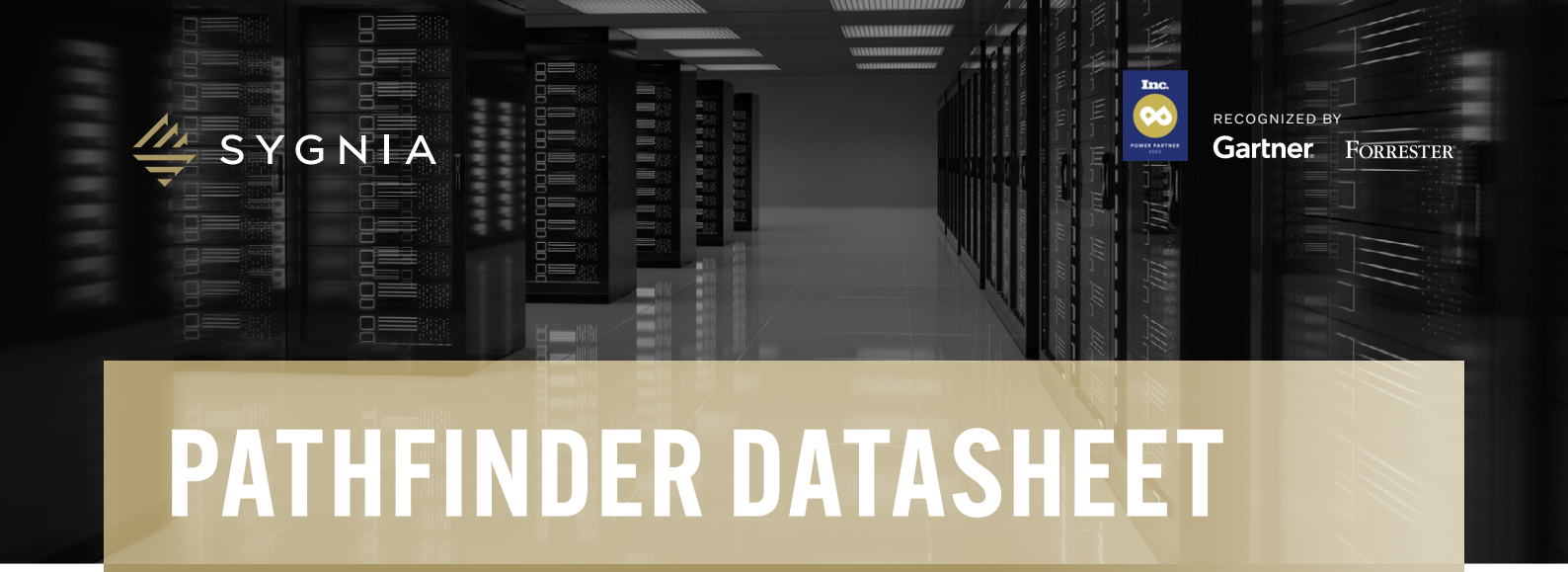

SYGNIA

RECOGNIZED BY Gartner FORRESTER

PATHFINDER DATASHEET

PRODUCT OVERVIEW

Pathfinder is Sygnia's proprietary, lightweight agent, built to enable, enhance and supplement existing binary data collection from servers and workstations as part of Velocity deployment. Additionally, Pathfinder allows administrators to easily install and configure 3rd party log collectors (ie: Sysmon, Filebeat, and Winlogbeat) on servers and workstations, providing a more robust, accessible and extensive security analysis.

PATHFINDER IN THE VELOCITY ECOSYSTEM

Velocity is Sygnia's unified cyber analytics and security platform, purposely built to empower security analysts to conduct triage, hunt for threats and investigate efficiently and effectively, independently or as part of a service provided by Sygnia. The platform collects, processes and queries vast amounts of data from a variety of sources in real-time.

Velocity uses top-of-the-line threat intelligence engines and advanced machine learning capabilities to enrich security insights. The Velocity platform provides a simple, user-friendly interface for users to configure alerts for better risk detection, enhancing visibility and speeding up response times.

