



# RevBits Full EDR Capabilities Protect Air-Gapped Critical Infrastructure

## Table of contents

Introduction.....	3
The National Cybersecurity Strategy outlines defense measures for critical infrastructure.....	4
Critical air-gapped infrastructure is increasingly targeted.....	5
The need for EDR protection within an air-gapped network.....	6
EDR with full capabilities - without Internet connectivity.....	7
RevBits Endpoint Security.....	8
Installing RevBits ES within an air-gapped environment without Internet connectivity.....	11
Cybersecurity forensics.....	12

---

## RevBits product line



Cyber Intelligence  
Platform



Endpoint Security



Email Security



Privileged Access  
Management



Zero Trust Network



Deception  
Technology

## Introduction

**Every industry faces the ongoing challenge of protecting their data and IT resources from cyber attackers. This is particularly true for critical infrastructure within air-gapped networks.** Even though they provide a highly effective barrier against cyberattacks, air-gapped networks are not immune to targeted attacks. In fact, many of our critical infrastructure may already have malware hidden within the systems, biding their time until threat actors determine the right moment to execute the payloads.

Threat actors range from individual hackers to cyber gangs and nation-state-sponsored cyberattack groups. As you might expect, it is the latter who are most capable of infiltrating well protected critical infrastructure to perform cyber espionage, and ultimately initiate the attacks.

There are over a dozen critical infrastructure sectors whose networks, assets, and systems are considered so vital to their countries that if they became incapacitated, it would have a debilitating effect on the nation's economic security and public health and safety. These industry sectors include chemical, communications, manufacturing, dams, military defense, emergency services, energy facilities, financial services, food and agriculture, government agencies, healthcare, nuclear facilities, transportation, water, and others.

## The National Cybersecurity Strategy outlines defense measures for critical infrastructure

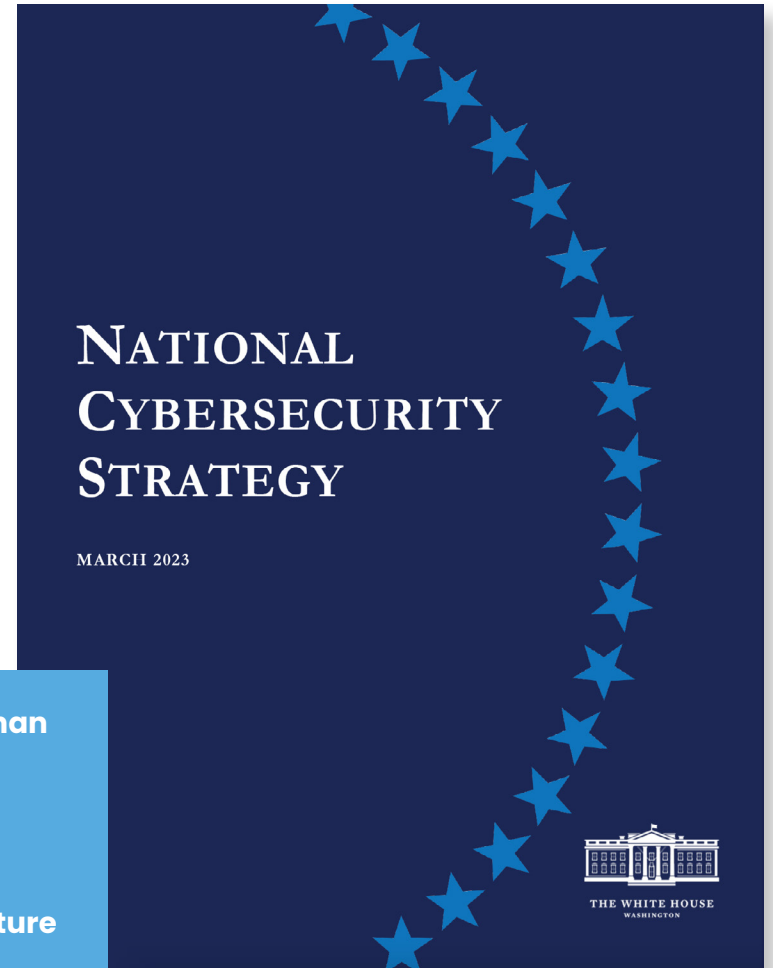
On March 2, 2023, the much anticipated release of the United States [National Cybersecurity Strategy](#) finally arrived. The White House released the comprehensive document that outlines essential changes in how the U.S. allocates roles, responsibilities, and resources in cyberspace. The strategy involves more than 20 government agencies and private sector organizations. It covers cybersecurity weaknesses and challenges from software and infrastructure vulnerabilities to workforce shortages. The strategy includes five “Pillars”, the first of which is “Defend Critical Infrastructure”, as detailed in the excerpt below.

