Technical Brief

Global Peripheral Policy
Enforcing Consistent, Context-Aware Hardware Access Across the Enterprise

Introduction

Peripheral devices are essential to modern business operations, but they also create a significant and frequently overlooked attack surface.

USB storage devices, keyboards, network adapters, docking stations, cameras, mobile phones, remote-access hardware, and other peripherals are often trusted according to what they declare themselves to be. Their operating-system classification, serial number, vendor identifier, or device class may appear legitimate even when the hardware is unauthorized, deceptive, or operating outside organizational policy.

This creates a fundamental Zero Trust challenge: an authenticated user and a managed endpoint do not automatically make every connected device trustworthy.

Sepio's Global Peripheral Policy enables organizations to centrally define, apply, and enforce peripheral-access rules across users, endpoints, locations, business units, and device categories. It extends Zero Trust Hardware Access to the peripheral layer by ensuring that hardware access decisions are based on verified device identity, organizational context, and policy.

The Peripheral Security Challenge

Traditional peripheral controls commonly rely on broad allowlists, operating-system classifications, vendor identifiers, serial numbers, or locally configured endpoint rules.

These approaches create several limitations:

- Declared device attributes can be incomplete, cloned, or manipulated.
- A malicious USB device may present itself as a standard keyboard or other trusted Human Interface Device.
- Static allowlists may approve an entire device class instead of a specific authorized device.
- Local policies can become inconsistent across regions, business units, and endpoint groups.
- Blanket restrictions may interfere with legitimate business requirements.
- Security teams may lack the context needed to determine whether a device is appropriate for a particular user, host, or location.

As a result, organizations are often forced to choose between overly permissive access and inflexible restrictions.

Global Peripheral Policy provides a more precise approach by combining verified hardware identity with enterprise-wide policy and operational context.

What Is Global Peripheral Policy?

Global Peripheral Policy is a centralized capability within the Sepio Platform that enables security and IT teams to establish consistent peripheral-access controls across the organization.

Policies can be defined according to factors such as:

- User or user group
- Endpoint or host group
- Business unit
- Geographic or physical location
- Peripheral type or device class
- Approved hardware identity
- Risk level
- Policy status
- Temporary or documented exception

This enables organizations to establish a common security baseline while preserving the flexibility required by different business functions and operational environments.

For example, removable storage may be prohibited across standard corporate endpoints while remaining available to approved administrators, laboratory personnel, or designated operational systems. Specialized peripherals may be permitted within a specific department or site while being restricted everywhere else.

Extending Zero Trust to Peripheral Access

Sepio applies a Zero Trust Hardware Access model based on four continuous stages:

Discover

Identify connected peripheral devices, including known, unknown, unmanaged, misclassified, or potentially deceptive hardware.

Verify

Establish the device's hardware identity rather than relying only on its declared operating-system identity, vendor label, or device class.

Validate

Compare the device against the expected user, host, location, business role, ownership, and applicable policy.

Enforce

Generate alerts, provide remediation guidance, document exceptions, and initiate actions through integrated security and IT platforms.

This approach allows organizations to grant access because a device has been verified and determined to be policy-valid—not simply because it appears familiar.

Why Declared Identity Is Not Enough

A peripheral device can claim to be a keyboard, storage device, network adapter, or other trusted accessory. Conventional endpoint controls may accept this classification without independently validating the underlying hardware.

This is particularly relevant to attacks involving:

- BadUSB devices
- HID-emulation tools
- Unauthorized removable storage
- Rogue USB network adapters
- Mobile-phone tethering
- Hidden remote-access devices
- IP-KVM hardware
- Unauthorized docking stations
- Insider-introduced peripherals
- Third-party or contractor hardware

For example, a malicious USB device may emulate a keyboard and execute automated commands through keystrokes. To the operating system, the device may appear to be an ordinary keyboard, and the activity may occur too quickly for manual intervention.

Sepio addresses this risk by classifying peripherals according to hardware identity, identifying unexpected device classes, and supporting policy decisions based on the specific user, host, location, and device type.

Centralized Governance Without Blanket Restrictions

Global organizations frequently operate across different regulatory environments, business units, endpoint configurations, and operational requirements.

A single rigid peripheral policy may be too restrictive for some teams and too permissive for others. At the same time, independently managed local policies can create inconsistency, administrative overhead, and audit gaps.

Global Peripheral Policy supports a layered governance model:

Global Baseline
Establish organization-wide rules that apply to all users and endpoints.

Contextual Policies
Apply more specific controls to particular departments, locations, host groups, or operational environments.

Approved Exceptions
Permit defined devices or device classes for authorized users, business processes, or time-limited requirements.

Continuous Validation
Reassess connected devices against current identity, risk, and policy information.

This approach enables organizations to reduce peripheral-based risk without unnecessarily disrupting legitimate operations.

