White Paper

spirent
Promise. Assured.

Optimizing Your Cybersecurity Investments

The Risk Mitigation Cycle: Continuous Visibility, Validation, and Improvement

How Effective is the Protection You've Put in Place?

Despite ever-increasing investments in cybersecurity solutions, technologies, and methodologies, many organizations cannot quickly and accurately answer the question above.

Spirent believes guesswork and optimism have no place in today's security landscape. We have devised a pragmatic framework for accurately assessing the strength of an organization's security posture and continuously improving it. We call it the **risk mitigation cycle**.

By addressing each phase of the risk mitigation cycle, enterprises can begin to see precisely what value they're getting from their current security spending and ensure new purchases are more effective and strategic. Simply put, they can optimize their cybersecurity investments continuously.

More specifically, the risk mitigation cycle enables organizations to:

- Quickly identify new vulnerabilities and gaps in coverage
- Determine whether current protection mechanisms are actually effective
- Prioritize remediation efforts according to business objectives
- Validate the impact of policy changes on your overall security posture and compliance status
- Deliver the right training to the right people at the right time
- Constantly improve and refine security measures

This paper presents an overview of the risk mitigation cycle, describes the pros and cons of traditional testing and validation solutions, and summarizes how Spirent offerings address all phases of the cycle, enabling you to optimize security investments.

Risk Mitigation Cycle: See Vulnerabilities, Strengthen Security Continuously

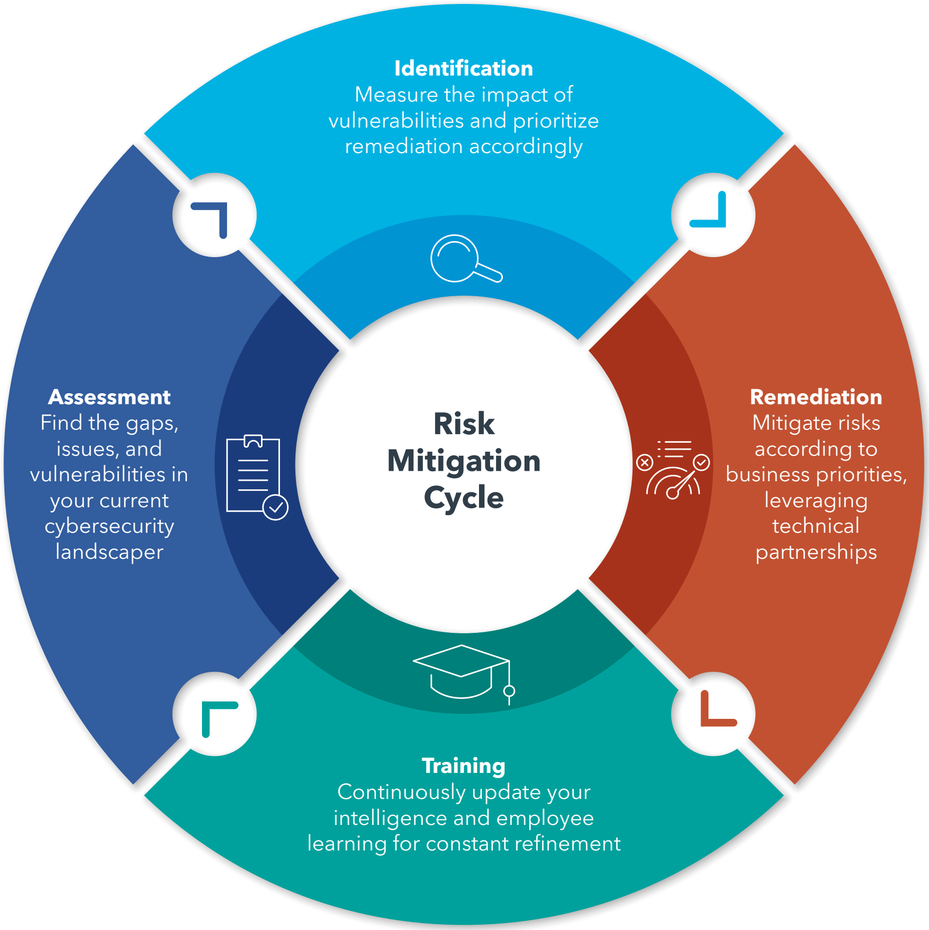
No single solution "solves" all cybersecurity challenges. The keys to minimizing risk exposure and optimizing cybersecurity spending are **visibility** into the current security posture and continuous **validation** of the security landscape.