Defend Critical Infrastructure summary:

We will give the American people confidence in the availability and resilience of our critical infrastructure and the essential services it provides, including:

- Expanding the use of minimum cybersecurity requirements in critical sectors to ensure national security and public safety and harmonizing regulations to reduce the burden of compliance
- Enabling public-private collaboration at the speed and scale necessary to defend critical infrastructure and essential services
- Defending and modernizing Federal networks and updating Federal incident response policy

**“The strategy involves more than 20 government agencies and private sector organizations. It covers cybersecurity weaknesses and challenges from software and infrastructure vulnerabilities to workforce shortages.”**



## Critical air-gapped infrastructure is increasingly targeted

While a strong cyber defense is of utmost importance for the United States, every country faces similar security risks. Their critical infrastructure must employ cybersecurity that is highly effective in repelling the most sophisticated attacks from both internal and external threat actors.

All commercial organizations have some level of Information Technology (IT), but for critical industrial infrastructure, Operational Technology (OT) controls and monitors the hardware and software for industrial equipment, assets, processes, and events. OT is deployed within many of the industry sectors listed above to control and monitor industrial control systems (ICS), including programmable logic controllers (PLC), distributed control systems, supervisory control and data acquisition (SCADA) and other mission-critical systems. RevBits CEO David Schiffer recently wrote an article in Forbes that covered this topic entitled [“IT And OT Convergence Need Holistic Cybersecurity Protection”](#).

OT is often found within air-gapped networks, which are completely disconnected from other networks like the public Internet, to ensure isolation. Within a true air-gapped network, IT and security teams maintain strict adherence to ensure total network isolation, both physically and logically.

For the sake of clarity, and to alleviate vendor-defined air gap market positioning, we look to NIST for our air gap definition. “Air gap is an interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control).” Within a true air-gapped network, all software and hardware is completely on-premises. This means no cloud-native and delivered software can be deployed.

Aside from the NIST defined air-gapped environment that is physically and logically separated, some organizations deploy air gap variants that have limited connectivity to clouds and other sources. Regardless of how an air gap network is deployed, RevBits Endpoint Security (ES) provides full features and complete capabilities, within strictly on-premises or hybrid environments.

Because true air-gapped networks are physically separate from other non-air gapped networks, the most effective way for threat actors to infiltrate them is to use external devices, like USB drives, other removable media, and authorized laptops. All these external devices require an authorized person to physically connect and disconnect them, with WiFi and Bluetooth turned off, and Ethernet cables unplugged.

IT and security teams monitoring and controlling critical infrastructure must be hyper vigilant, and their systems must be extremely locked down. This means no public email access to the air-gapped systems. This requires an architecture with browser and email isolation, and all email activity performed within a separate, independent environment.

Because external USB drives are the most prominent method for penetration, organizations must lock down all computer ports from accepting USB devices. The exception is a specific administrator’s machine with specialized software that sanitizes the USB process before, during, and after USB drive insertion.

## The need for EDR protection within an air-gapped network

There are a number of fundamental reasons for deploying Endpoint Detection and Response (EDR) into an air-gapped network, including:

- Detecting and responding to malicious insiders and external bad actors who manage to get malware inside the air-gapped environment
- Conducting forensic investigations of indicator of compromise (IOC), for data, system log entries, and files, with potential malicious activity
- EDR solutions with USB device policies prevent newly added exploits and zero day attacks
- Within an air-gapped environment, software needs to be updated, and thorough investigation must be made to ensure no malware and other exploits are hidden within the update
- EDR provides the necessary protection for when dormant malware activates and executes



**“EDR provides the necessary protection for when dormant malware activates and executes.”**


## EDR with full capabilities – without Internet connectivity

While EDR can be an effective cybersecurity solution to protect air-gapped critical infrastructure, not all EDRs are able to support a true air-gapped environment. An EDR that is capable of being deployed on-premises within the air-gapped network can perform ongoing

analysis of the systems, looking for and removing any found malware. For this to be effective, the EDR must have all of its capabilities and functions intact within the air gap - without Internet connectivity.



