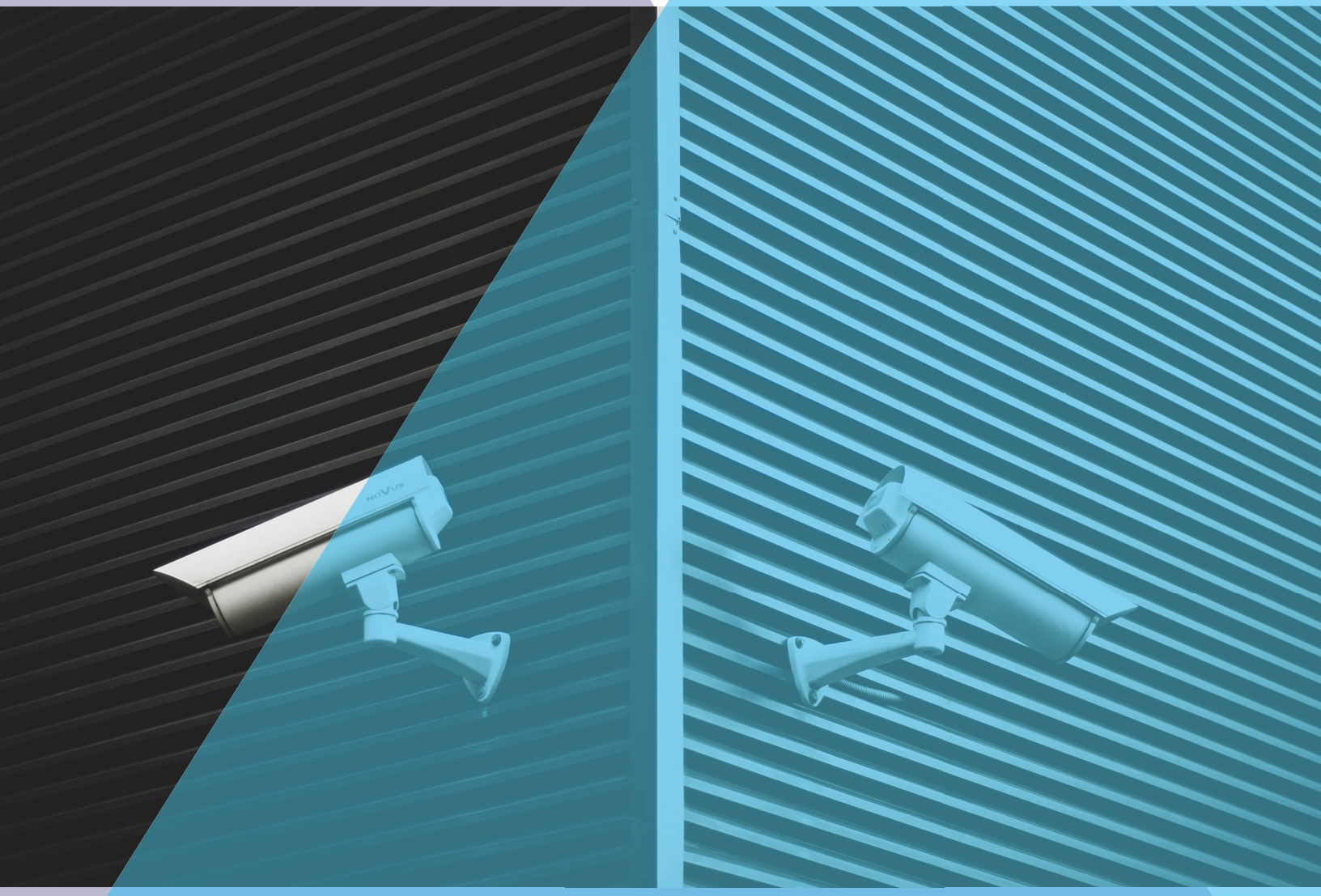
Altronix®

WHITE PAPER

MITIGATE SECURITY VULNERABILITIES WITH NETWAY SPECTRUM SERIES SWITCHES



DECEMBER 2023

Introduction:

Today's modern security and surveillance installations incorporate networked connectivity between devices such as door controllers, cameras, etc. and their respective management systems. The advantages attached to these networked systems are apparent, however it must be recognized, that they may also present intrusion vulnerabilities if not properly designed.

