Spirent **CyberFlood Data Breach Assessment**

The simple way to find and fix your security vulnerabilities—accurately and continuously.

Spirent **CyberFlood Data Breach Assessment**

Get Proactive About Assessing Your Security Posture.

It's no secret that data breaches are increasingly common—and costly. The hard-dollar costs of addressing a data breach are only part of the expense. You also need to factor in the opportunity costs of delayed strategic initiatives, inability to focus on regulatory compliance, or damage to the reputation of the company and its security operations.

But what's the secret to effective protection against data breaches? Keeping up with the surge in attacks, the increasing sophistication of attackers, and the sheer volume of new threats can be insanely complicated. And clearly, traditional approaches don't always give you the coverages you really need.

The Solution is Surprisingly Simple.

CyberFlood Data Breach Assessment provides a safe and easy way to get proactive about assessing your security posture. It delivers accurate, automated, continuous and thorough assessment of your live production environment—using always-up-to-date threat intelligence. So you can identify and address weaknesses in your security stance before attackers do.

Unlike other solutions in the category Gartner refers to as "Breach and Attack Simulation" (BAS), CyberFlood Data Breach Assessment is based on emulation, not simulation. Emulation replicates attack scenarios precisely, from the ground up, using fully stateful traffic and real attack vectors that real cyber criminals put on the wire. Simulation only "resembles" such a scenario and will not necessarily give you an accurate view of your security coverage. That's a crucial difference when it comes to accurate, dependable assessment.

Unique Capabilities for Uniquely Effective Protection.

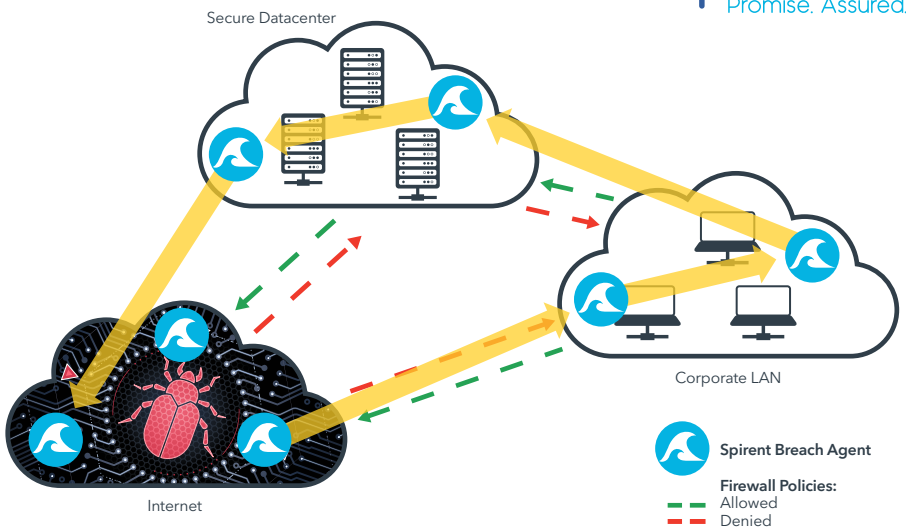
CyberFlood Data Breach Assessment delivers accurate, automated, continuous and thorough assessment of live production network environments, using an always-up-to-date database of hyper-realistic attack, malware, data loss prevention, and applications scenarios to safely and accurately validate your security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

- **Assessment based on reality:** Our solution safely generates hyper-realistic emulated security assessment traffic on the exact services you are protecting—so you can assess your security landscape with real attacks, malware, and sensitive data scenarios. It emulates attack propagation and pivoting behavior so you get an accurate assessment of complex security countermeasures. This in turn enables you to fine-tune security policies—more frequently and more completely.
- **Continuously updated threat intelligence:** The solution harnesses constantly updated threat intelligence feeds containing tens of thousands of scenarios for maximum accuracy, including:
  - **Applications:** Everything from Netflix to Salesforce to Skype, so you can validate app ID policies.
  - **Attacks & exploits:** targeting known vulnerabilities, enabling you to verify IDS/IPS security coverage.
  - **Malware threats:** including near zero-day scenarios, so you can verify malware prevention capabilities.
  - **Sensitive data emulation:** including corporate intellectual property and customer protected data, allowing you to validate data loss prevention policies confirming sensitive information does not escape your organization's exfiltration policies.
  - **Encrypted traffic:** users can quickly change TCP based attacks or malware to be sent over TLS encrypted flows, this greatly challenges mitigation services ability to detect malicious content.
- **Comprehensive, automated assessment of production networks:** CyberFlood Data Breach Assessment creates comprehensive assessments between lightweight Spirent CyberFlood Virtual (CFV) Agents at critical intersections within your network infrastructure. It defines a network topology, including network zone details, allowing you to find security issues and gauge security efficacy. The solution automatically analyzes logs and correlates them to the assessment's security events in SIEM systems such as Splunk, Elasticsearch and others, and also submits and tracks discovered issues into the most popular issue tracking systems such as ServiceNow, JIRA, and ZenDesk. This gives you a complete, end-to-end assessment including traceability from issue detection to resolution.

