DATASHEET

SECDO

AGENTS

SECURITY BREACHES ARE INEVITABLE. SOCS ARE ALWAYS ON THE LOOKOUT. COLLECTING EVIDENCE IS NECESSARY FOR INVESTIGATING ALERTS AND THEIR THREAT POTENTIAL. WHY WAIT UNTIL AN INCIDENT HAPPENS TO PERFORM THE NECESSARY DATA COLLECTION WHEN TIME IS CRITICAL AND PRESSURE IS INTENSE?

OPERATION

Secdo provides unmatched, zero-gap, endpoint visibility by continuously collecting all endpoint and server (host) activities.

A single Secdo Agent runs on each host—Windows and Linux—throughout the enterprise. Using negligible resources, the Agent continuously collects all host activities, behaviors and events, and sends them to the Secdo Server where they are stored and accessible.

The aggregate data collected by all the Agents provides absolute, enterprise-wide historical visibility, vital for knowing everything that is happening or has ever happened on any host and across hosts. Extremely granular visibility enables security and IT teams to see how any host, user, or process behaved, to the thread level. Agents provide highly useful support for File Integrity Monitoring (FIM), Endpoint and Server connection monitoring, process monitoring and inventory management.

KEY FEATURES

- **Records every event and behavior from every host and sends it to the Secdo server for long-term storage (100 days or more) and security/IT use**
- **Joins Windows and Linux hosts into a unified monitoring and response regime**
- **Delivers industry-leading, granular, endpoint visibility**
- **Enables easy querying and threat-hunting on any matter of interest**
- **Feeds Secdo's Causality Analysis Engine™ which creates billions of causality chains for automatic alert correlation and validation, and quick investigations and response**
- **Uniquely facilitates remote remediation on any endpoint even while the end-user is working**
- **Works with Secdo Responder to reduce re-imaging by more than 90%**

From each endpoint and server across the network, the Secdo Agent gathers data preemptively, so when incidents occur, forensic investigations can be performed efficiently, taking seconds or minutes rather than hours or days. Transparent to users, the Agent records every endpoint and server activity, behavior and event in preparation for incidents before they happen.

WHAT DOES THE SECDO AGENT COLLECT?

FILES

Dir List, Create, Modify, Delete, Rename, Access, Attributes, ...

PROCESSES

Start, Stop, Child, Parent, DLL, Signature, Hash, ...

THREADS

Start, Stop, Injections, ...

NETWORK

Connections, Failed Connections, Traffic Up/Down, ...

USER

Physical Presence, Screen, Session, Accounts, ...

REGISTRY

Important Key List, Create, Modify, ...

HARDWARE

USB, Physical Presence (Keyboard/Mouse), ...

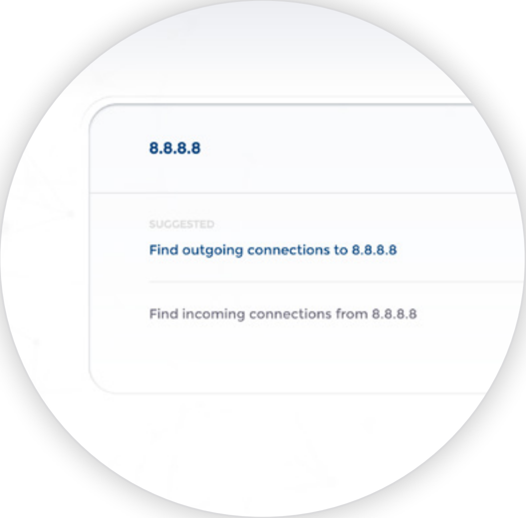
OTHER

Event Log, Host Attributes, Installed Applications, Shares ...

QUERYING AND THREAT-HUNTING

Secdo provides powerful structured and unstructured facilities for easy querying of the host-activity data without limitations. If you can think of the query, Secdo can promptly respond with a helpful display. Answers to questions like these are instantly obtained:

Which users accessed www.ebay.com between 9.41:15 and 9:47:20 on April 2, 2017?... ***What hosts*** are running this Base64 PowerShell script?... ***What versions*** of Chrome are installed and where?... ***Who accessed*** files on a certain sensitive network drive?... ***What files*** were copied from a specific USB on this date?



