CYREN

Cyren Sandboxing

Enterprise Security SaaS

Stop evasive zero-day threats with Cyren's sandbox array in the cloud

Today's cyberthreats are constantly evolving. Your business faces zero-day exploits, targeted attacks, and advanced persistent threats that have never been seen before, and are specifically designed to evade traditional malware defenses and first-generation sandboxes. No company is immune, with attacks impacting organizations of all sizes and across all industries—in fact, 60% of all targeted attacks focus on SMBs.

Zero-day protection with innovative Cloud Sandbox Array

Cyren Sandboxing protects your business against breaches and data loss from today's evasive zero-day threats with an easy-to-use, cost-effective cloud solution. Powered by the industry's first cloud sandbox array, Cyren Sandboxing analyzes suspicious files and URLs that your users try to access in email or on the web. Once we identify a new threat, we immediately implement protective measures for everyone across the entire Cyren network by blocking the identified malicious files, URLs, and command & control traffic.

Scalable protection for all users and all web traffic, including SSL

Today's zero-day threats and APT attacks increasingly leverage evasive techniques that check if they are being run in a virtual sandbox, and then alter their behavior to avoid detection, among numerous other techniques. This increasing sophistication is effectively overwhelming the processing and architectural limitations of traditional appliances.

Cyren Sandboxing is designed to protect all of your users, from roaming employees to branch offices to headquarters — from the cloud, where our massively scalable security platform already sees over 17 billion web and email transactions a day, delivering the fastest threat analysis and the highest catch rates. In our unified, global security cloud, elastic compute resources can perform full behavioral analysis as necessary to identify a threat, including the additional processing load of fully inspecting threats hidden in encrypted SSL traffic.

Integrated security layer in a cloud platform — just turn it on

Cyren Sandboxing is delivered as an integrated part of our multi-layered security cloud. This means instant deployment and full synergy between the sandboxing system and other layers, like dynamic web reputation analysis. As a cloud-based SaaS, there are no time-consuming updates and you are always running the latest version.

CYREN Sandboxing

The Cloud Sandbox Array Difference

Cyren's patent-pending sandbox array technology is a fundamental step forward in the battle against hyper-evasive malware, providing:

Superior Detection

- Our cloud-based array exposes files to not only different environments but also different sandbox types running on both virtual and physical machines.
- Cyren has automated the complex process of file analysis usually done manually by malware researchers, producing better analysis and deeper zero-day threat intelligence.

Unlimited Scalability

- As Cyren's sandbox array is n the cloud (as opposed to an appliance), it allows us to scale easily, utilizing more machines and resources as requried

Faster Analysis

- In many cases, a file's risk profile can be determined even before the actual dynamic analysis on the sandbox starts.

Richer Reporting

- Although we may analyze a file across different sandbox types, we provide a single unified report and risk score. The information provided in the report includes the merged list of risks observed in all the different analyses conducted. across environments.

www.Cyren.com

sales@cyren.com

25B Security Transactions Daily

1.3B Users Protected

300M Threats Blocked Daily

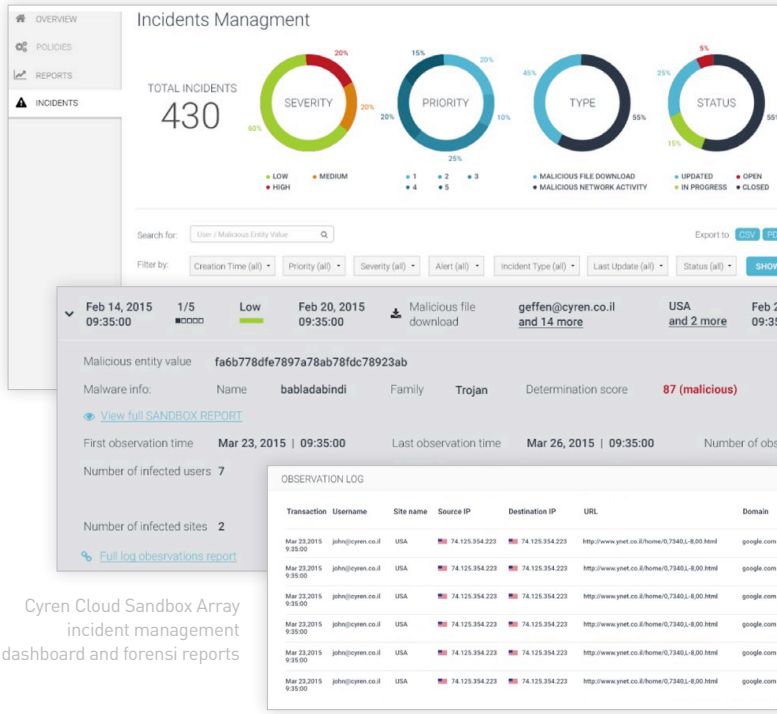
CYREN

CYREN SANDBOXING

Enterprise Security SaaS

Get actionable indicators of compromise

For security teams seeking detail to identify systems requiring remediation, Cyren provides an Incident Management dashboard and detailed forensic reports which include security bypass techniques, network activity, persistence techniques, detection evading techniques, system and file configuration changes, memory and process analysis, packet captures for detailed analysis, and origin and destination analysis for suspect locations.



Cyren Cloud Sandbox Array incident management dashboard and forensi reports

How it works

Cyren Sandboxing uses an innovative, patent-pending multi-sandbox array technology coordinated by a sophisticated heuristics-based engine to ensure that unknown files are completely analyzed, even those attempting to evade detection.

1. Sophisticated pre-processing combines static and dynamic analysis; then the expected behavior of the file is predicted and an appropriate sandbox is selected.
2. The file is submitted to the selected sandbox and monitored for malicious activity, as well as complete expression of all expected behavior.
3. If the full set of expected behavior is not seen, then the file is recursively submitted to different types of sandboxes—which may vary by operating system, browser type, or virtual or physical environment—until full behavior is observed, and an aggregate threat score is calculated.
4. Once malicious files and URLs are identified, Cyren fingerprints and blocks them across its global network within seconds, providing a protection "network effect" for all Cyren customers.