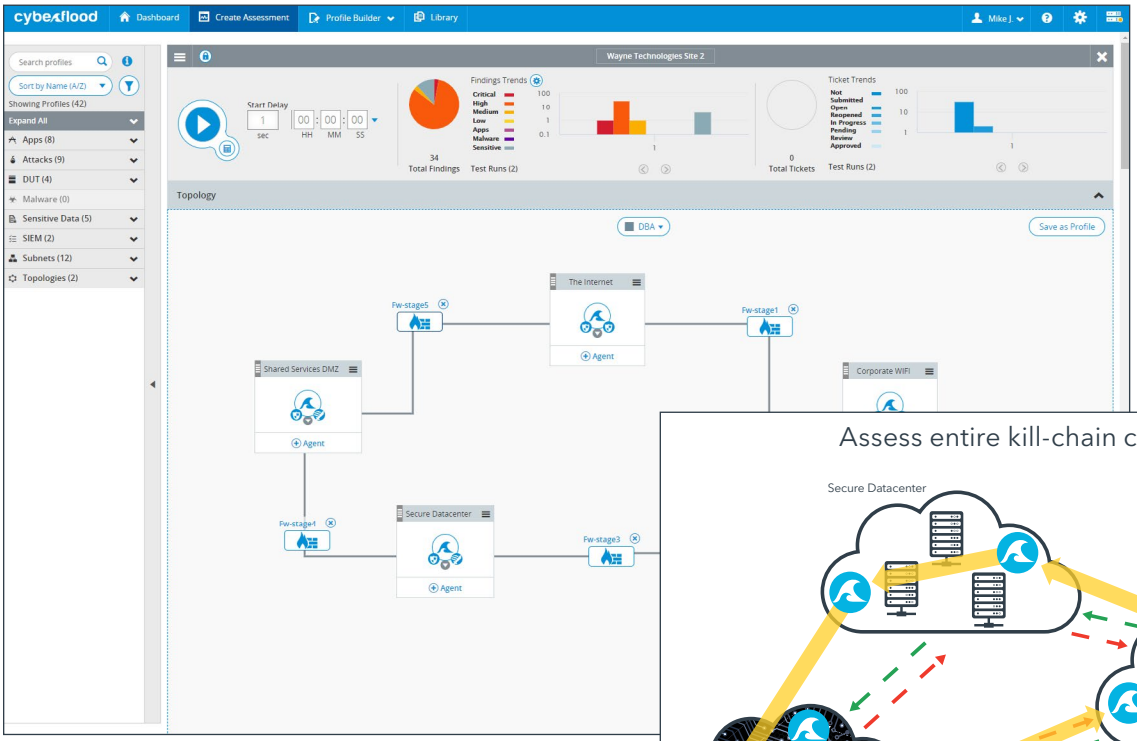
Spirent **CyberFlood Data Breach Assessment**

Hyper-Realistic, Continuous Assessment of Your Threat Landscape

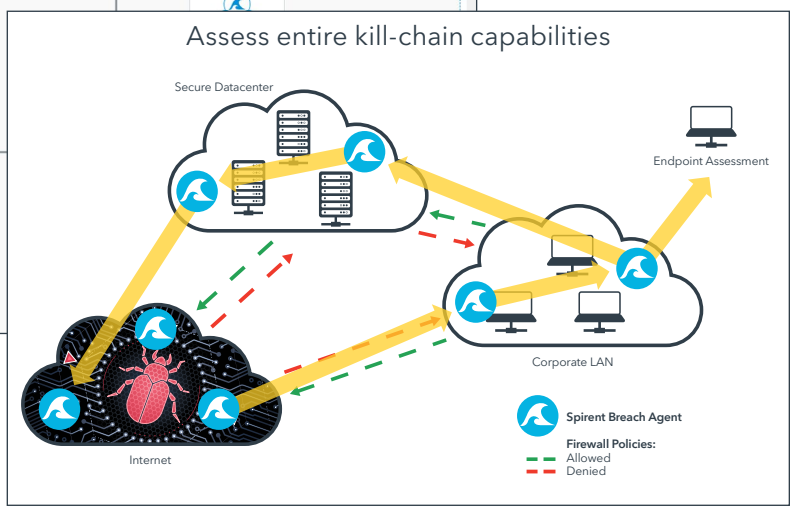
CyberFlood Data Breach Assessment delivers accurate, automated, continuous and thorough assessment of live production network environments, using an always-up-to-date database of hyper-realistic attack, malware, data loss prevention, and applications scenarios to safely and accurately validate your security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

