NETWITNESS

Zero Trust Architecture and NetWitness Platform XDR

Discussion of How NetWitness Platform XDR is a Key Component of a Zero Trust Architecture

Version 1.2

Contents

This document is a short internal discussion of Zero Trust Architecture and NetWitness XDR Capabilities

Zero Trust and XDR

Are XDR and Zero Trust just two new security buzz words? There is a lot of talk about both, but the question you may be asking is, “Are they related, if so, how?”

To level set the conversation let’s look at the two terms. The premise of Zero Trust is around the idea that enterprises should not inherently trust any attempt to connect to a business system or application and must be verified before any level of user access is granted.

The premise around XDR is that XDR collects and automatically correlates data across multiple security layers – identity, asset, user, endpoint, email, server, cloud workloads, and network – so threats are detected faster, and security analysts improve investigation and response times.

How Did We Get Here?

Before we examine if these relate, we need to understand why they are such a relevant topic.

The way in which organizations operate is changing due to seismic shifts in the way employees access information and other macro-pressures from the last 18 months, primarily the global pandemic. These new realities are forcing organizations to accelerate their digital transformation by expediting large transformational projects.

This results in a massive shift and expansion of the threat landscape at a faster pace than most would have expected. These are created in part by:

- Embracing remote workers who access sensitive information from many devices spread across the globe.
- A changing approach to data storage is causing many organizations to migrate their traditional physical data centers to flexible and dynamic cloud infrastructure.
- New applications being developed, adopted, and moved to production at a rapid pace, often using publicly available code structures.

As this adjustment is embraced it brings along increasing security challenges that coincide with the respective areas of change. Namely...

1. The expansion of connected users and devices from remote workers that extend beyond the physical boundaries of the company.
2. Third-party infrastructure that diminishes an organization's ability to administrator granular controls.
3. Rapid adoption of new software with wide ranging code-bases and versions, often outside the purview of an organizations’ control.

Organizations need to rethink security in the present and future. Any device attaching to the network, any application being moved into production, and all users must be scrutinized.

This is the new normal.

Zero Trust Is a Requirement of the New Network Perimeter

The erosion of the security perimeter paved the way for zero trust requiring organizations to find new ways to establish trustworthiness.

There is a statement in this blog that states, “Where traditional security says, ‘trust but verify,’ zero trust says, ‘never trust, always verify.’ Zero trust security never really 'clears' anything. Instead, zero trust considers all resources to be external to an organization's network, continuously verifying users, resources, devices, and applications before granting only the minimum level of access required.”

Zero Trust is proving to be a strong solution to addressing security holistically with the ability to keep up with the shift and expansion of the threat landscape.

If an organization implements tenet of Zero Trust, they have a significant risk-reduction when they accelerate digital transformation initiatives. For example, rapid adoption of new software applications, or a new IaaS provider for a critical project, all become a natural part of your ‘security-glue’ because Zero Trust assumes nothing is trusted until it proves itself to be trusted.

Keeping this in mind, security organizations need a mechanism that constantly surveys the environment and identifies known risks and emerging or unforeseen new threats across every attack surface anywhere in this modern expanded infrastructure.

XDR as a Key Component to a Zero Trust Approach

The National Institute of Standard and Technology (NIST) looks at Zero Trust[1] and puts forward that visibility is a key requirement for a Zero Trust Architecture. Below we call out some excerpts that reference the need for deep visibility and speed of detection.

1. Zero trust architecture is an end-to-end approach to enterprise resource and data security that encompasses identity (person and nonperson entities), credentials, access management, operations, endpoints, hosting environments, and the interconnecting infrastructure.
2. Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently (including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others.
3. An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects.
4. All traffic is inspected and logged onto the network and analyzed to identify and react to potential attacks against the enterprise. However, some (possibly the majority) of the traffic on the enterprise network may be opaque to layer 3 network analysis tools. This traffic may originate from non-enterprise-owned assets (e.g., contracted services that use the enterprise infrastructure to access the internet) or applications/services that are

[1] NIST Special Publication 800-207, ”Zero Trust Architecture”: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

resistant to passive monitoring. An enterprise that cannot perform deep packet inspection or examine the encrypted traffic must use other methods to assess a possible attacker on the network. That does not mean that the enterprise is unable to analyze encrypted traffic that it sees on the network. The enterprise can collect metadata (e.g., source and destination addresses, etc.) the encrypted traffic and use that to detect an active attacker or possible malware communicating on the network. Machine learning techniques can be used to analyze traffic that cannot be decrypted and examined. Employing this type of machine learning would allow the enterprise to categorize traffic as valid or possibly malicious and subject to remediation.

5. Network Requirements to Support Zero Trust Architecture: The enterprise can observe all network traffic. The enterprise records packets seen on the data plane, even if it is not able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE as it evaluates access requests.

XDR Delivers Comprehensive Visibility

The NIST Paper referenced above specifically calls out the need for deep visibility in the network. If Zero Trust requires organizations "…to collect data about security posture security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement", then having the ability to abstract data from every data source across the endpoint and network becomes more important.

Layer on top of this the ability to use machine-learning based analytics to identify anomalies such as new endpoints or users, or anomalous changes in behavior, and XDR becomes a powerful way to trust, but always verify those end devices. Leveraging automation actions through orchestration and automation when endpoints or users are deemed risky takes this approach a step further to ensure assets are swiftly removed when their trustworthiness is brought into question.

For organizations adopting a Zero Trust model the visibility of XDR should be viewed as a key requirement in this strategy.

Speed Detection and Reduce Dwell Time

Referring to the same NIST paper, 'Zero trust security models assume that an attacker is present in the environment and that an enterprise-owned environment is no different—or no more trustworthy—than any non-enterprise owned environment'.

If we do the analogy in our lives, imagine a stranger hiding in your residence in an area lacking surveillance going unnoticed; the consequences threaten both the assets you own and your own safety. Being able to quickly react and respond is essential and our human brain, one of the most sophisticated neural networks, is trained to react quickly to those emergencies.

XDR is a zero trust enabler when it comes to elevating the speed of detection; a very important concept if we consider an attacker is already present. To thwart attackers and reduce dwell time; it is imperative to act fast and be able to quickly analyze Indicators of Compromise and Behavioral anomalies in a central location having all contextual information related to the business asset, identity and threat intelligence across the endpoint and network infrastructure.

Incorporating identity awareness and understanding doubles down on the idea of zero-trust architectures speeding detection and response processes by aiding the response process with additional data enrichment and context. With access to end-user entitlements at your fingertip while carrying out an investigation, an XDR platform becomes more efficient in invoking authentication mechanisms when a breach or threat is suspected. For example, invoking a step-up authentication mechanism leveraging biometrics as a response to an XDR-identified anomaly. This is a powerful enabler for the SOC grounded in zero-trust principles