Cyberstanc

Intelligent world class, New Age Anti-Malware engine
for Enterprise and Integrators

Disrupting Decades of Detection

Deep Tech: Cyberstanc uses simulated intelligence and emulation-based sandboxing to proactively detect and neutralize zero-day attacks and APTs, ensuring advanced protection.

Ransomware Response & Simulation Hub: Cyberstanc's dedicated ransomware program and advanced simulation lab analyze malware in real-time, uncovering key artifacts for precise threat detection and mitigation.

Next-Gen Threat Detection: Protecting servers, cloud, and hybrid networks with lightweight agents & agentless APIs. Seamless, real-time threat intel sharing for unstoppable security

Global Recognition: Endorsed by programs like Mach37 and accredited by AMTSO, Cyberstanc has built over 100 alliances and received multiple innovation awards, solidifying our leadership in cybersecurity.

Company Verticals

Anti-malware Engine

Environment learning
Deep Tech Model

Threat Integrations

100+ Alliance Partners
60+ Research Projects

Ransomware Study

Collaborative Response to Ransomware Threats.

R&D Center

Cyber Attack Simulation Learning Lab

Inside Scrutiny Technology

Modular Defense

Equipped with advanced microscanners and deobfuscation tools, it features multi-layered detection, a modular set, and cross-platform support for new detections.

Fast detection

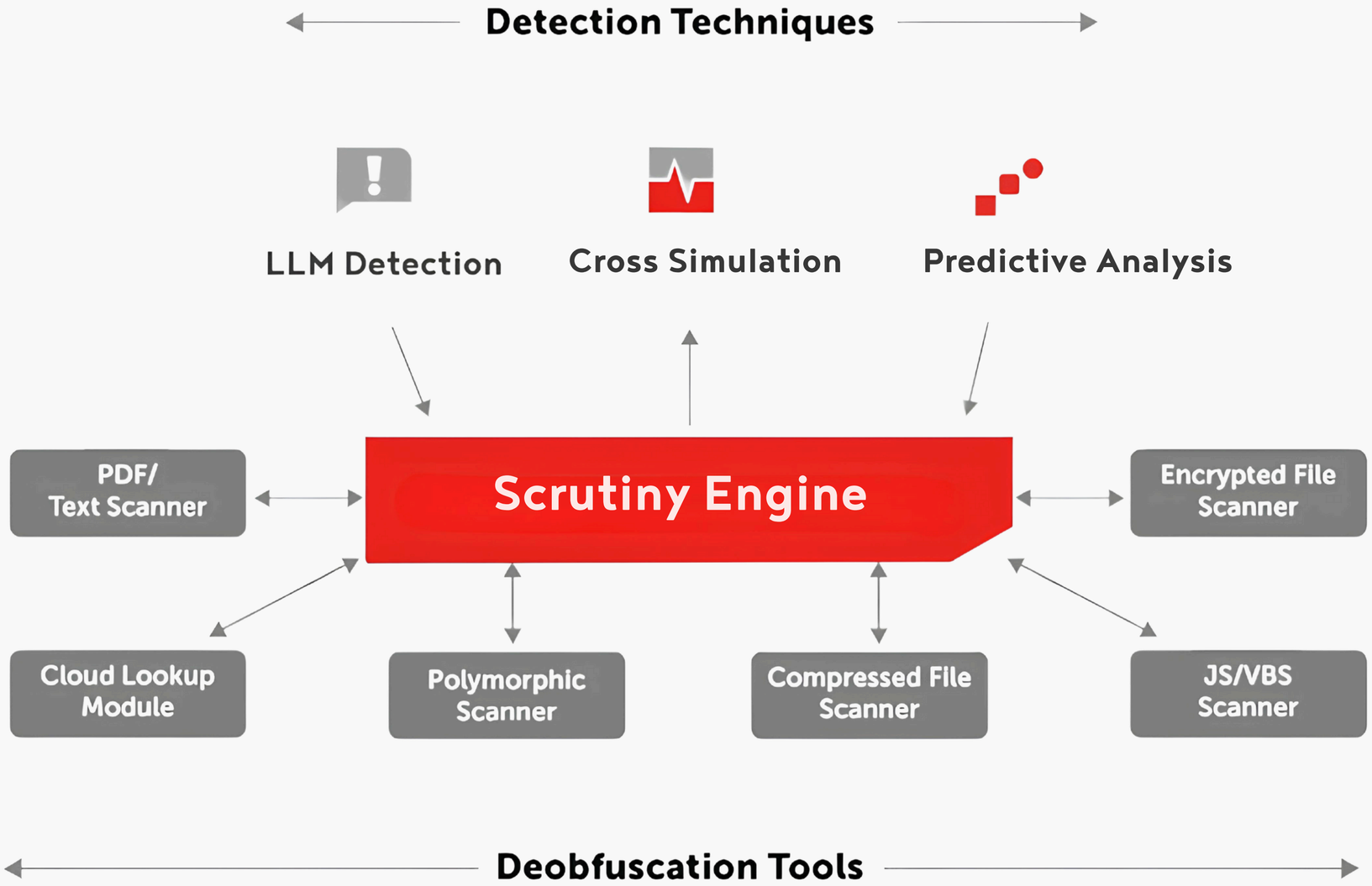
Enhances threat detection accuracy to 90% while conserving device resources, providing immediate malware verdicts with a rapid 4-second Mean Time to Detect (MTTD) for both known and unknown threats.