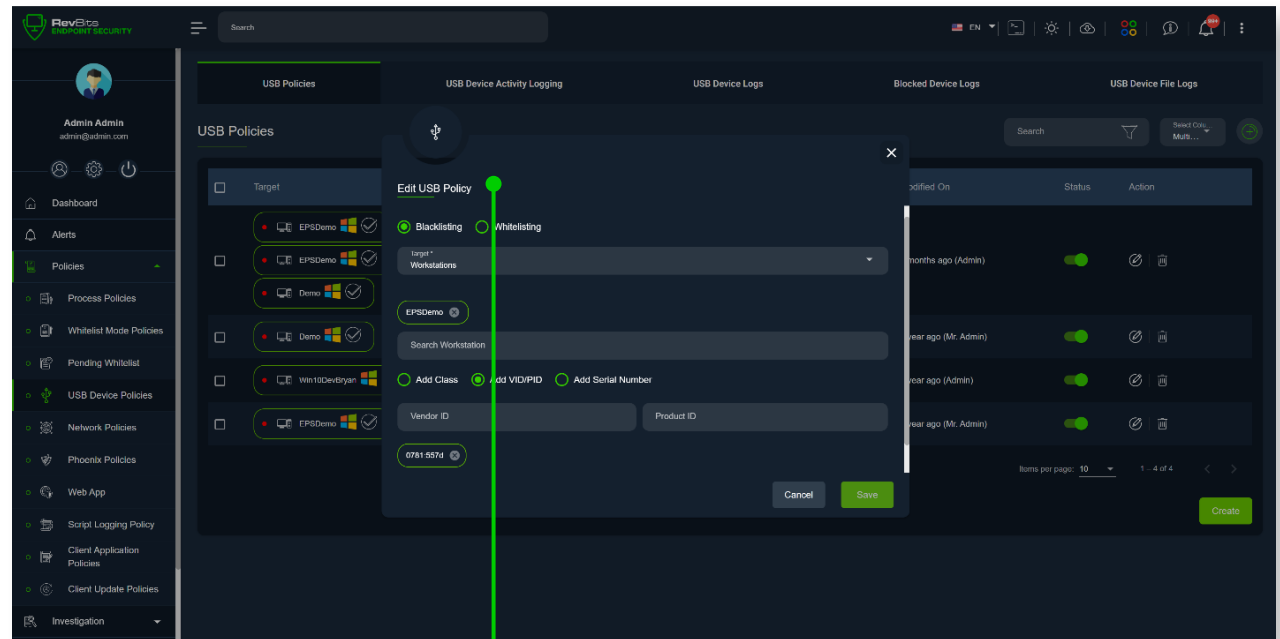
## RevBits Endpoint Security

 RevBits EPS is a unique EDR solution, with its ability to be deployed on-premises within an air-gapped network, with complete user control and full detection and response (DR) capabilities. Every DR feature, and all forensics and mitigation capabilities, are fully functional without Internet connectivity.

As you might expect, because of the nature of air-gapped networks, user administration is more involved. But this aspect is already in place within an air-gapped environment. All RevBits EPS functions run without external dependencies, including licensing, malware detection and blocking, forensic extraction, rootkit detection, USB control, scanning, and analysis.

Within an air-gapped network, RevBits EPS conducts a unique three-phase analysis on all new executables. This includes signature scanning, machine learning and behavioral analysis, which maximizes the accuracy of malware detection and minimizes false positives. Additional RevBits EPS capabilities include:

**USB device management** – RevBits EPS includes USB device policies to whitelist or blacklist all USB devices. Whitelisting and blacklisting can be applied by Vendor ID, Product ID, and device type (e.g. webcams, wireless adapters, storage, etc.).

