

The Technology of NOX: An Explanation

Executive Summary

Currently marketed security systems require manual monitoring of captured video. Alerts and alarms reveal only movement of doors, not movement of specific items. Hidden objects are missed by the security equipment. As a result, commercial and government security systems in place today provide only an illusion of security, and offer a placebo in place of asset protection. Given the reliance on human intervention, business losses are not significantly reduced through conventional security measures.

NOX Defense systems provide a combination of active and passive RFID, proprietary NOX technology, Expert Systems, and Business Intelligence Systems, dynamically operational in an undetectable surveillance and response system. This system operates in an unattended environment, alerts designated executive and response teams to a breach, sets off response and reset protocols, and collects forensic evidence in high definition video and court-usable reporting. Interested government and commercial parties may submit their environment for an analysis for suitability for implementation.

What is the business threat?

According to the American Management Association, employees steal over a billion dollars a week from their employers. It takes \$20Billion in sales each week to cover the losses. In most businesses, declining profits, unexplained inventory shortages, and whispered rumors around the office are the only indicators of what is happening. Threats from a professional robber may be unlikely, but 95% of all businesses are hit by an “inside job”. Victimization by employees is the rule, not the exception in American business, and 90% of insider employees are susceptible to the kind of minor pilfering which seems trivial, but adds up to a sizable loss. Managers are reluctant to ask questions and search for answers, because trusted employees feel offended by the suggestion that they might be thieves.

A University of Florida study sponsored by the National Retail Federation says 47% of retail shrinkage in 2006 was due to employee theft, while only 32% was attributed to shoplifting. The rest, it seems, was administrative or vendor error. Indeed, a Deloitte study reveals that most companies cite human error as their prime security concern. If our only way of finding the source of inventory shrinkage is to hire a human being to sit and watch a grainy videotape 24 hours a day, human error does become an overwhelming consideration. We’ve all seen enough Miami Vice reruns to recognize that the “stakeout” is a highly inefficient method of ensuring asset security. Given the state of security technology, we have two choices. We could surrender, and plan on significant inventory losses every year. Or, we could drive ourselves crazy with locks and counter-locks, passwords and secret handshakes, fences, gates, and video monitors that only provide us the illusion of security. Too often, we put in extensive camera systems, only to find that we can’t sustain the work involved in keeping the cameras watched by a human eye. That human eye is too fallible to provide the level of security business needs. In fifteen minutes of staring at a screen, the human eye stops seeing what’s really there.

The Technology of NOX: An Explanation

How serious is my risk?

If you have something to insure, you have assets at risk. Whether it is equipment, inventory, or proprietary documents, you have a stake in both securing them from theft, and catching the thief if your security fails. Do you need to know if the receptionist in your Atlanta office is passing new product designs to her boyfriend who works for a competitor? A grainy videotape watched by a human guard won't tell you that.

Are you worried that your top sales executive is sneaking contract information out of the office in his socks? You'll get no help from a conventional video system there, either.

If you're wondering why that counter you installed on the copy machine keeps counting up, while the log doesn't record the activity, you'll have nothing to analyze from your standard security information on that issue.

Are you confused over an inconsistency in the inventory coming in and the shipments going out? You'll get nada, from your in-house security logs.

And if you're baffled by a shortage of PC equipment, printers, monitors, when you're sure you ordered enough to go around, don't even think of asking your security system what happened there.

Unhinged by your office supply bills? Squeezed by an economic downturn that means pennies have to count? Outraged by the helplessness of knowing you're being ripped off, but not knowing what to do about it? It does no good to build fences, lock locks, collect fingerprints, capture videos, issue passwords, and patrol perimeters, if you cannot detect the theft as it is happening, if you cannot see the thief in the act, if you cannot identify the culprit, and if you cannot do it with the routine and the stamina of a machine, instead of the human vulnerability of an employee, set to the task of watching.

If your security depends on the stamina of human eyes, the immediacy of human responses, and the flawed human skill of detection, your security is significantly limited. Your security is an illusion.

What neutralizes my problem?

"It takes a criminal twelve seconds to defeat a lock or fence. Yet, we spend hundreds of thousands of dollars to create fences that only provide an illusion of security. NOX creates a virtual perimeter that tells us who is penetrating that perimeter, when they are doing it, and where it's happening. With this information, we can respond with the appropriate level of force and prevent further penetration." --- a Naval Criminal Investigative Service (NCIS) commander

Some things are best done by people. Responding with appropriate force to a threat, is an example of a task that belongs to human beings. Choosing and deciding a strategic direction, is an example of a task that is done best by human beings. Identifying a goal, is a task best left to humanity.

The Technology of NOX: An Explanation

Meeting a challenge, rallying to a cause, overcoming an obstacle, and leading an adventure, are all human tasks, best assigned to a living and breathing organism.

But counting, watching, monitoring, checking, and minutely observing every detail of a scene? Seeing through walls, clothes, briefcases, and obfuscations, to find a hidden object? Noting the movement of an object six inches? Putting out an alert when a condition is changed? For this kind of excruciating detail, exacting precision, and mind-numbing calculation, we are best-served by the routine and repeating abilities of a machine. The more successful we are at removing the element of human error in this process, the more effective our security will be.

There is serious motivation to deploy NOX Defense as a replacement for traditional security measures, in government and commercial installations. When there is no longer a need for personnel to watch the monitors, the people you hire can focus their efforts on productive response.