Unique integration

Offers complete protection for web portals, applications, servers, cloud environments, and email gateways, easily managed via ICAP and HTTP, with seamless SDK/API integration for deployment in standalone, cluster, or Docker container environments.

False Positives

Our advanced model effectively reduces false positive detections while accurately classifying goodware and malware, even in unpacked, obfuscated, and hidden formats.



How does it work?

Bulk file scanning

Supports scanning of 100+ file types with no bottlenecks, delivering results within seconds, all while maintaining a strict **no data acquisition policy**.

Modern Scanning Methodology

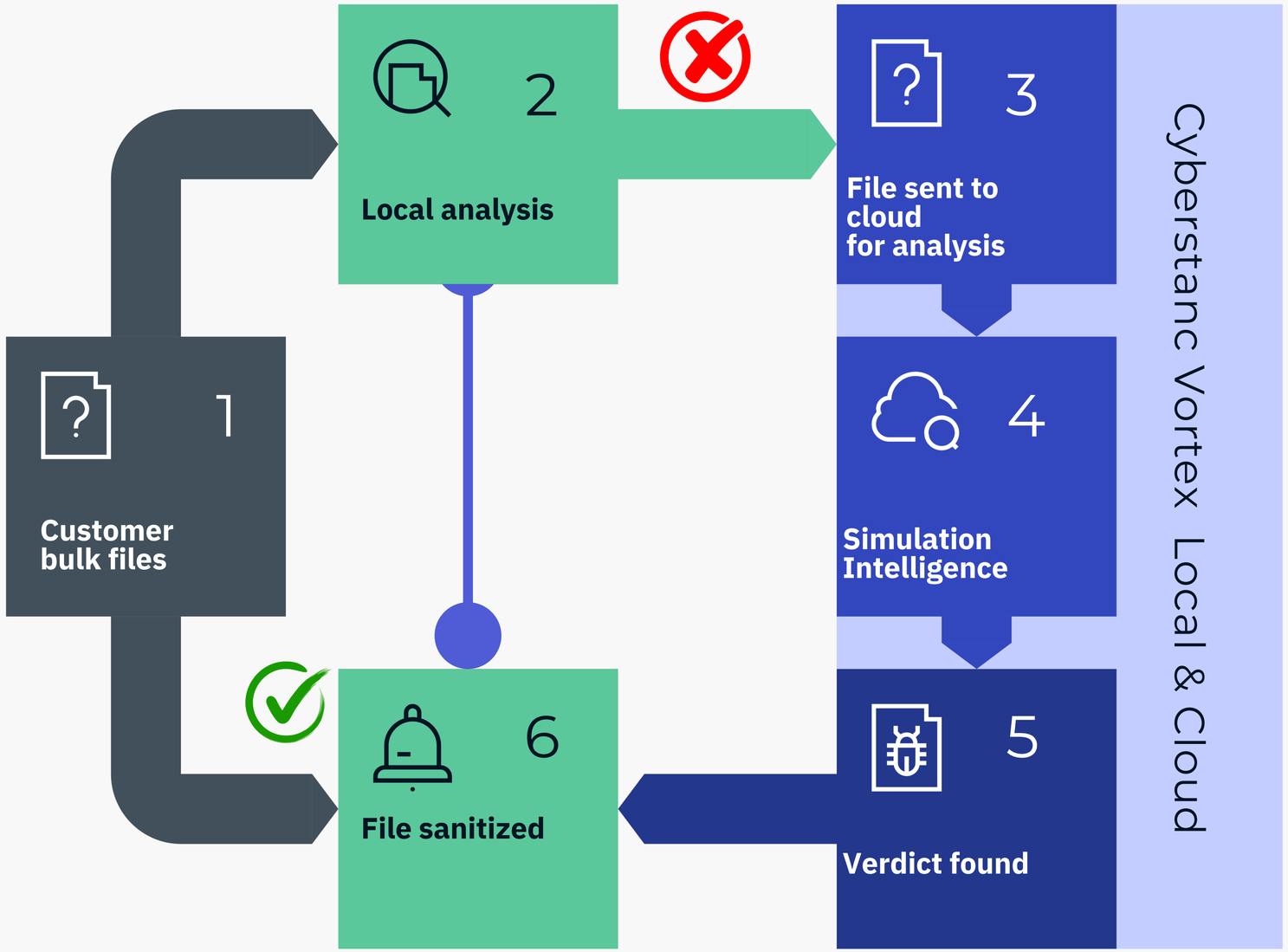
Scans files using a layered approach, analyzing data chunks and cross-simulating in an emulation-based sandbox for rapid local and detailed cloud insights.

Evidence based verdicts

A precise classification (benign, suspicious, or malicious) is returned to the endpoint. If malicious, the file is automatically quarantined or sanitized to neutralize the threat and results are stored for further analysis.