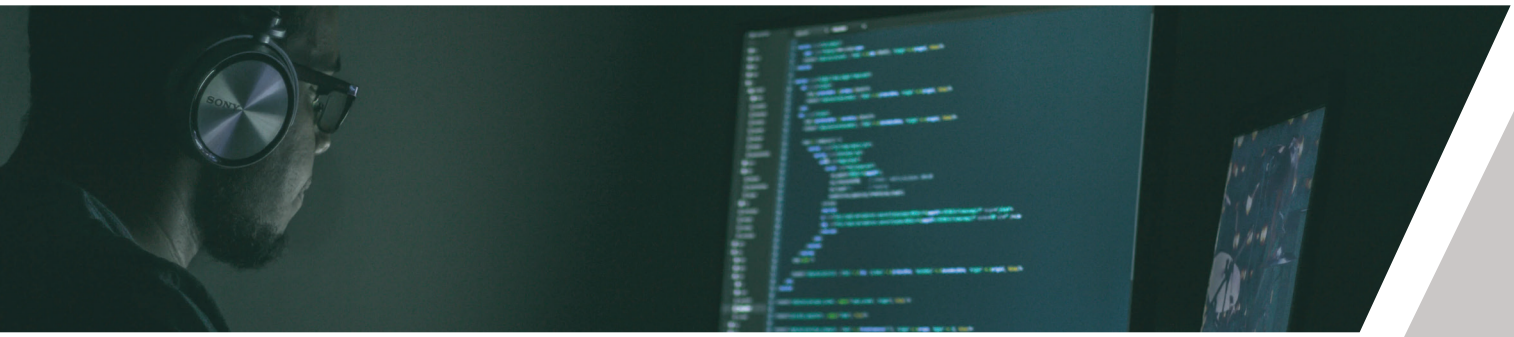
There are potentially multiple attack opportunities exposed to a security system. In broad terms, these threats may be assessed by point of entry into the system;

An inside job, whereby an authorized employee may exploit their trusted position[1], or security credentials are inadvertently offered to a phishing expedition or other forms of stealing credentials by unauthorized players.

Penetration via an networked device of opportunity[2], i.e. a switch, router, edge device or management software.

Item 1, deals with amorphous human factors that must be addressed by protocols, such as multi-factor authentication, personnel vetting and training, etc. and is outside the scope of this paper.

Item 2, however, is a more crystallized subject whereby hardware and software penetration surfaces into a system can be identified, quantified and addressed in a more explicit manner to mediate or in some cases eliminate threat of attack through certain networked devices.



This document describes a special class of **Altronix** products that erase a device direct cyberattack surface and thus are inherently safe to attach to the network as further explained.

It is important to understand methods of attack.

Physical Attack - All network equipment should be securely installed to minimize the ability against a physical attack on a network infrastructure, such as by cutting a cable or entering a secured equipment closet to vandalize it. As no system is completely protected against all forms of a physical attack, the system should be capable of issuing alerts or heartbeat signals to recognize an potential assault or gross system malfunction.

Cyberattack – This form of attack may present the greatest security threat since the attack surface is less visible and potentially can penetrate deeper into a system. With respect to a device, such as a POE switch, the attacker may attempt to reconfigure the switch, shut down a critical port or disable a POE output, thus depowering all other devices attached to its port.

Examples of vulnerabilities and their mitigation:

Example 1 - Many software vendors will configure their product with “backdoor” technology so to provide services such as software update management and authorized maintenance for their end users. This legitimate design feature is increasingly being exploited [4] by sophisticated attackers who rely on these backdoors for malicious purposes.
Altronix Immunity - Altronix removes this attack possibility by not providing backdoor technology in this special class of reduced attack service product.