From Visibility to Enforcement

Peripheral visibility alone is not sufficient. Security teams must be able to translate device identity and risk into an operational response.

When Sepio identifies an unknown, mismatched, or unauthorized peripheral, Global Peripheral Policy can provide relevant context, including:

- Connected host
- USB or peripheral interface
- Physical or organizational location
- Device category
- Hardware identity
- Policy status
- Risk indicators
- Associated business context

The device can then be compared against the applicable policy and routed into existing response processes.

Depending on the organization's configuration and integrations, actions may include:

- Generating a security alert
- Opening an IT service-management ticket
- Escalating an event to the SIEM
- Invoking a SOAR workflow
- Providing remediation instructions
- Initiating an enforcement action through an integrated control
- Recording an approved exception
- Updating the applicable policy or baseline

This creates a repeatable operational cycle:

1. Detect an unknown, mismatched, or policy-violating peripheral.
2. Locate the relevant host, interface, user group, or location.
3. Validate the device against identity, role, and policy.
4. Respond through security and IT workflows.
5. Learn by updating baselines, exceptions, and future enforcement rules.

Key Use Cases

Malicious USB and HID Emulation

Detect peripherals that present themselves as trusted keyboards or Human Interface Devices while introducing unauthorized functionality.

Unauthorized Removable Storage

Apply differentiated storage policies based on user, host, department, location, and approved device identity.

Insider Risk and Policy Bypass

Identify situations in which an authorized user connects unauthorized hardware to a trusted endpoint.

Rogue Network Connectivity

Detect unauthorized USB network adapters, tethering devices, wireless interfaces, or other hardware that creates an alternative communication path.

Hidden Remote Access

Identify connected IP-KVM or remote-control hardware that may bypass software-based remote-access controls.

Contractor and Third-Party Access

Restrict peripherals introduced by external personnel while allowing approved equipment for defined work activities.

Specialized Operational Environments

Apply tailored controls to healthcare systems, laboratories, engineering workstations, manufacturing environments, data centers, and other specialized assets.

Supporting Insider-Risk Reduction

Peripheral access is often treated as an endpoint configuration issue, but it can also represent an insider-risk concern.

An authorized user may connect:

- Personal storage media
- An unauthorized mobile device
- A rogue access point
- A tethering adapter
- A concealed remote-access device
- A peripheral capable of data collection or exfiltration

Because the user is already authenticated, conventional controls may interpret the activity as legitimate or lack sufficient context to determine intent.

Global Peripheral Policy helps address this issue by validating the hardware attached to trusted endpoints, detecting deviations from permitted device classes, and associating peripheral activity with the relevant host and location.

This extends least-privilege principles beyond the user account and into the hardware-access layer.

Operational and Business Benefits

For Security Leadership

- Extend Zero Trust to peripheral identity
- Reduce hardware-based attack paths
- Establish consistent global governance
- Improve control over authorized and unauthorized hardware

For Security Operations

- Prioritize policy-violating peripherals
- Obtain host and location context
- Accelerate investigation and response
- Integrate findings into existing SIEM and SOAR workflows

For IT and Endpoint Teams

- Replace fragmented local rules with centralized policy
- Reduce manual peripheral administration
- Support legitimate business exceptions
- Improve consistency across endpoint groups

For Compliance and Audit Teams

- Produce continuous evidence of policy implementation
- Maintain traceable exceptions
- Demonstrate consistent peripheral governance
- Reduce the effort required to prepare for audits

Global Peripheral Policy in the Sepio Platform

Global Peripheral Policy is delivered as part of the Sepio Platform's peripheral security and Zero Trust Hardware Access capabilities.

Sepio enables organizations to discover, verify, validate, and control connected hardware across enterprise, branch, data-center, healthcare, OT, IoT, and other critical environments.

Using AssetDNA and hardware-level intelligence, Sepio helps identify known, unknown, unmanaged, and potentially deceptive devices without relying solely on declared identity or network traffic inspection.

The platform enables organizations to translate verified hardware identity into policy decisions, remediation guidance, and integrated enforcement workflows.

Conclusion

Peripheral devices should not be trusted simply because they appear to belong to an approved category.

Effective peripheral security requires organizations to verify the hardware, understand its operational context, compare it against policy, and respond when trust requirements are not met.

Sepio's Global Peripheral Policy provides a centralized and scalable framework for applying these principles across the enterprise. It enables organizations to move beyond broad allowlists and blanket restrictions toward precise, context-aware hardware-access decisions.

The result is a stronger Zero Trust posture in which the right device is permitted for the right user, on the right endpoint, in the right location.

The structure and technical tone follow the attached Sepio technical-brief reference, which presents a technology overview, operational explanation, key advantages, detection methodology, and conclusion rather than announcement-oriented press-release language.