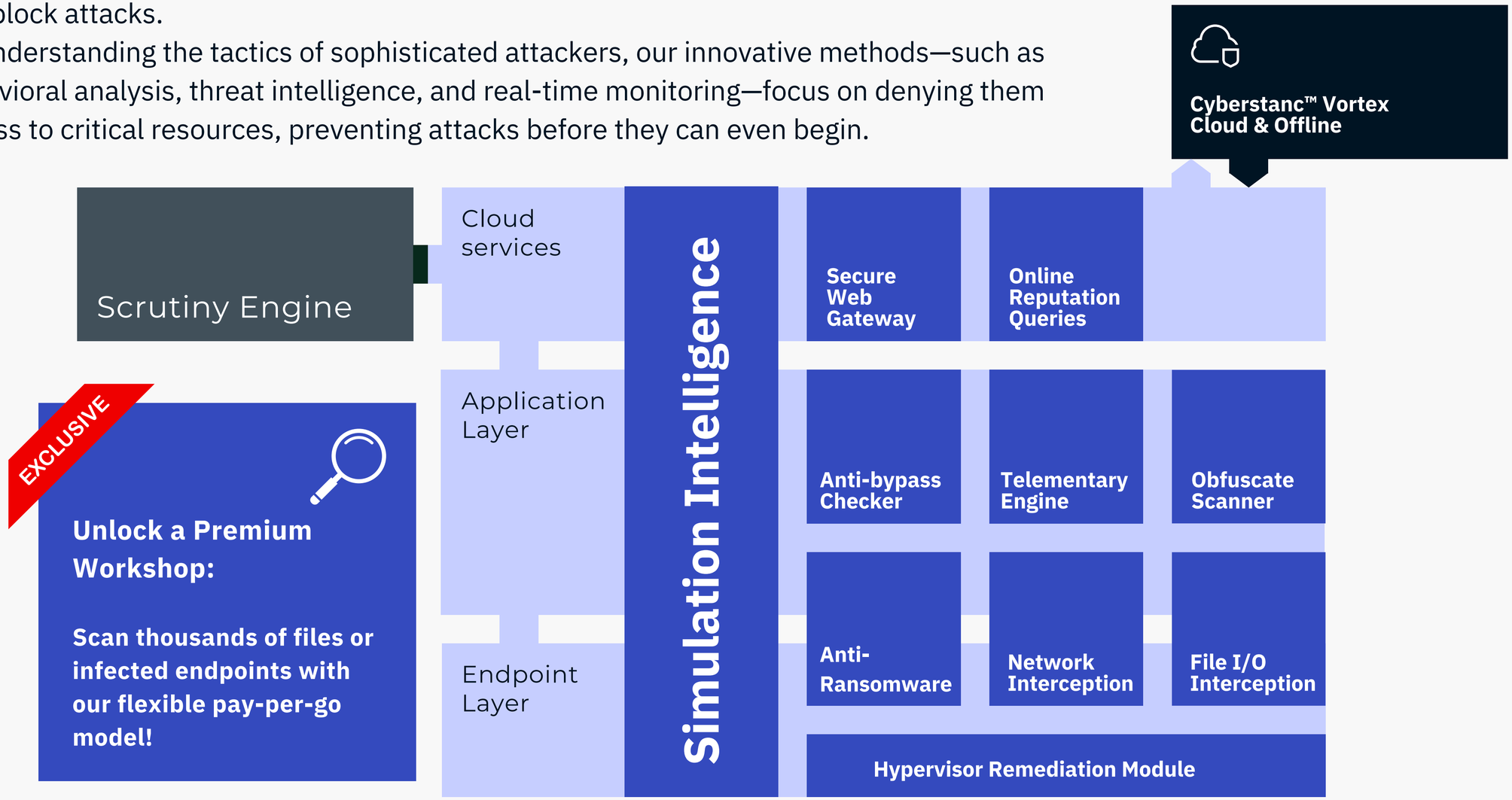
Fast Performance and Scalability

Delivers decisions 500 times faster with complete reliability, supporting all types of integrations in-house and in the cloud.



Welcome to the new age of proactive security!

Our protection strategy combines advanced technologies that work in unison to detect and block attacks.
By understanding the tactics of sophisticated attackers, our innovative methods—such as behavioral analysis, threat intelligence, and real-time monitoring—focus on denying them access to critical resources, preventing attacks before they can even begin.



Addressing Industry Challenges via Integration Solutions

Network layer

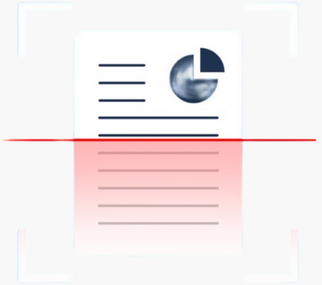
- Prevent hostile material from unknown sources
- Maintain secure file transfer
- Prevent Malicious downloads

Filesystem layer

- Backups and Storage
- High Volume file scanning

Execution layer

- Supply chain protection
- Prevent exploitation attempts
- Open Critical Servers