The NOX: Intelligent Perimeter Defense system uses Radio-Frequency Identification (RFID) in both active and passive forms, along with proprietary nano-intelligence (NOX chips) to provide you with:

- ***Clandestine Surveillance:*** Readers hidden inside walls, ceilings, air vents. Item tags, discreetly placed, sprinkled, and undetectable. Customers, suppliers, and employees need not know how and where your valuables are monitored for movement or removal. Maintenance and installation teams know how to keep it secret.
- ***Triggered alerts:*** No longer do you need personnel to watch or review security tapes. An event that triggers perimeter security sends an alert instantly to a designated phone, cell, Blackberry, or iPhone. It can lock the gates first, and call your response team simultaneously. NOX technology allows you to see the theft in high definition, as it happens, even if the stolen object is inside a briefcase, under a jacket, or stuffed in a sandwich wrapper.
- ***Property protection:*** Select the assets you wish to protect, tag them discreetly with NOX tags, and the system will ensure that you always know where they are and who's got them. Even if your valuables are documents, NOX will track them as they move through your building, identify them as they lay in an inbox, and capture video of them if they grow legs and try to walk out the door. Like the hen that laid the golden eggs in Jack and the Beanstalk, your valuables will squeal for help automatically if some dastardly vandal tries to steal them.
- ***Evidence and compliance:*** When the time comes that you need to prove something, high resolution video, trackable identification, and an effective map of the movement of your assets will show intent and actuality for any type of dispute.
- ***Forensic analysis and theft recovery:*** NOX systems don't end when the squealing items walk out your door. Pattern identification, communication, response, and reconstruction components of the system handle the procedures for analysis after the fact, too. The NOX

The Technology of NOX: An Explanation

system will help you get your assets back, and identify your thief. With NOX, you will know where your valuables are. You will know how to keep them safe.

How can I get this system in place?

Every NOX Defense system consists of the following pieces. Each delivered system addresses all components of the system in some form, although the extent of each component is different in each case. The system responds in an entangled, organic process, in keeping with its model as a nano-intelligence. In terms of understanding how it operates, we can think of it as similar to the human immune system: it sets boundaries, detects threats, recognizes anomalies and intruders, patterns responses, alerts the response teams, sends out the emergency protocols, updates the databases with new information, reports the events, resets the alarms, creates a record, and updates protocols based on lessons learned. It does this in the “subsystem”. When the humans are called in, the action and its consequence are laid out and ready to resolve. It is an intelligent perimeter defense system, not a set of networked cameras and locks.

Components of NOX:

The Boundary System

Every system needs a “skin”. The boundaries of your NOX Defense will be defined by walls, windows, doors, fences, roads, gates, or even geographic coordinates. You will choose a clearly delineated, closed and contained area to be defended. Access points will be portals into the area, defended by sensors, readers, cameras, and passkeys. Areas that are not designated access points will be protected with sensory equipment. Procedures and rules for entry and exit will be defined by you, in concert with the NOX installation team. Your NOX system will implement the rules you design.

The Detection System

At non-portal areas of the boundary, NOX detection systems patrol the border. Breaks in the beam set a process in motion. Nothing goes in or out through a non-portal without setting off the alerts. Any break in the wavelengths is read as an intrusion, so jamming and interference is impossible. At portal areas, detection systems read the rules of entry and exit, as defined by you, the customer. Any detection information is collected and communicated to the database of the Pattern ID system. Movement through the area can also be identified, depending on the Boundary rules you, the customer, initially specified.

The Pattern ID System

Here’s where the rules identify Friend or Foe. Patterning rules in the NOX recognize authorized or unauthorized movement, entry and exit. Patterning rules determine whether the movement should be alerted, and what form of response it should call out. Feedback systems reach ahead to response

The Technology of NOX: An Explanation

and reconstruction of the events, dynamically changing in response to situations defined, and situations learned.

The Communication System

If the break in the beam, or the movement identified is determined to be “Foe” by the Pattern ID system, the communication system is activated. An Alert Notification protocol is defined, identifying who should be alerted, under what circumstances, and in what order. The alerts begin automatically, in response to the breach. The alert system is unique to the organization being defended, and is set to arm the Response System.

The Response System

Based on the results of the Alert Notification Protocol and the Patterning Rules, each organization defines its own Response Protocol. This is the set of rules which defines what level of response will be set in motion. The responses and their patterns could range from calling 9-1-1 to sending in a SWAT team. The building could be locked down, the gates secured. The Response Protocol will describe each organization’s decisions about how to respond to each type of breach. The Response system includes reports, including high definition video capture of the exact event, for forensic analysis.

The Reconstruction System

Each organization will define its own Reset Protocol, to return its system to steady state after an event has occurred. The Reset Protocol includes a review of forensic reporting, so that information learned from the breach can be incorporated into an update of employee training, and a strengthening of the organization’s perimeter defense systems based on lessons learned.

Conclusion

The NOX Defense system is a revolutionary surveillance technology, based on passive and active RFID, combined with Expert Systems, Business Intelligence Systems, and “NOX Chips”. It operates in an interactive and dynamic process, leaping back and ahead to ensure organic coverage of its assigned duty. Most importantly, it solves a business problem which was previously gapped in its resolution: it provides unattended surveillance, in a rules-based environment, which allows security breaches to be captured and acted upon in a timeframe that catches thieves.

NOX technology is proceeding through the patent process. Interested parties may apply for analysis of their environment for suitability for a NOX Defense solution.