

Endpoint Security

RevBits Endpoint Security Delivers Robust USB Device Protection for Mission-Critical Networks



The game plan for safeguarding an enterprise from insider threats and external bad actors requires diverse lock-down capabilities without causing business disruption. Mission-critical networks, such as corporate enterprises, government, and public utility infrastructure, rely on removable media, such as USB devices and external hard drives. However, this reliance also opens avenues for potential threats from cyber attackers looking to breach these networks.

Cyberattacks using USB flash drives are one of the most aggressive types of cyber espionage that target public and private sector organizations globally across industries. Among the vulnerabilities, USB devices stand out as a significant weak link, implicated in numerous breaches of air-gapped and non-air-gapped networks. Malicious programs like USBStealer, USBFerry, Fanny, USBCulprit, PlugX, and others exploit these devices.

USB attacks that physically access targeted computers to insert their malware continue to grow. Cybersecurity products must protect against their stealthy ability to bypass security mechanisms to gain initial access to critical networks, including infecting systems within air-gapped networks.

Malware delivered via USB drives targets and disrupts industrial control systems (ICS). Bad actors use USB removable media as an initial attack vector to try and establish remote connectivity for downloading their malicious payloads, exfiltrating data, and establishing command and control.

USB flash drive campaign techniques

USB flash drive campaigns can create a backdoor on the host system, allowing attackers to remotely issue system commands and expand to other USB flash drives to propagate throughout the network. Once the threat actor gains system access, they can execute payloads using the Windows Command Prompt, taking over removable media devices, creating staging directories, and modifying the Windows registry.

An infected USB flash drive can have multiple malicious software that loads its payload in memory through DLL hijacking. The infection chain typically has a legitimate

executable, a malicious DLL loader, and an encrypted payload. When the legitimate executable is run, a malicious DLL file can be side-loaded, loaded with a decrypted shellcode as a .dat file, and executed in memory. The infection can continually drop batch files into the RECYCLE.BIN file path.

To maintain persistence on the system, the malware can create a directory that masquerades as a legitimate program setting the directory attribute to hidden, copying its main components to this directory, and creating a Run registry key with the same name as the directory created earlier. The Run registry keys can then run programs automatically when a user logs on.



Cyberattacks using USB flash drives are one of the most aggressive types of cyber espionage that target public and private sector organizations globally across industries

Malware can include HTTP(S), custom binary protocols over TCP/UDP, and ICMP to communicate with its command and control server. They can support commands, including file transfer, execution, remote



desktop, screenshot capture, reverse shell, and keylogging. It can also copy onto new removable drives plugged into an infected system for malicious payloads to spread to other systems and potentially collect data from air-gapped systems.

Another form of infected USB flash drive lures unsuspecting victims into clicking on a malicious file masquerading as a legitimate executable. The executed malicious file can trigger a chain of executions, each designed to perform its specific task throughout the attack lifecycle. The infection chain typically starts with an executable that is a dropper responsible for writing malicious files to disk and launching them. The encrypted files will contain executables and DLLs extracted and written in the directory. These files can be broken down into multiple components: a legitimate executable and a malicious DLL loaded via DLL search order hijacking.

The shellcode-based backdoor generates a unique identifier based on the system name, username, and volume serial number. This identifier serves as a unique ID when communicating to its command and control server with the domain hard-coded in the shellcode.

The malware can copy itself to removable drives plugged into an infected system. It then creates a folder on the removable drive and copies the encrypted files that

contain the malicious components. An executable is extracted from the file and written to a .exe, which is responsible for removing and executing the content of the encrypted files.

To fortify against these potentially catastrophic breaches, RevBits Endpoint Security (EPS) offers robust policy controls that empower administrators to enforce device whitelisting and blacklisting, including USBs and external hard drives.