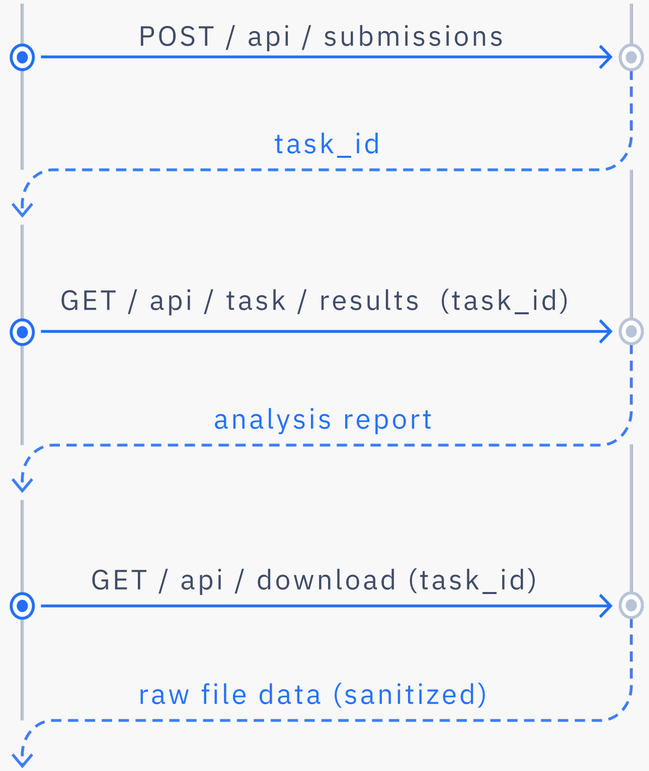
C# C++ C# SDK Bindings GO

APPLICATION INTEGRATION

REST API

REST client

Scrutiny Engine



Enterprise Case Study

Saving cost and precious time by offloading scanning & sanitizing hundreds thousand+ files a day with Cyberstanc's™ Scrutiny Engine,

Problem Statement

An Enterprise NBFC organization, like many financial institutions handle large volumes of sensitive financial and user data, but relied on outdated or inadequate antivirus solutions. This lead to insufficient file scanning, no security measure in place to securely process the data.