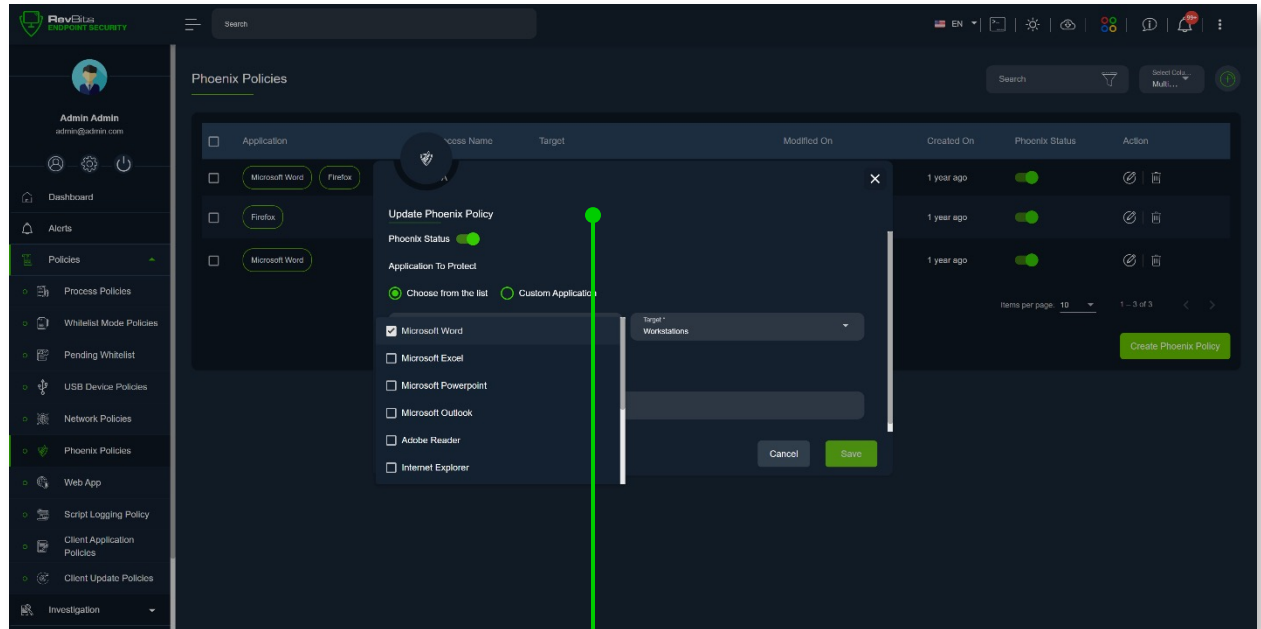


RevBit EPS has a deep and robust USB control policy environment



### Detect and block exploits automatically –

RevBits EPS automatically detects, classifies, blocks and reports exploit attempts of vulnerabilities, including Zero days. RevBits EPS detects and classifies all common exploit techniques, including but not limited to heap overflow, buffer overflow, memory corruption, use-after-free, ROP gadgets, heap spraying, and more..



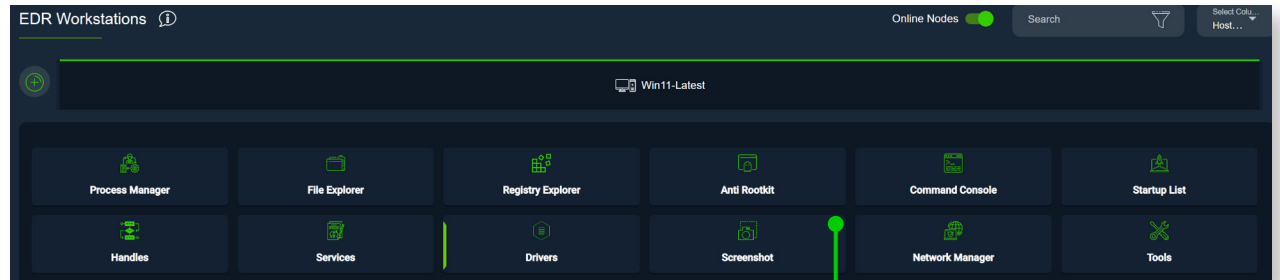
The screenshot displays the RevBits Phoenix Policies management interface. The main panel shows a table of policies with columns for Application, Process Name, Target, Modified On, Created On, Phoenix Status, and Action. A modal window titled "Update Phoenix Policy" is open, showing the "Application To Protect" dropdown set to "Microsoft Word" and the "Target" dropdown set to "Workstations". The "Phoenix Status" is toggled on. The interface also includes a sidebar with navigation options like Dashboard, Alerts, Policies, Process Policies, Whitelisted Mode Policies, Pending Whitelist, USB Device Policies, Network Policies, Phoenix Policies, Web App, Script Logging Policy, Client Application Policies, Client Update Policies, and Investigation.