Of course, there are many security products and services that offer partial solutions—from vulnerability scanning to penetration testing to various attack simulation products. The question is how to select among them and "rightsize" multiple assessment approaches to fit the organization's unique situation and requirements.

The risk mitigation cycle provides a structured way to get the visibility and validation needed to prioritize security investments and improvements. It includes four phases:

- **Assessment** of gaps in cybersecurity coverage—in the lab or in live production environments
- **Identification** of vulnerabilities and their impact, so you can prioritize risk mitigation efforts
- **Remediation** of vulnerabilities according to criticality and business priorities
- **Training** for continuous learning and refinement of your security measures and policies

Note that the Assessment and Identification phases involve measuring the **strength** of your current environment, while the Remediation and Training phases focus on determining how to continuously **improve and evolve** in mitigating risks.


Identification
Measure the impact of vulnerabilities and prioritize remediation accordingly
Assessment
Find the gaps, issues, and vulnerabilities in your current cybersecurity landscaper
Risk Mitigation Cycle
Remediation
Mitigate risks according to business priorities, leveraging technical partnerships
Training
Continuously update your intelligence and employee learning for constant refinement

Transforming Piecemeal Approaches into a Unified Strategy

In evaluating the various tools and services available today for assessing the organization's security posture, the question is not just when to use which or how to cobble together the best solution to fit specific priorities. The question is how to craft a strategy that addresses each phase of the risk mitigation cycle effectively. This requires evaluating the pros and cons of all of the following:

- **Vulnerability scanning:** Users conduct automated scans on their web, mobile and cloud applications and receive actionable insights and reporting about vulnerabilities detected. These scans make it easy to analyze and monitor an organization's security infrastructure, but they are point-in-time scans and depend on users to update the information regularly.
- **Pentesting (Red team assessments):** This approach identifies weaknesses in systems and networks. While these assessments can be valuable, they are specific to a point in time and typically do not recur often enough to provide true visibility into the ever-changing threat landscape.
- **Defensive approach (Blue team assessments):** Defensive solutions identify security gaps, verify the effectiveness of each security measure, and ensure security measures will remain effective after implementation. They are often run in conjunction with pentesting, which means they are still not frequent enough and can be very costly.
- **Hybrid approach (Purple team assessments):** Hybrid assessments combine the Red team and Blue team approaches to identify attack vectors that could lead to a breach. They 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.
- **Consulting services:** Many cybersecurity vendors offer professional services to help you assess your security posture and make needed changes. The problem is, most of them can only offer advice, not lifecycle testing solutions. In most cases they can address one or two elements of the risk mitigation cycle, but not the full cycle.

Without a structured approach to assessing and deploying these options, companies end up testing the wrong things, testing too little, testing too infrequently—or simply relying on vendor-supplied security metrics and not testing at all. The risk mitigation cycle provides a simple way to understand, prioritize, and select the right solutions.

Spirent facilitates this effort by providing solutions that not only cover each phase of the cycle but also work well together to complement and add value to each other. Our unified solutions enable organizations to minimize their investment of capital, staff time, and IT resources while maximizing the effectiveness of the security they put in place.

Spirent: Covering Every Phase of the Risk Mitigation Cycle

Spirent cybersecurity solutions reduce the complexities of security and performance validation and address each phase of the risk mitigation cycle.

Spirent is currently the only company that covers the entire risk mitigation cycle with unified security and performance testing solutions. We combine our CyberFlood, CyberFlood Data Breach Assessment, SecurityLabs testing solutions and services, and Spirent Education Services to enable organizations to visualize and validate their security posture and optimize their security investments. Below is a brief summary of the core solutions; the next section illustrates how they address the requirements of each phase of the risk mitigation cycle.