This powerful solution 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 2019 more than 5,200 data breaches occurred, exposing more than eight billion records—at an average cost of $3.92 million[1] 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 emulating the true behavior of legitimate and malicious assessment scenarios (including encrypted attacks and malware), and it draws on continuously updated threat intelligence and Spirent's decades of expertise in testing and assessment.



Assessment Topology

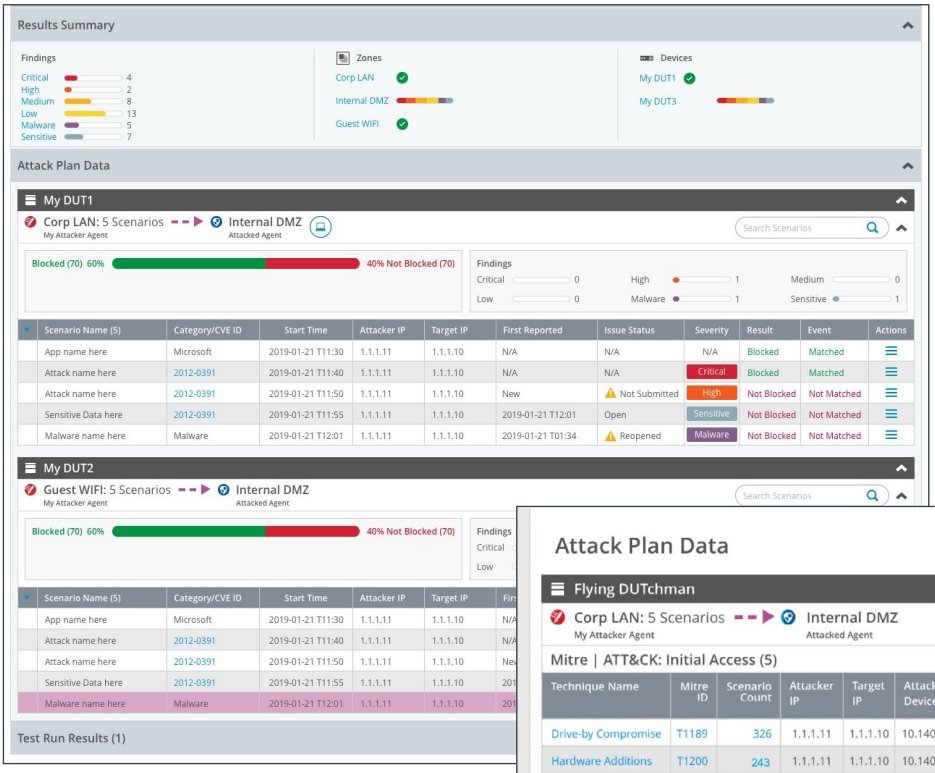


1) Source: Ponemon Institute, 2019.