8.8.8.8

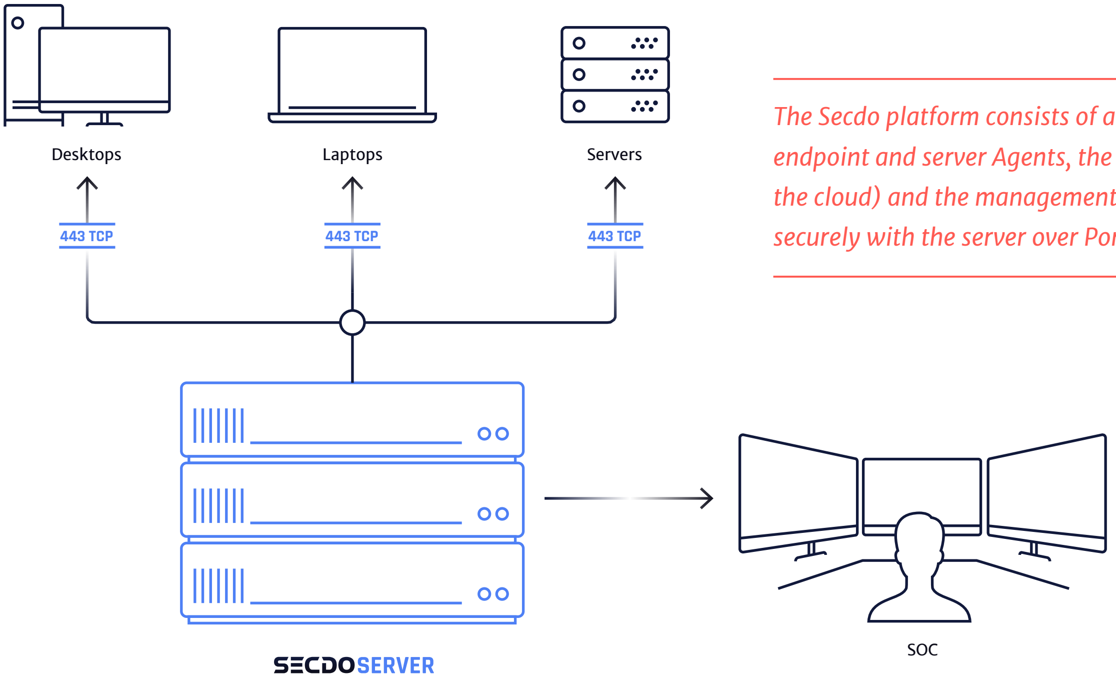
SUGGESTED

Find outgoing connections to 8.8.8.8

Find incoming connections from 8.8.8.8

The data is especially useful for quick and accurate threat-hunting and IOC searches as analysts have the entire database of all host activities and events far into the past at their immediate disposal.

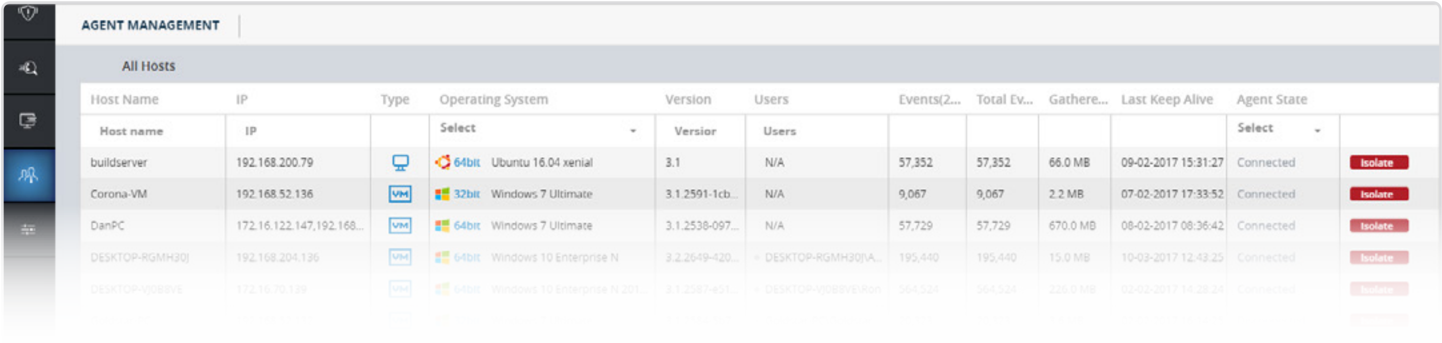
ARCHITECTURE



The Secdo platform consists of an unlimited number of endpoint and server Agents, the Secdo Server (on-prem or in the cloud) and the management console. Agents communicate securely with the server over Port 443 TCP.