Protect against Zero-days with RevBits EPSs' native exploit detection engine – Phoenix

### Advanced, patented anti-rootkit protection

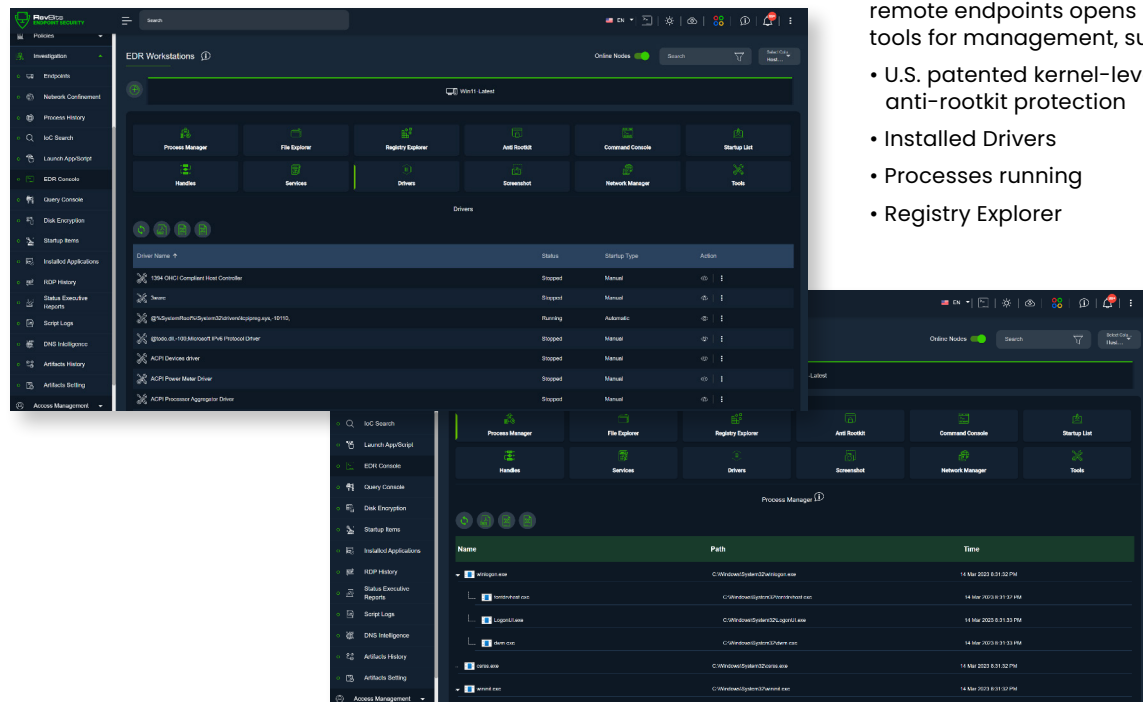
– RevBits EPS patented anti-rootkit protection provides full visibility into the kernel and detects, blocks, and removes all unauthorized signed or unsigned drivers from accessing the kernel. Cyberattacks on Microsoft signed drivers are an increasing threat, and there is nothing a signature-based or behavioral-based anti-virus product can do against them. There needs to be a system and process that enables an administrator to decide which drivers and applications are permitted access to a kernel space.

RevBits EPS includes anti-rootkit software that patches drivers in memory before they access the kernel space. This allows administrators to decide which drivers are allowed, and which are denied access to the kernel space. RevBits has a U.S. patent for detecting and blocking signed and unsigned drivers attempting to access the kernel-level OS. RevBits EPS detects and alerts on known and unknown malicious rootkits, using its unique modeling techniques, and removing them through callback capabilities, whether they're signed by Microsoft or any other CA.



Launching the RevBits EDR module on remote endpoints opens a myriad of tools for management, such as:

- U.S. patented kernel-level anti-rootkit protection
- Installed Drivers
- Processes running
- Registry Explorer



This section contains two detailed screenshots of the RevBits EDR interface. The top screenshot shows the 'Drivers' management page with a table of installed drivers. The bottom screenshot shows the 'Process Manager' page with a table of running processes.