Example 2 - Software supply chain attacks are increasingly becoming an attack vector for intruders. As more software vendors rely on publicly available open source projects, attackers are finding it increasingly easier to breach their targets by manipulating the software dependencies of products for which their targets depend on[5] [6] [7] [8] [9].

Altronix Immunity - Altronix removes this attack possibility by not deploying any software solutions on this specific class of products.

How does Altronix Eliminate a Cyberattack Surface:

It should be noted, that while Altronix eliminates direct cyberattack surface vulnerabilities with respect to its equipment, other procured upstream and downstream equipment should be evaluated for any surface vulnerabilities they may have.

Altronix achieves this inherent immunity by designing a class of Standalone POE network switches, which eliminates susceptibility to the most notorious attack vectors.

Altronix Standalone class of POE network switches, eliminates these attack vulnerabilities by designing a product that operates without any form of management software or execution environment nor is there an ability to host an IP address. This restricted environment completely eliminates any susceptibility to an API or malware threat, In brief there simply is no form of software to exploit.

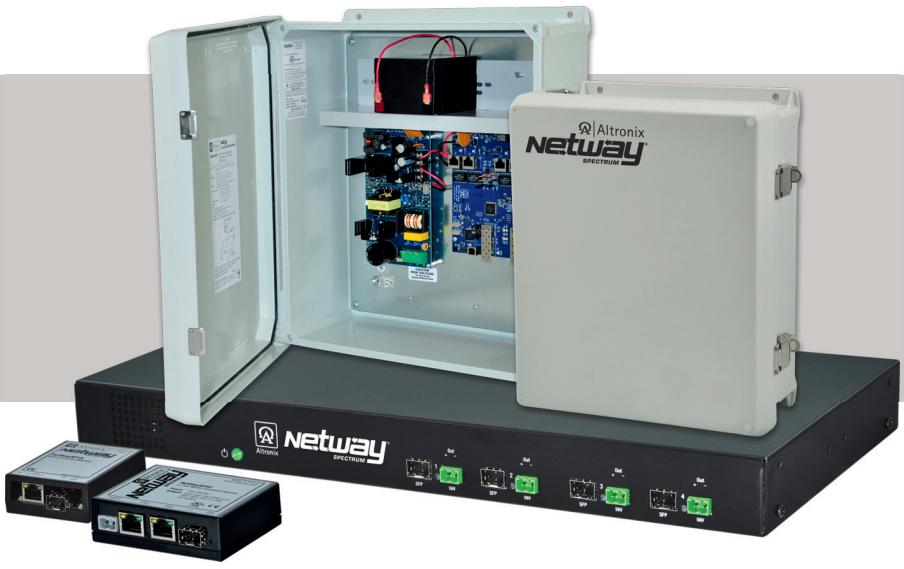
The POE switch is implemented and operates in a pure and streamlined hardware manner and cannot be reconfigured in any form.

Altronix Standalone Class of POE Switches:

The following series of Altronix Standalone POE switches with the inherent attack immunity as described above are:

Fiber POE switches
NetwaySP41WP Series, NetwaySP41BTWP(3) Series, Netway4E1 Series, and Netway4E1BT(3) Series

POE and non-POE switches:
Netway5P, NetWay5BT, Netway5A, and Netway5B



Conclusion

The ever-increasing complexity of modern security and surveillance network infrastructures has given the malevolent players undue opportunity to attack these systems. Altronix' Standalone POE switch products helps tip the scales back in favor of the defender, by eliminating unnecessary complexity, and adding the essential intelligence, switching and POE features via a robust hardware only implementation. When there is no software available to exploit, your system becomes inhospitable to a cyberattack.

References:

[1] Disgruntled employee
[2] Unpatched router firmware
[3] Mirai
[4] Solarwinds
[5] Dependency confusion
[6] Attackers steal 100k npm user credentials
[7] PHP backdoored
[8] Rogue opensource maintainer
[9] Rogue opensource maintainer