- **CyberFlood:** A powerful, easy-to-use L4-7 testing solution. Used in lab settings, it generates realistic application traffic, attacks, and malware to validate the performance, scalability, and security of today's application-aware network devices and infrastructures, and enables teams to test and enforce policies, benchmark performance and capacities, and validate network security.
- **CyberFlood Data Breach Assessment:** Provides accurate, automated, continuous and thorough production environment assessment of the organization's security posture using always-up-to-date threat intelligence and hacker techniques. It enables teams to identify and respond to vulnerabilities before incidents occur and fine-tune security policies more frequently, completely, and accurately—without degrading the performance experienced by end users.
- **SecurityLabs:** Provides comprehensive managed security testing services and consulting services delivered by certified, seasoned security professionals. Our independent, third-party testing and reporting services facilitate compliance and security audits; supplement the organization's internal expertise; streamline testing processes; and unburden staff while improving the security posture.
- **Spirent Education Services:** We offer ongoing training options so teams can obtain comprehensive instruction on current and emerging technologies and continuously refine the protections they've put in place.

In short, Spirent delivers the broad spectrum of capabilities organizations need to address the key questions at each phase of the risk mitigation cycle, as discussed below.

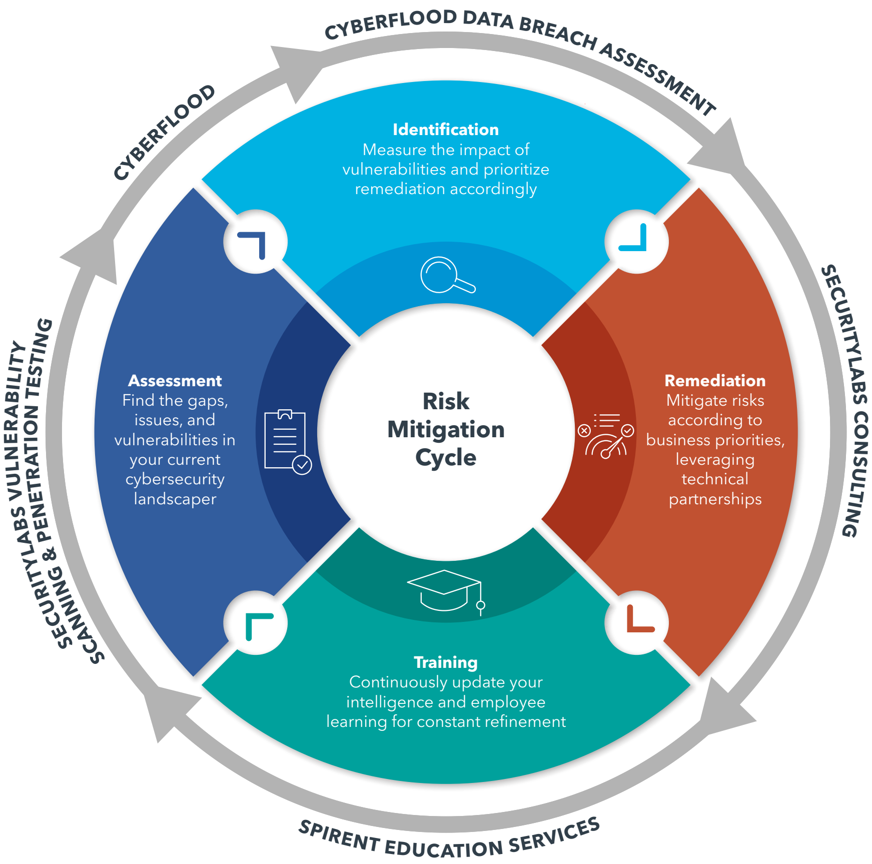
Assessment

The big question in this phase is "where are the holes in our defenses today?" Spirent answers with a range of services and capabilities that can be combined based on each organization's priorities. For example:

- Spirent Security Labs provides managed security services that enable organizations to proactively, independently, and objectively identify security vulnerabilities. We can perform comprehensive scanning, penetration testing, and monitoring of networks, applications, devices and endpoints, or our consultants can ensure that teams have the right skill sets and tools to perform those tasks on their own.
- CyberFlood can ensure that organizations are able to assess at the depth needed to identify risks at all layers, including L4-7. TestCloud, a core component of CyberFlood, has a library of tens of thousands of realistic applications and attack vectors and is regularly updated to ensure load and functional testing with unparalleled scalability.
- CyberFlood Data Breach Assessment combines the capabilities of Red and Blue team assessments, and harnesses automation to move beyond "point-in-time" testing to continuous testing. It uses emulation techniques that replicate attack and evasion scenarios precisely, employing hyper-realistic attack vectors and behaviors to get an accurate view of the organization's security coverage in production environments.