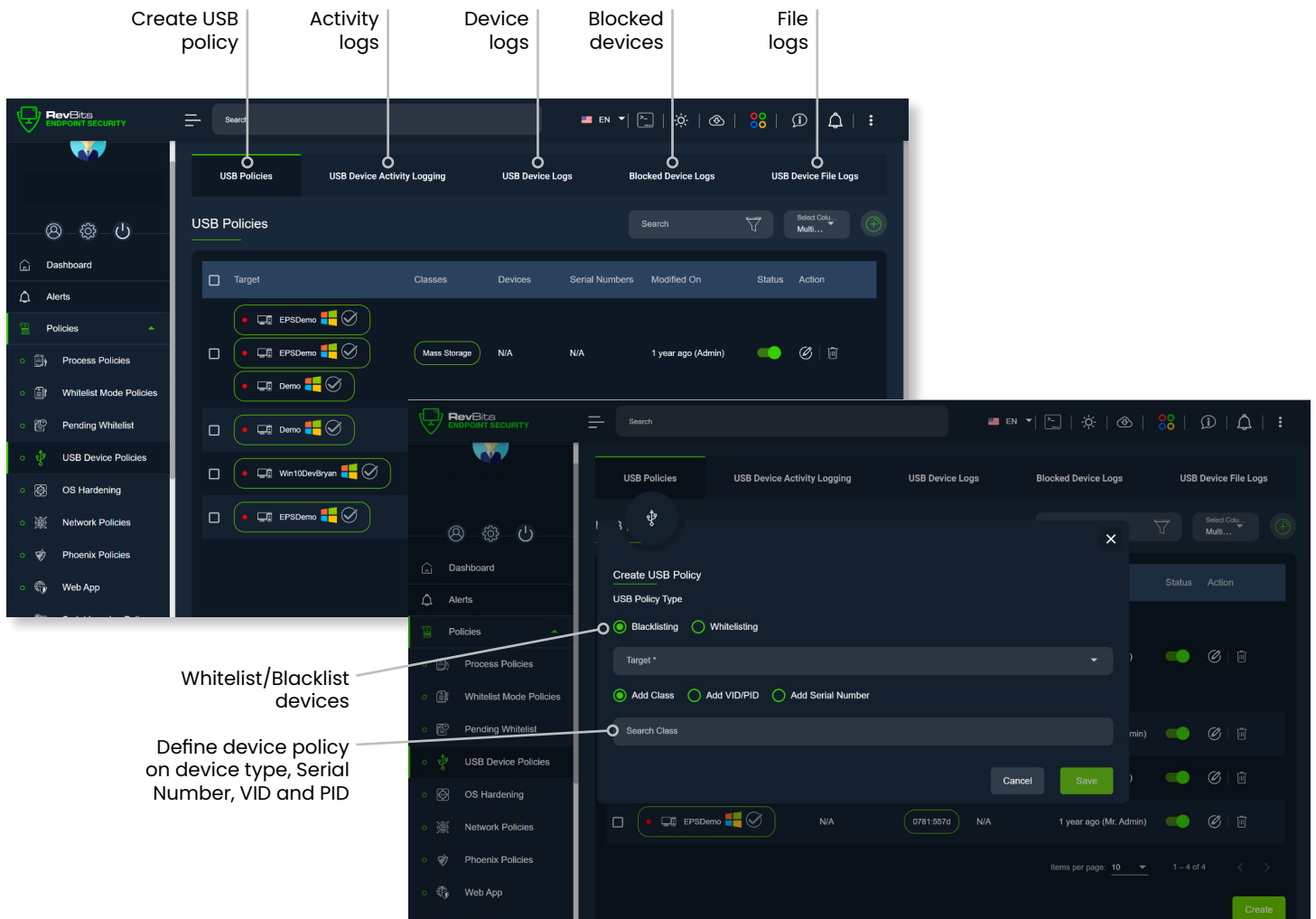
RevBits safeguards organizations from USB-enabled malware and data extraction

RevBits Endpoint Security (EPS) is a multi-layered solution with comprehensive USB device security policies. RevBits EPS makes it easy for IT to restrict any use, or group of users, to specific company-provided printers, external drives, and other USB-enabled devices. It provides administrators with a potent whitelist/blacklist framework to limit or lock-down USB access on an entire network, individual workstations/laptops, and workstation/laptop groups.