Driver Name	Status	Startup Type	Action
1384 OHCI Compliant Host Controller	Stopped	Manual	[Stop] [Refresh]
Term	Stopped	Manual	[Stop] [Refresh]
@%SystemRoot%\System32\wininit.sys_18110	Running	Automatic	[Stop] [Refresh]
@%windir%\hiberfil.sys_Phibus01.Drivers	Stopped	Manual	[Stop] [Refresh]
ACPI Device driver	Stopped	Manual	[Stop] [Refresh]
ACPI Power Meter Driver	Stopped	Manual	[Stop] [Refresh]
ACPI Processor Agreement Driver	Stopped	Manual	[Stop] [Refresh]

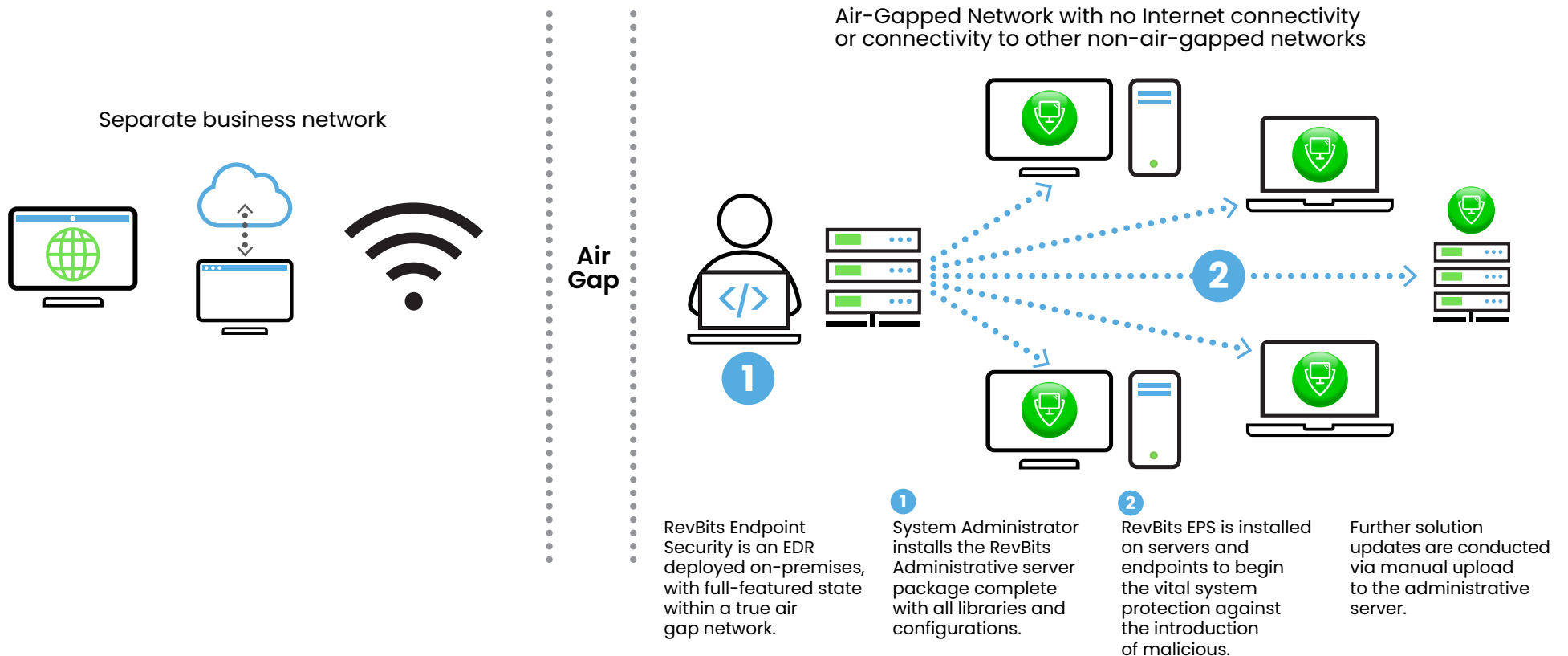
  

Name	Path	Time
System Idle Process	C:\Windows\System32\smss.exe	14 May 2023 8:31:32 PM
smss.exe	C:\Windows\System32\smss.exe	14 May 2023 8:31:32 PM
csrss.exe	C:\Windows\System32\csrss.exe	14 May 2023 8:31:32 PM
System	C:\Windows\System32\System.exe	14 May 2023 8:31:32 PM
System	C:\Windows\System32\System.exe	14 May 2023 8:31:32 PM
smss.exe	C:\Windows\System32\smss.exe	14 May 2023 8:31:32 PM
csrss.exe	C:\Windows\System32\csrss.exe	14 May 2023 8:31:32 PM