With CyberFlood Data Breach Assessment, Spirent can set up a baseline measurement of your risks by harnessing a framework such as MITRE ATT&CK or the NetSecOPEN framework, then continuously validate against an ever-growing list of evasion techniques, such as IP segmentation, timing evasions, and binary obfuscation to ensure an accurate assessment of security gaps.

CyberFlood Data Breach Assessment leverages constantly updated threat intelligence from multiple sources to find new and emerging vulnerabilities in app ID policies, IDS/IPS coverage, DLP, and so on.


CYBERFLOOD DATA BREACH ASSESSMENT
SECURITYLABS CONSULTING
SPIRENT EDUCATION SERVICES
SECURITYLABS VULNERABILITY SCANNING & PENETRATION TESTING
CYBERFLOOD
Identification
Measure the impact of vulnerabilities and prioritize remediation accordingly
Remediation
Mitigate risks according to business priorities, leveraging technical partnerships
Training
Continuously update your intelligence and employee learning for constant refinement
Assessment
Find the gaps, issues, and vulnerabilities in your current cybersecurity landscaper
Risk Mitigation Cycle

Identification

The key issue in the Identification phase is how to prioritize remediation efforts. With CyberFlood Data Breach Assessment and SecurityLabs consulting services, organizations can measure the financial impact and opportunity cost of downtime caused by identified vulnerabilities; consider the impact on both users and the business; and get the customized reporting needed to understand and respond to the highest cybersecurity remediation priorities.

In addition, CyberFlood Data Breach Assessment enables security teams to generate emulated traffic for the same services they are protecting, so they can assess the impacts of security in real time. They can identify security policies that degrade performance without providing additional security coverage, so teams can make changes and verify the balance between performance and security continuously.

With the combination of CyberFlood Data Breach Assessment and SecurityLabs consulting services, organizations can also supplement the internal team's findings with advice and insights from certified consultants with experience in risk assessment and mitigation.

Remediation

In the remediation phase, it is important to measure the impact of the changes made to the environment. With CyberFlood Data Breach Assessment, the environment is continuously assessed so teams can draw accurate, meaningful comparisons of the effectiveness of remediations from one period to the next. They can assess and validate the impact of policy changes on the overall security posture and compliance status. And they can draw on Spirent's strong technology partnerships to get a full picture of the types of vulnerabilities that can be remediated through a single source.

Training

The key in this phase is ensuring continuous learning and refinement of the environment. With Spirent Education Solutions, organizations can institute regular, required training programs to advance the knowledge and skills of SecOps teams. These training services make it easy for all constituents (SecOps teams and business stakeholders) to see, understand, and act upon the vulnerability information presented by scans and assessments.

Seasoned instructors teach hands-on courses that are delivered off-site or on-site using proven instruction techniques. The specific offerings include:

- **Web-based training:** On-demand access to courses covering a broad array of test and measurement fundamentals.
- **Instructor-led training:** To help master the latest testing technologies and apply the latest testing methodologies and applications.
- **On-site training:** Allows teams to fully leverage the latest testing methodologies and applications in their unique testing environment, at a lower cost than instructor-led training.
- **Custom training:** Tailored to each company’s needs.
- **Distance learning:** Instructor-led customized courses delivered via the Web.
- **Certification:** These programs validate the tester’s skills and provide a benchmark to evaluate candidates.

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

Learn More

The risk mitigation cycle provides a structure approach for getting the visibility and validation needed to optimize security investments. Spirent is the one and only vendor that can cover the entire risk mitigation cycle with testing and validation solutions, consulting services, managed security services, and education services that give organizations the visibility they need to measure, manage, and improve security continuously.

spirent™
Promise. Assured.

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 A | 03/20