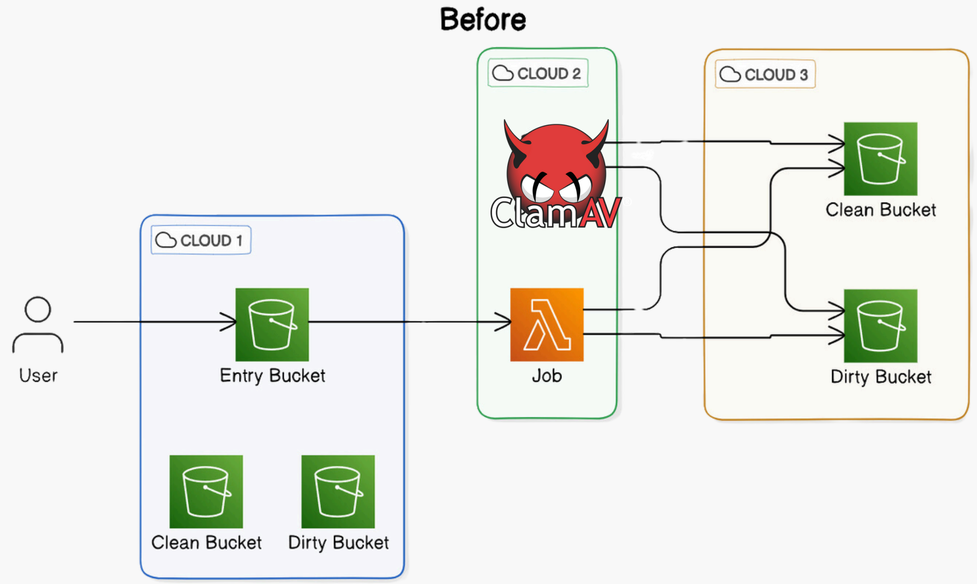
Our Solution

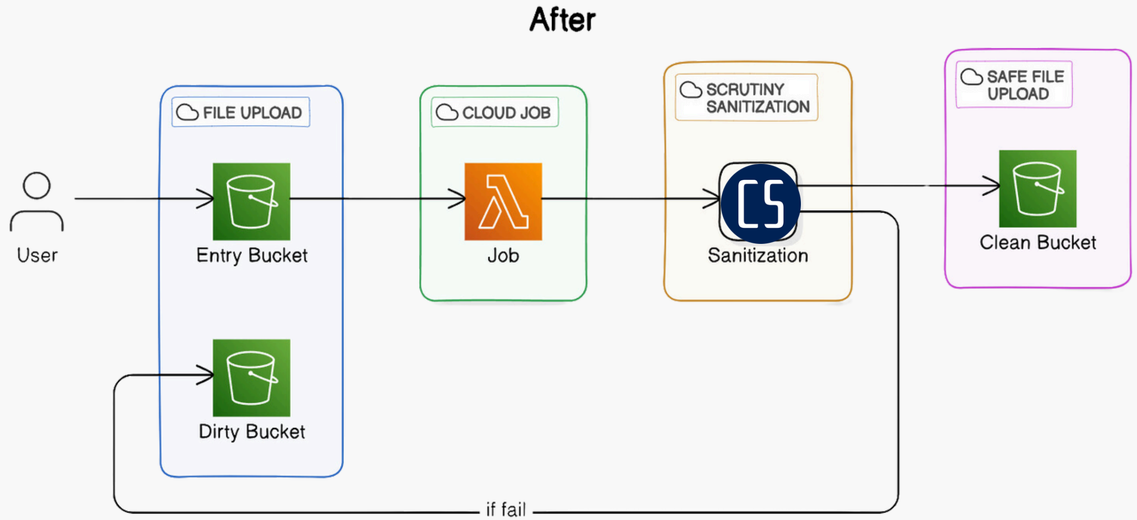
Detect and sanitize file-based threats from crimeware to advanced implants and provide local disinfection capabilities. It is lightweight since it does not carry a complete database of malware signatures, and integrates with any application including AWS S3 etc. providing large volume file scanning capabilities without any bottlenecks and false positives.

Impact

After implementing Cyberstanc's™ Scrutiny Engine, the organization immediately observed the following success metrics:

- **Zero false positives** in malware detection, ensuring accurate and reliable scanning.
- **Scales up to 100,000 files per day**, delivering a 6x increase in file scanning capacity over the previous setup.
- Provides an extra layer of security through **file sanitization**, beyond standard malware scanning.
- Saved AWS EC2 and S3 costs, offering a more efficient cloud scanning solution.
- No engineer support or software maintenance required, reducing operational complexity.





Comparison Battlecard

Why Settle for Ordinary? Choose the Engine SDK that Defends Extraordinary!

FEATURES	CYLANCE	SOPHOS	QUICKHEAL	CISCO CLAMAV	CYBERSTANC
LLM Assisted Detection					✓
Cloud Lookup	✓	✓	✓		✓
Swift Precision		✓			✓
Zero Data Capture				✓	✓
REST API	✓				✓
Custom Integration	✓	✓		✓	✓

