DARKPOINT

a cyberpoint product

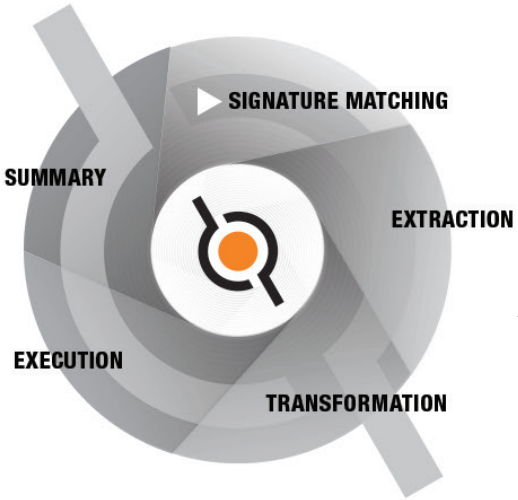
Malicious Digital Artifact Identification & Analysis

Any digital artifact—any file, program, document, image, link, script, or email—is potentially malicious. DarkPoint makes it easy to identify which ones actually are, and what you can do about it.

DarkPoint puts a powerful set of automated analytical tools at the fingertips of your help desk, security operations center, forensic investigators, and even ordinary users. Novice users can get quick answers about suspicious artifacts just by uploading them and reviewing a report, and experts can dive deep into the technical details and behaviors of advanced threats.

DarkPoint Benefits

- It's easy to use and enables novices and experts alike to identify threats fast.
- Saves time by automating common tasks: virus signature matching, reputation scans, and metadata extraction.
- Automatically executes cutting-edge analysis: artifact similarity search, severity score assessment, non-signature based threat detection, and more.
- Automatically decompresses and extracts files from supported archive types.
- Re-ingests and analyzes new artifacts discovered during analysis *(e.g. child malware)*.
- Allows users to customize analysis workflows to specific mission needs.
- Provides easy to understand mitigation strategies.
- Provides both summary level and in-depth reports.
- Alerting – publish or push results to common aggregation points *(syslog, email, web hooks)*.
- Create and share workflows to respond to specific threats, controlling each step of execution based on analysis results.



DarkPoint makes it easy to identify malicious artifacts and lets you know what you can do about it.

How DarkPoint Works

DarkPoint scans artifacts for known or unknown threats. Leveraging the power of open-source and patented CyberPoint technology, DarkPoint conducts flexible but powerful analyses of supported file types in near-real-time.

SIGNATURE MATCHING. DarkPoint scans artifacts for known malicious signatures.

EXTRACTION. DarkPoint identifies, decodes, and saves important elements from each artifact. This saves forensic investigations valuable time.

TRANSFORMATION. DarkPoint converts the artifact or its extracted elements into a format suitable for deeper analysis or searching. Where appropriate, it converts the artifact into a readable or previewable form.

EXECUTION. DarkPoint opens or executes the artifact in a carefully instrumented environment, observing and recording its behavior.

SUMMARY. DarkPoint loads and distills its analysis into a human-readable report so you can rapidly assess and mitigate the threat.

DarkPoint automatically identifies known threats, flags suspicious artifacts, and decodes binary files for network and system threat awareness. Its powerful deterministic expert system normalizes an artifact's analytical results and converts them into a clear, actionable report on the threat.

Develop for DarkPoint

DarkPoint provides robust APIs in Python and Java for adding and updating new analysis capabilities.

REST clients are also provided in Python, C#, and Java for developing external connections or connectors into DarkPoint.

Supported Artifacts

Type	Signature Match	Extract	Transform	Execute	Summary
Archive *(ZIP, RAR, TAR GZ, BZ, 7z, LO1, rpm, deb, etc.)*	✔	✔	N/A	N/A	N/A
Portable executable *(including .NET)*	✔	✔	✔	✔	✔
Executable and Linkable Format *(ELF)*	✔	✔	✔		
Mach-O	✔	✔	✔		
Portable Document Format *(PDF)*	✔	✔	✔	✔	✔
HTML	✔	N/A	✔	✔	✔
JavaScript	✔	N/A	✔	N/A	✔
Electronic mail *(email)*	✔	✔	✔	✔	✔
Network packet capture *(PCAP)*	✔	✔	✔		✔
Windows prefetch	✔	✔		N/A	
Window Registry hives	✔	✔	✔	N/A	
SQLite database	✔	✔		N/A	
URL	✔	N/A	✔	✔	✔
Android APK and Dex *(Dalvik Executable)*	✔	✔	✔		
Java Class and JAR	✔	✔	✔	✔	✔
Rich Text Format *(RTF)*	✔	✔			✔
X509 certificate	✔	✔		N/A	
Microsoft Office document formats	✔	✔		✔	
Image *(PNG, JPG, GIF)*	✔	✔	✔		✔
Firmware	✔	✔	✔		

What Can I Buy?

Configurations	DarkPoint Cloud (DPC) DarkPoint Enterprise (DPE) *(on-site)*
Customizations*	Control the number of sandbox VMs on DPE Enable or disable unneeded analyzers Spin up additional copies of important analyzers
Training*	Classes for operation, management and development Training available at CyberPoint or on-location Class sizes range from 3 to 20 participants

FREE TRIAL OFFER

To learn about our free 14-day trial subscription visit darkpoint.us today.

Buying DarkPoint

There is more to DarkPoint than we can put on paper—and we're constantly adding more. Visit darkpoint.us for the latest information.

3rd party licenses are required for some external service integration (e.g. distorm, IDAPro, Microsoft Windows 7 (with Office), VirusTotal (optional), OPSWAT (optional)).
NOTE: DarkPoint will function as normal without these services.

**Will result in increased cost.*

DARKPOINT
a cyberpoint product

CyberPoint International
621 East Pratt Street, suite 610
Baltimore MD 21202
phone +1 410 779 6700