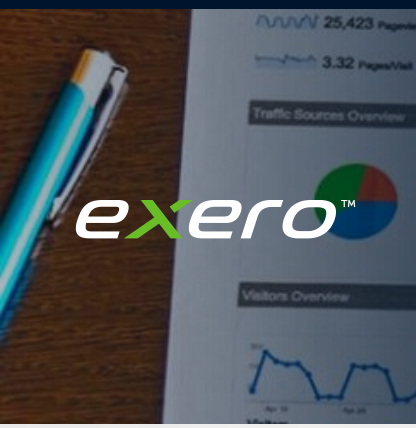
Proactive Security Monitoring and Decision Making with Exero

With **PSB Exero**, you are in command of your world.



EXERO Is the private cloud-based business intelligence tool that delivers data and insight from your interconnected devices and other physical and networked environments through a user-friendly dashboard. Our goal is to put you in command of your world by providing you with Insight that informs, Insight that empowers, Automation that quantifies and provides answers real-time and Knowledge that supports and enables compliance.

Exero provides data regarding the activity as transmitted by security devices, data stores and other networked components within an organization. Designed especially for decision-makers that are responsible for managing, analyzing, presenting data and who need to be deeply informed, including those who are responsible for auditing and compliance.

Exero overcomes challenges of gathering and comparing data from interconnected devices providing real-time analysis and visualization. This provides greater insight into your business, allowing you to be proactive and in control.

The Problem

With nearly 4 million threats released each day, how can you protect your infrastructure from malware, spyware or ransomware if you don't actually know how many assets you really have?

The obsolete break/fix model can result in devastating consequences since issues are only confronted after damage has been done. There is a better, more proactive approach

Common issues from break/fix customers who want a better and more proactive solution.

- I don't know how many devices I have on the Security Network and their IP Numbers
- Camera was off line only to find out when trying to retrieve video.
- We didn't know the NVR stop recording.
- A Windows or Linux service has stopped and we didn't know
- RAID card reporting a errors for a month before it failed. We lost everything.
- No notice that storage is nearing full on a server or NVR.
- I have a smart UPS and Battery needed replacement. I didn't know until we had a power outage.
- Access Door controllers were offline and operating in a degraded mode not accepting new access cards.
- Can the switch on the security network handle any more cameras?

Exero is an extensible platform that informs and delivers actionable insights from security networks

Cybersecurity Insights that are commonly overlooked in the Physical Security Space

- Patches on operating systems are out of date
- Camera has a vulnerable firmware version
- Default manufacturer passwords are in use
- Camera has been tampered with
- Camera performed an unscheduled restart. Why?
- An unknown device has been inserted onto the Network
- Piece of malware or a virus found on server
- Switch or Firewall configuration has changed

Our Services

Identification and Asset Management

- Find authorized and unauthorized devices and software across your infrastructure, and categorize them more reliably into a robust asset inventory system.

Protection and Detection

- Powerful dashboard engine lets you continually monitor mission-critical environments. Set benchmarks & view device history to isolate anomalies, identify trends & more.

Response and Recovery

- Configure alerts to activate processes and automation for incident response.

Exero's performance monitoring first identifies all your devices across your entire infrastructure and categorizes them in a robust asset inventory system.

Identity

- Discovers and inventories servers, workstations, IP and IOT devices
- Monitors for fault conditions – heartbeat, SNMP polling, traps, syslog, others
- Collects installed software and firmware versions
- Reports network devices (such as cameras) using default manufacturer passwords
- Graphically displays topology illustrating device dependencies
- Performs periodic discovery and provisions new assets (or alternatively warns without provisioning)

A powerful, user-friendly dashboard engine protects these assets by continuously monitoring, identifying trends, and detecting anomalies.

Protect

- Enforces 2-factor authentication to security systems
- Manages updates to commonly installed (but vulnerable) apps like Adobe Reader
- Defends against signature (and non-signature) based exploits
- Automates OS patch management and reports missing patches
- Conducts file or volume based backup to local and/or external storage (AWS, Acronis, Azure)
- Network Configuration Management (NCM) backup of switches and routers

Detect

- Live event viewer collects all alarms and notifications
- Live configurable dashboards visualize status and trends
- Notifies of software and patch levels out of compliance
- Notifies when backup image of switch or router has changed
- Reports when thresholds (static or dynamic) are crossed

If something is wrong, Exero's response and recovery will notify the specific responsible stakeholders. If the condition persists, Exero will automatically initiate additional workflow escalations for continuous protection of your assets.

Respond

- Policy based automation to notify and remediate common issues
- Sends emails, text messages, SNMP traps upon alarm conditions being met
- Allows for consistent response to events with an established criteria
- Features built in escalation workflows to alert different levels of management
- Provides information crucial to any forensic investigation

Recover

- Takes automated remediation steps such as restarting a process or shutting down a switched port
- Quick recovery of files or volumes after an incident
- Backups mountable as VM's to virtually any hypervisor platform
- Supports vPro for out of band maintenance

Dashboard Extensions to Application Layers

Get Connected with Us

Have Questions ? We would love to answer them! Demo's available – Contact us to set up an appointment.

43 River Road
Nutley, NJ 07110

(844) 72-EXERO

www.psbexero.com