Enterprise Ready -Offerings

Save cost and precious time by offloading scanning & sanitizing hundreds thousand+ files a day with Cyberstanc's™ Scrutiny Engine,

#bestdeal

Scrutiny SDK

Annual Starter Pack

Vortex Platform

Annual Starter Pack

Pay-per-Go

Scrutiny API

up to 10k files/month

- Support for:
  - Windows 10 & 11
  - Windows Server 2012, 2012 R2, 2016, 2019, 2022
  - Linux · CentOS 7.0+
    - · RedHat Enterprise 7.0+, 8.0
    - · Debian 9.0+, 11.0+
    - · Ubuntu 18.04, 20.04, 22.04
- Support for VMWare and VirtualBox
- Cloud deployments: AWS, Azure, Google Cloud Platform
- Container Support: Docker, Kubernetes
- Cloud integration available via vortex.cyberstanc.com

Deployment

- Online or offline environments
- Air gapped environment
- Remote assisted installations and workshops

Integrations

- SIEM / XDR for enhanced detection workflow
- Mail systems (e.g., SendMail, Qmail, Postfix, Exim) and proxy servers, including ICAP support.
- Rest API HTTP(S) standalone service

Key Benefits

High accuracy and reliable results

Cyberstanc's™ advanced scan engine delivers over 99% malware detection for Windows/Linux executables, PDFs, Office docs, leveraging predictive models on crowdsourced platforms like OPSWAT* and Polyswarm*. Traditional engines like Microsoft Defender only reach 40%, with Kaspersky, Bitdefender, and Sophos maxing out at 70%.

