Flare Sentinel/Snare

Deception Decoy Solution

FLARE SENTINEL

FLARE SNARE

CYBX

Why CybX?

Solutions use proprietary encryption strategies

Combined 55 years' experience of leadership and innovation in data and data center protection

Trusted, reliable solutions. Located in a secure facility in McKeesport PA.

CybX holds six immune architecture patents

Solutions You Can Trust

CybX solutions are developed in line with:

ISO

- International Organization for Standardization.

NIST

- National Institute of Standards and Technology.

ANSI

- American National Standards Institute.

CIS

- Computer Information Science.

The Problem

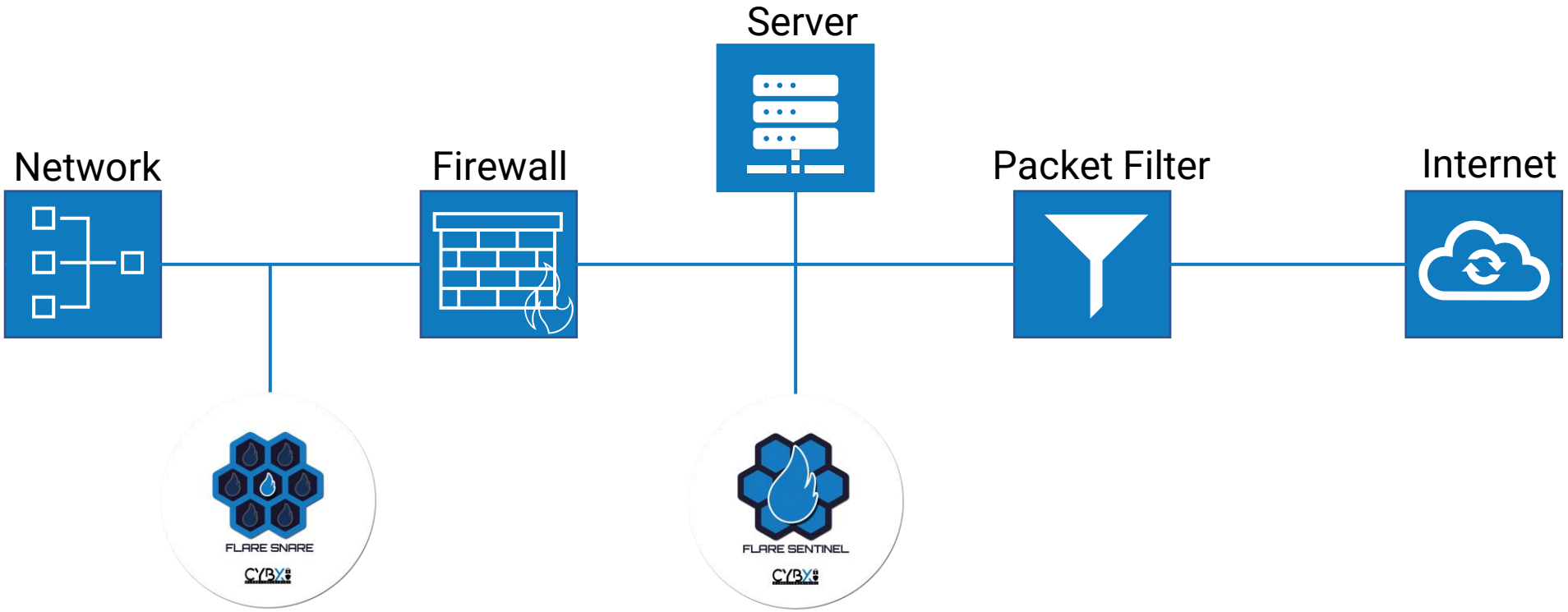
- A year from today, there will be **1,460,000** ransomware attacks targeting U.S. organizations.
  If your organization is a victim of just **ONE** malware attack, or **ONE** ransomware attack, the results will be devastating.

Our Decoy Solution

- **Flare Sentinel** and **Flare Snare** are deception and decoy solutions that are located at the perimeter and inside your network.
- **Flare Sentinel** is designed to mimic real perimeter hardware and software, and acts as a "honeypot" for cyber attackers. Sentinel gathers data constantly about the attacker's activity, including passwords used, methods employed and other invaluable data points.
- **Flare Snare** is a "honeynet" designed to mimic real devices. Snare is deployed inside your network and will capture any attempts to hack or disrupt devices by hackers or internal threats.

Why Flare Sentinel/Snare?

- By carefully analyzing the data provided by these deception & decoy systems, we are able to strengthen your security posture, understand the methods and tactics used by attackers, and highlight the origins of attacks.



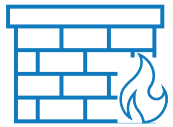
How?

- All it takes is one consultation to complete **traffic analysis**. Our expert-led team will test for vulnerabilities across your entire organization:

Data Security Analysis (e.g. encryption, storage)

Ransomware Defense Analysis

Website/Web App Vulnerabilities



Perimester Network Security (e.g. firewall)

Endpoints (e.g. computers, laptops)

IoT Devices (e.g. CCTV, printers, smart devices)

What Happens Next?

- **Best Case Scenario:** We find no vulnerabilities on your network, and both your infrastructure and data are secure. Our post-test consultation will validate your cybersecurity investment.
- **Worst Case Scenario:** If we do find vulnerabilities, we provide recommendations to remediate security issues with **zero obligation** to use our solutions.

Our Primary Objective is to Ensure Your Data Is Secure.

Set up a consultation today!

Thank you