Move Beyond Traditional Security Assessments

CyberFlood Data Breach Assessment enhances the best aspects of your current approaches and adds new capabilities. It overcomes the challenges of reactive methods and delivers a continual assessment of your vulnerabilities.

- **Pentesting (Red team):** An important capability, but these point-in-time assessments are not frequent enough to provide a true vision of the threat landscape and usually require human interaction.
- **Defensive testing (Blue team):** Can only be run in conjunction with pentesting, so not frequent enough and potentially very costly.
- **Hybrid approach (Purple team):** Mimics the complexity of the real world, but at a significant cost: lack of complete or continuous vision of the threat landscape.
- **Commercial simulation solutions:** Replay previously captured traffic, sometimes in the form of a packet capture, leading to unrealistic assessments, a false sense of security, and false positives.



CyberFlood Data Breach Assessment emulates scenarios, including evasions techniques, that look and feel like a real attacker.

- **Limits the impact to users:** CyberFlood Data Breach Assessment identifies security policies that degrade performance without providing additional security coverage, so you can make changes and verify the balance between performance and security continuously.
- **Can be used in a variety of environments:** CyberFlood Data Breach Assessment can be deployed for use in on-premises networks, hybrid, and cloud environments. With support for ESXi, KVM, AWS, Azure and more, assessment visibility is assured for your specific infrastructure.
- **MITRE ATT&CK and other security frameworks:** Data Breach Assessment incorporates a multitude of reporting and assessment authoring. This includes 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.
- **Powerful capabilities:** Create extensive assessments covering small network segments to enterprise wide validation. Use built-in evasion techniques to verify security solutions can mitigate attacks and malware under the most adverse conditions. Schedule assessments to run at specific times, at recurrence intervals, or to automatically verify remediation attempts. And much more.
- **Draws on our experience:** The solution leverages many years of security content cultivated by Spirent's Threat Research and SecurityLabs teams. The combination of our internal Security Services and Threat Research teams, along with external partnerships across the threat intelligence community, enable Spirent to continuously collect and use a wide variety of real-world attack components.
- **Proven solution from a reliable partner.** CyberFlood Data Breach Assessment expands on the proven capabilities of CyberFlood, the powerful, easy-to-use test solution that generates realistic application traffic and attacks to test the performance, scalability and security of today's application-aware network infrastructures.

And it's from Spirent, an established company that combines the agility and innovation of a start-up with the resources and backing of a large, revenue-positive enterprise, backed by decades of data communications test and assessment expertise.

"The company continues to increase its value to customers by expanding its capabilities to the attacks most relevant to its customer base, which is exactly what it did with the launch of its breach-emulation feature, which focuses on more sophisticated multi-layer attack campaigns."
–451 Research

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

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

Tame the Complexity of Effective Data Breach Assessment

CyberFlood Data Breach Assessment dramatically simplifies and streamlines assessment of your security posture. It enables your enterprise and your security teams to:

Be Secure

Find the holes in your security before someone else does. It gives you clarity and confidence in your security posture with remediation guidance from Data Breach Assessment visibility.

Stay Sane

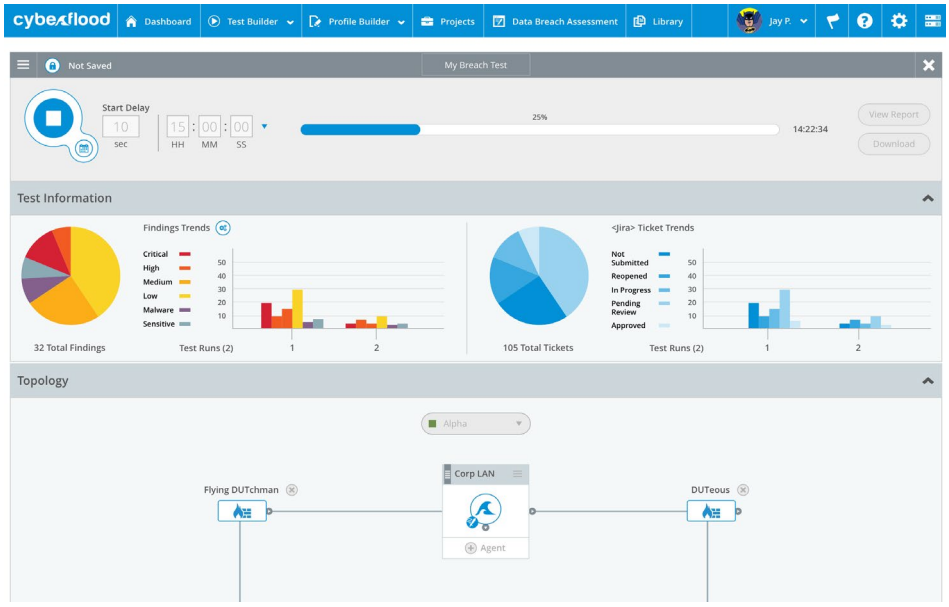
The solution reduces burden of your security teams of very time-consuming fire-fighting activities so they can focus on addressing holes in your threat landscape.

Elevate Security Influence

CyberFlood Data Breach Assessment underscores the value of QA and Ops/production teams in supporting organization's security priorities.

Innovate with Intention

When you have confidence in your security posture, you are free to innovate like never before.



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.

Rev E | 05/20