Simulation Intelligence

Leverage cross-simulation to analyze millions of tracks within each file, categorizing them by evidence. This approach strengthens security, compelling attackers to exert exponentially greater effort to circumvent our advanced detection capabilities.

Local and API Embed

Leverage a self-contained, small-footprint service that seamlessly integrates into SaaS products or appliances. Running locally, it eliminates the need for file execution or cloud lookups, ensuring instant deployment and enhanced security without compromising performance.

Offline environment compatibility

Many customers, especially in government and defense, demand offline functionality. Cyberstanc’s advanced scan engine is optimized for seamless integration in airgapped networks, enabling detection updates through custom update server mirrors, independent of internet connectivity.

High-Volume File Scanning

Enables bulk scanning of data across application servers, storage, backups, and NAS. It integrates with Microsoft Azure, Amazon EC2, and Google Cloud, supporting rapid analysis of millions of files.

Hardware or Software bundling

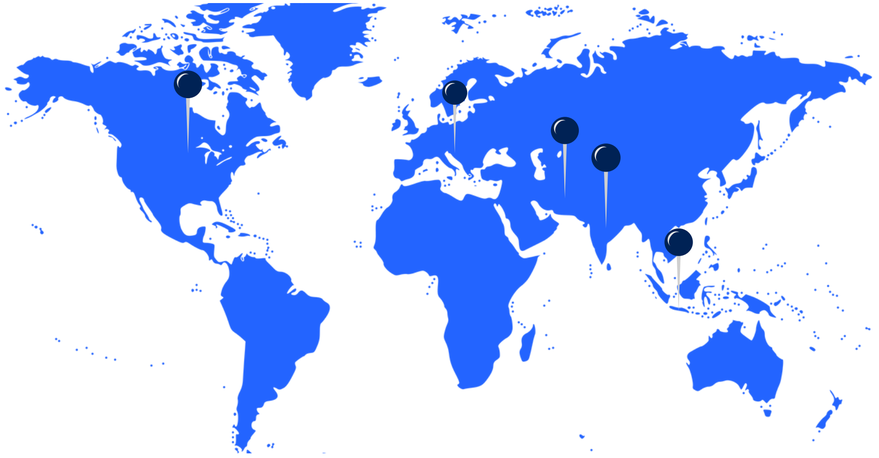
Bundle the Scrutiny SDK with your product or pre-install it on your hardware for seamless integration. Enjoy a lightweight, user-friendly experience with no complex configurations, rapid expansion and minimal integrator effort.

https://cyberstanc.com/blog/vortex/

https://cyberstanc.com/blog/cyberstanc-partners-with-polyswarm/

https://cyberstanc.com/blog/opswat-collaboration-with-cyberstanc/

Trusted By Many



CISA Applauds Scrutiny's Detection

CISA reports that Scrutiny was the first to identify **Daxin APT and Volt Typhoon** zero-day threats, enhancing federal agencies' detection capabilities.

Scrutiny Powers OneCard Security

With its capabilities, Scrutiny has seamlessly replaced **OneCard's ClamAV** setup, enhancing malware detection speed and scalability in both local and cloud setups

INDIAN Air Force Adopts Multi AV

Indian Air Force teams up with Cyberstanc for a Multi AV solution, offering a homegrown alternative to **Virustotal** while prioritizing data privacy!

Infra Secured from Ransomware

Apollo Pipes sought our help during an active **Mallox ransomware attack**. With the Scrutiny Anti-Ransomware solution, we swiftly secured their systems

For inquiries, contact us.

EMAIL partner@cyberstanc.com

WEBSITE https://cyberstanc.com

VORTEX FREEMIUM vortex.cyberstanc.com