MANAGEMENT AND DEPLOYMENT

Agents are remotely deployed and monitored via the Secdo Management Console. The Agent Management function provides excellent visibility over all agents running on thousands of endpoints and servers. The console displays the status of each agent along with information regarding its current operation and accumulated statistics such as how much data it has collected and sent, on what operating system it resides and much more. Agents can be easily stopped and re-started, new versions can be downloaded and more.



Host Name	IP	Type	Operating System	Version	Users	Events(2...	Total Ev...	Gathere...	Last Keep Alive	Agent State	
Host name	IP		Select	Versior	Users					Select	
buildserver	192.168.200.79	🖥	64bit Ubuntu 16.04 xenial	3.1	N/A	57,352	57,352	66.0 MB	09-02-2017 15:31:27	Connected	Isolate
Corona-VM	192.168.52.136	VM	32bit Windows 7 Ultimate	3.1.2591-1cb...	N/A	9,067	9,067	2.2 MB	07-02-2017 17:33:52	Connected	Isolate
DanPC	172.16.122.147,192.168...	VM	64bit Windows 7 Ultimate	3.1.2538-097...	N/A	57,729	57,729	670.0 MB	08-02-2017 08:36:42	Connected	Isolate
DESKTOP-RGMH30J	192.168.204.136	VM	64bit Windows 10 Enterprise N	3.2.2649-420...	DESKTOP-RGMH30J\A...	195,440	195,440	15.0 MB	10-03-2017 12:43:25	Connected	Isolate
DESKTOP-VJ0B8VE	172.16.70.139	VM	64bit Windows 10 Enterprise N 201...	3.1.2587-e51...	DESKTOP-VJ0B8VE\Ron	564,524	564,524	226.0 MB	02-02-2017 14:28:24	Connected	Isolate

Agent Management

ENABLING EFFECTIVE INCIDENT RESPONSE

From the Management Console, analysts can utilize Agents to deliver a new level of powerful remote remediations on individual or groups of endpoints and servers. Remediation is surgical and imperceptible to users and their work.

ICEBLOCK™

Secdo's unique technology freezes execution chains in memory, enabling users to continue to work safely while the malicious process is frozen. Analysts don't have to kill and delete threats, the highly disruptive method used by most enterprises today.

REMOTE SCREEN CAPTURE

Analysts/IR teams/IT can take screen shots remotely from any endpoint to obtain additional evidence for use in the remediation and other IT processes.

ISOLATION

A single click quarantines infected hosts from the network while allowing secure, remote access and prompt remediation.

LIVE FORENSICS

Analysts can collect memory dumps and perform memory forensics remotely, saving time and network resource consumption and avoiding the need to send memory dumps (4-32GB) across the network.

LIVE REMOTE TERMINAL

Analysts and IT personnel can run commands and code interactively (Python, PowerShell, etc.) on any host. They can create their own executables, commands and code for inclusion in the automated investigation process for accurate processing of future alerts and threats.

PYTHON

Builds complex response scripts and scenarios without the need to install Python on endpoints.

SPECIFICATIONS

OPERATING SYSTEMS	Windows, Linux (Beta)
RESOURCES	Less than 1% CPU, 50MB RAM
NETWORK	<5MB of network traffic per day
DATA COLLECTION	Non-stop collection of all activity including: user, file, memory, process, thread, registry, network, USB and more. Everything!
CAPACITY	7TB for 5,000 hosts for 100 days of retention, expandable as needed
TAMPER-PROOF	Kernel-level memory and file system self-protect
VISIBILITY	Thread-level
COMMUNICATIONS	SSL-encrypted