## Installing RevBits ES within an air-gapped environment without Internet connectivity

Installing and setting up RevBits EPS software within an air-gapped network is accomplished by loading it onto a secure USB. Admins insert the USB drive with the RevBits software, install it on a dedicated machine, where it is tested and validated before it goes into production. A special

GitHub repository is required for the RevBits software to be loaded. Administrators obtain the RevBits EPS software from the GitHub clone, and install everything locally from the Zipped packages inside the USB.



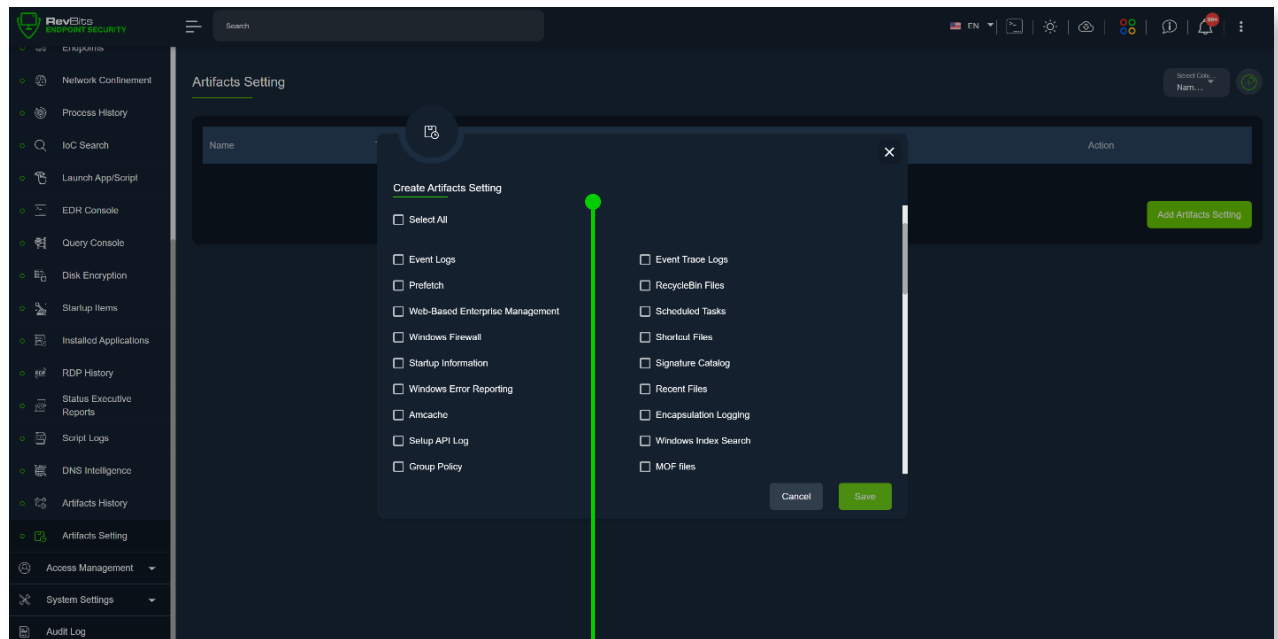
## Cybersecurity forensics

RevBits EPS single button forensics gathers 72 artifacts, such as registry keys, files, time stamps, and event logs. This can be set up to run either scheduled or on-demand. RevBits EPS monitors and controls kernel access, file registries and processes, and will terminate malware actions and anything that looks suspicious or abnormal. RevBits EPS conducts memory dumps with snapshots captured for analysis. The memory dump contains files of all the information stored in RAM prior to a system compromise for forensic investigation and diagnosing attack processes. RevBits EPS provides dump process memory, disk, drive and forensic artifact gathering.