IT and security teams have a highly flexible and granular approach to controlling USB-enabled devices, such as external hard drives and flash drives, printers, keyboards, monitors, mice, etc. By policy-enabling workstation and laptop USB ports, as well as USB-enabled device Vendor ID, Product ID, Serial Number, and Device Type, they can address diverse security protections while accommodating the organization's varied business requirements. RevBits EPS secures its enabled workstations and laptops that connect to USB devices on the Internet, off the Internet, "in the corporate office, or remotely anywhere in the world. Even if malware is on a USB device, RevBits EPS will identify and block it before it can load onto a workstation or laptop.

The RevBits EPS security capabilities deliver far more than USB device protection from malware. It also protects organizations by controlling data loss (malicious or not) from insiders downloading internal corporate data and files onto an external drive and taking it outside the company. RevBits EPS allows administrators to whitelist sanctioned devices, so employees and contractors can only use USB devices that the organization has approved and authorized.

This level of control extends to individual laptops and workstations, enabling administrators to turn specific USB ports on or off and limit port acceptance of particular devices. RevBits Endpoint Security addresses the vulnerabilities posed by USB devices and elevates the overall security posture through proactive monitoring,



Labels in the image:

- Create USB policy
- Activity logs
- Device logs
- Blocked devices
- File logs
- Whitelist/Blacklist devices
- Define device policy on device type, Serial Number, VID and PID

The screenshot displays the RevBits Endpoint Security dashboard. The main area shows a table of USB Policies with columns for Target, Classes, Devices, Serial Numbers, Modified On, Status, and Action. A 'Create USB Policy' dialog is open, allowing users to select a USB Policy Type (Blacklisting or Whitelisting), set a Target, and define device policy using Add Class, Add VID/PID, or Add Serial Number. The dialog also includes a Search Class field and Save/Cancel buttons.

RevBits Endpoint Security & EDR offers the most granular USB device policy environment to help control the USB threat landscape.

precise control, and insightful historical tracking. RevBits EPS amplifies safeguarding mission-critical networks by immediately and automatically detecting USB insertions. The security log triggers automatic notifications to administrators through the RevBits admin panel. With a single click, administrators can whitelist or blacklist the inserted device. Whitelisted devices necessitate reinsertion for network login, further bolstering security measures.

RevBits EPS meticulously logs each USB insertion and removal event, regardless of authorization. Unauthorized or blacklisted devices trigger an immediate blockage, accompanied by a detailed “Blocked Devices Log” alert for administrators.

Additionally, RevBits EPS archives historical data, allowing it to identify and alert administrators to malicious insider activity. In cases where an insider attempts to exploit USBs across different computers to gain unauthorized access, the system not only notifies the admin but also provides a detailed history – comprising timestamps, user accounts, USB details, and target computers. Importantly, these capabilities are integral to the RevBits EPS product without incurring extra costs.

RevBits EPS records historical information on all activity. If a malicious insider moves from one computer to another, inserting a USB and attempting to log into Microsoft Windows, RevBits EPS alerts the security admin and provides the historical information that identifies the times, the user, the USB, and all the computers they tried to log into.

Other endpoint security solutions may offer some level of USB whitelisting and blacklisting capabilities, but they fall short in terms of real-time activity logging and instant admin notifications. Often requiring integration with a Security Information and Event Management (SIEM) system, other endpoint security products with USB support are either available as a separate product for purchase or are part of an additional product bundle, requiring an additional cost.

[View](#) our short demo of RevBits Endpoint security's USB features and capabilities to learn more.

Keep Your Enterprise Protected. [Get a Demo or Free Evaluation.](#)
To learn more, visit www.revbits.com