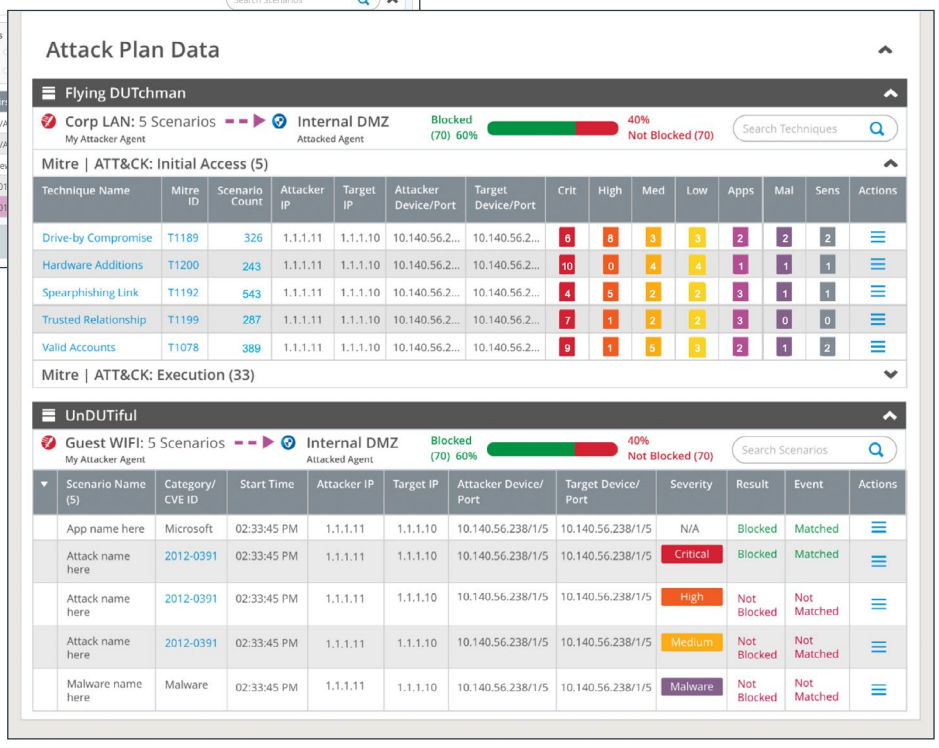
Advantages of an Emulation-based Approach

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 on top of emulation structure, we employ real hacker behavior—emulating 1000's of attack permutations via evasion techniques and scenarios over encryption, challenging security solutions in the most realistic, yet production-safe manner possible. 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.



Detailed Live Results



MITRE ATT&CK Framework Reporting

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.
- **MITRE ATT&CK and Other Security Frameworks:** Data Breach Assessment now incorporates a multitude of reporting and assessment authoring. This included the MITRE ATT&CK framework, which provides assessments that utilize hacker techniques based on real world threat models and exploit scenarios. In addition, Data Breach Assessment provides NetSecOPEN security framework, providing flexible reporting for maximum security visibility.
- **Endpoint assessment:** Easily validate your last line of defense by adding representative endpoints, such as a windows laptop/server, to verify company endpoint security defense profiles - prior to major corporate wide endpoint defense updates.
- **Expanded CyberFlood agent deployment options:** Users can now quickly install agents on desktop hypervisors (e.g. Windows/Mac) to quickly create assessment points in the corporate network or specific network segments.
- **Hacker Behavior:** Easily add numerous evasion techniques to an assessment to put further pressure on the security architecture to attempt to bypass mitigation policies.
- **Extensive API Interface:** CyberFlood Data Breach Assessment is built on an API driven framework allowing customers ultimate flexibility in deployment. Standard deployment options include software deployed by customers or managed service by Spirent or a trusted partner, with the flexibility to switch deployment options as an organization's needs change. For more complex environments, APIs can be leveraged to incorporate the solution into existing frameworks and user interfaces.
- **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, including Single Sign On (SSO) compatibility. This protects sensitive results details and which individuals are allowed to create and execute assessments.
  - **Custom traffic:** Allows users to import their own application or attack traffic to recreate scenarios that are unique to specific environments.
  - **Encrypted traffic:** Users can quickly change any TCP based attacks or malware to be sent over TLS encrypted flows, this greatly challenges mitigation services ability to detect malicious content.
- **Comprehensive assessment of production networks:** Creates complete, automated assessments between lightweight Spirent CyberFlood Virtual (CFV) Agents at critical intersections within your network infrastructure or compatible cloud environments such as AWS and Azure.
  - **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.
- **Remediation:** Provides direct policy remediation guidance on attack and malware incidents found during an assessment for a growing list of compatible security solutions.
- **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.

Only solution that allows you to assess with attack and application scenarios over encryption.

First solution to perform ongoing Data Loss Prevention (DLP) assessments.

Leverages advanced threat intelligence for realistic assessment wth 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 finger printing network zone details.

Only solution that allows you to assess with real-world hacker techniques such as evasions and attacks/malware over encryption.

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.

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.

Draws on our experience: the solution leverages many years of security content cultivated by Spirent's Threat Research and SecurityLabs teams.

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.

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

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

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

Rev E | 02/20