The Velocity server manages and provisions Pathfinder, allowing admins to view information and real-time status of machines with Pathfinder installed. Admins can also generate operations and send them to one or more Pathfinders at a time, including:

- **Initial collection:**
  Collects targeted binary file types, registry hives of Software/System/ntuser.dat, startup/MFT/AMCache information, WER reports, browsing history files, scheduled tasks and more (see full description in Appendix A).
- **Extended info collection:**
  Collects forensic materials (i.e. netstat, firewall rules, USB data, network interfaces, hostnames, disk information, memory information, etc.).
- **Files fetcher:**
  Fetches files that match a given pattern from a given list of root folders.
- **Hashes fetcher:**
  Fetches the SHA1 of all files that match the pattern in the given list of root folders including their path and size information.
- **MFT Collector:**
  Collects $MFT from the given list of drives using raw copy.
- **Registry fetcher:**
  Collects the given list of registry keys.
- **3rd party collectors' installation:**
  Allows to install and configure enhancement tools and collectors such as Sysmon, Winlogbeat, Filebeat and Auditbeat.

Operations can be sent to multiple Pathfinders at once by using tags to group machines or by specifying the target machines. Velocity also supports dynamic tags, which it assigns to new machines as they are added. A dynamic tag (workstations, servers, domain controllers, etc.) is automatically assigned according to machine registry information. If there are any pending operations related to the machine or assigned tag, Pathfinder automatically receives and executes them.

When an OS-specific operation (such as 32-bit or 64-bit installers for Windows) is sent to a machine, the Velocity server uses the machine information provided by Pathfinder to determine the appropriate action.

ADDITIONAL ADVANTAGES

- **Small footprint:**

  Pathfinder is designed to be as non-intrusive as possible. When idle, it uses on average 10MB of memory, and a maximum of 256MB of physical memory. Total virtual memory is limited to 512MB. In addition, Pathfinder runs with low priority and utilizes a single CPU core.

- **Minimal impact on user tasks:**

  Pathfinder only performs operations it receives from Velocity. A heartbeat is sent from Pathfinder to Velocity every 60 seconds, checking for new operation requests. There are no OS hooks or monitors of any kind, meaning negligible impact on performance while an operation is being executed (limited by the safety measures mentioned above) and no impact on performance when there are no ongoing operations.

- **Minimal presence on host event logs:**

  All actions performed by Pathfinder (except run executable) are done through OS APIs, so no CMD/Shell commands are called.

- **Managing 3rd party collectors**

  Installing Pathfinder enables easy installation and configuration of Microsoft (Sysmon) and Elastic (Winlogbeat, Filebeat, Auditbeat) log collectors, compatible with a machine's OS. Running 3rd party collectors enhances data collection and increases visibility.

PREREQUISITES

- **Privileges**

  Admin access

- **Communication**

  Communication enabled between Pathfinder endpoints and Velocity via port 443.

- **SSL inspection disabled**

Windows	Mac OS	Linux
	Full Support	
Windows 8	Mojave (macOS 10.14)	CentOS 8+
Windows 8.1	Catalina (macOS 10.15)	Debian 8+
Windows 10	Big Sur (macOS 11)	RHEL 8+
Windows 11	Monterey (macOS 12)	Ubuntu 16+
Windows Server 2012+	Ventura (macOS 13)	
	Sonoma (macOS 14)	
	Sequoia (macOS 15)	
	Limited Support	
Windows XP SP2	El Capitan (macOS X 10.11)	RHEL/CentOS/Debian 6 + 7
Windows Vista	Sierra (macOS 10.12)	Ubuntu 12.04 LTS
Windows 7	High Sierra (macOS 10.13)	
Windows Server 2003		
Windows Server 2008		

SUPPORTED MODES OF OPERATION

Pathfinder can operate in two modes; service and transient (specified upon installation):

- **Service Mode:**
  Pathfinder registers as a system service, sending a heartbeat every minute to Velocity to check for pending operations. In addition, once every 15 minutes Pathfinder will run to collect basic endpoint information (i.e. processes, services, network adapters, disks, etc.). To customize the time interval, contact your Sygnia representative or support.
- **Transient mode:**
  Pathfinder only runs until the system/machine is restarted.

HOW IT WORKS

Upon deployment, Pathfinder performs the following operations:

1. Pathfinder collects general information from the host machine (i.e. OS info, disk info, services, processes, environment variables, network adapters, time zone, hostname, available memory, etc.) and sends the collected information to Velocity.
2. Velocity returns a list of operations for Pathfinder to execute.
3. Pathfinder executes each operation sequentially, displaying progress status in Velocity's operation page. If the operation fails, Pathfinder executes the next operation in line.
   Note: Users can configure the number of retries for each operation prior to execution or manually retry once an operation has ended.
4. Pathfinder sends the updated status back to Velocity.