For forensic investigations, RevBit EPS provides access and complete artifact and process trees with complete visibility, and can be exported for immediate investigation. RevBits file manager

provides complete control, enabling admins to see all the files and handles that a process is holding. They can forcefully close any handles that prevent them from conducting their investigation. If a handle to a certain file is encrypting the file,

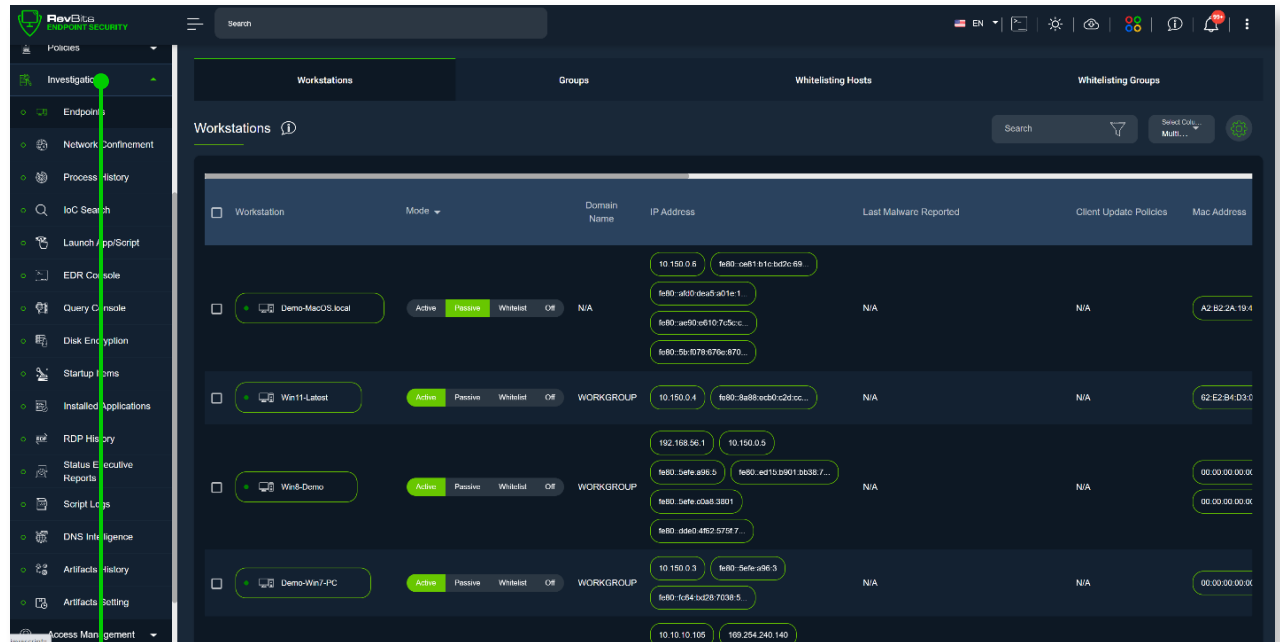
the admin can quickly and easily copy the file and close or delete the filer. This same capability can be accomplished for service lists, process callbacks, and software drivers.



RevBits EPS collects 70+ artifacts on schedule or on demand within the EDR module.

Organizations with critical infrastructure have an urgency in finding and removing cyber threats, and require an immediate response to mitigate them before disaster befalls. Without the right cybersecurity solution to facilitate expedient detection and resolution, security teams can waste precious hours collecting the forensic data they need to thwart an attack and minimize damage.

RevBits EPS is a robust EDR with an intuitive interface that provides full control and visibility over processes, trees, files, registries, handles, command prompt services, drivers, rootkit and kernel, startup items. It provides the ability to dump memory, disk, and drive data for immediate investigations. With any type of network, including air-gapped environments without Internet connectivity, RevBits Endpoint Security provides the full features and capabilities necessary to find, respond, and eliminate even the most sophisticated active threats.



RevBits EPS has the deepest investigative capability. The EDR module offers 20+ endpoint investigative and mitigation tools.

# Keep Your Enterprise Protected. Get a Demo or Free Evaluation.

To learn more, visit [www.revbits.com](http://www.revbits.com)



34 Willis Avenue • Mineola, NY 11501 • 844-4REVBIT (844-473-8248) • [www.revbits.com](http://www.revbits.com)

© 2023 RevBits, LLC. All rights reserved. This material is provided by RevBits, LLC. Further distribution is prohibited. **RB-EB-AG\_(03/2023)**