SECURITY

Velocity's installation files are digitally signed, verified & authorized by Sygnia to ensure zero risk for our clients upon installation.

All communications between Pathfinder and Velocity - including server-side authentication - take place over HTTPS (port 443) using SSL encryption.

For Sygnia's cloud tenant-based deployment:

- A dedicated, isolated tenant is created for each client.
- Network access is restricted by using cloud network security groups and blocking access from IPs not previously whitelisted.
- A proxy server is deployed within the client's network acts as a central communication point for all deployed Pathfinders, reducing the attack surface. This proxy can only access the external network and is whitelisted in the relevant security group.
- For deployment options in an on-premise network, the relevant hosts, IPs and ports must be permitted on the client's relevant security system (firewalls, routers, etc.), per Sygnia and authorized 3rd party security best practices.
- For Pathfinders installed on off-premise endpoints (i.e. laptops) to execute operations off-premise, a direct connection to Velocity must be established via port 443.

APPENDIX A: INITIAL DATA COLLECTION OPERATION

Upon the first connection to Velocity, a data collection operation to Pathfinder is triggered, fetching the following artifacts:

- **Netstat**
- **ARP Table**
- **Files:** Upon deployment, Pathfinder performs the following operations:
- **Registry:** Recent Commands, Firewall Rules, Typed URLs, USB, Shim Caches, WDigest, Image File Execution Options
- **WMI:** Drivers, Drives, Mapped Drives, Shares, Network Storage, Startup Commands, Users, Shortcuts, Route Table, Network Connections, User Accounts, Services, Processes, Hotfixes
- **Local disk files (under 10 MB) with the extensions:** .appref-ms, .asp, .aspx, .bat, .cc3, .cfm, .cmd, .cmdline, .com, .dll, .exe, .hta, .js, .jsp, .php, .ps, .ps1, .scr, .sys, .dat, .xxt, .hlp, .vbs, .jar, .py, .au3
- **The following registry keys and their children (recursively until depth 5):**
  HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
  HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
  HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellServiceObjectD elayLoad
  HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders
  HKLM\SYSTEM\CurrentControlSet\Services\Google Update\Image Path
  HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fSingleSessionPerUser
  HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections
  HKLM\Software\Microsoft\RPC\Security
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Ipstatus
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Level10
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Level01
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Level02
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Level03
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Level04
  HKLM\SYSTEM\CurrentControlSet\Control\WMI\Level05
  HKCU\SOFTWARE\Microsoft\Office\16.0\Word\Security\Trusted Documents\TrustRecords
  HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost
  HKLM\SYSTEM\CurrentControlSet\Services\AppMgmt\Parameters
  HKCU\Software\Microsoft\Windows\CurrentVersion\Run
  HKLM\Software\Microsoft\Windows\CurrentVersion\Run
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
  HKLM\Software\Microsoft\Windows NT\CurrentVersion\WbemPerf
  HKLM\SOFTWARE\Microsoft\VBA\VbaData
  HKLM\SOFTWARE\Microsoft\VBA\VbaList
  HKLM\SOFTWARE\Microsoft\VBA\Serv
  HKCU\SOFTWARE\Microsoft\VBA\VbaData
  HKCU\SOFTWARE\Microsoft\VBA\VbaList
  HKCU\SOFTWARE\Microsoft\VBA\Serv
  HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings
- **System registry hives:** Upon deployment, Pathfinder performs the following operations:
- **User registry hives smaller than 100 MB:** (ntuser.dat)
- **MFTs from all local disks**

SYGNIA

Sygnia is the foremost global cyber readiness and response team, applying creative approaches and battle-tested solutions to help organizations beat attackers and stay secure. Sygnia is a trusted advisor and service provider of technology and security teams, executives and boards of leading organizations worldwide.
Learn more at Sygnia.co.

A TEMASEK COMPANY AND MEMBER OF THE ISTARI COLLECTIVE

TEMASEK ISTARI

24/7
INCIDENT RESPONSE COVERAGE
Suspicious of an incident? Call +1-877-686-8680 now. Learn more at www.sygnia.co