Zero Trust Cybersecurity Model and the organizations offering them.

Ernst and Young LLP - Blog

By Jatin Dua, Senior 4, Ernst and Young.

Table of Contents:

1. The constant threat we are facing

The evolution of IT over the years has come up with various challenges pertaining to keeping our IT parameters secure. Business organizations have constantly kept an eye for a better security balance with respect to their critical business operations. So much so that businesses keep a segmented budget to keep their information secure. Organizations leave no space left to protocol, monitor remediate and improve their security parameters and yet try to strike a fine balance between information security and business operations. Perimeter-focussed security architecture is a by default high trust level for keeping internal network secure.
While multi-level security architecture is readily available in the market, yet, Perimeter-focused security architecture continue to fail drastically and costing huge penalties to the enterprise. Some examples to the recent huge cybersecurity failures are:
Aadhar – 1.1 billion users data breach;
Marriott Starwood Hotels – 5 million guests accounts copied;
Exactis – 340 million users data breach;
MyFitnessPal – 150 million users accounts hacked;
Quora – 100 million account information of user account hacked.
and the list goes on.

So where are we going wrong? Are we not evolving? Are we not expanding our security boundaries? Are we failing to control them? Are we not striving for technological advancement? The answer to all these questions is, Yes. Enterprises are doing all of these. But these may not be the only correct questions to ask. The important question is, “Do I have visibility to all assets in my network?”

The enterprise world now-a-days hugely depend upon cloud-based services, work from home culture, travelling workforce and organizations working in partnerships, all of which live beyond the organization’s owned, secured and monitored network parameters. Moreover, digital transformation requires greater agility with users and applications accessing more data, accounts and resources. Very soon, we will have more applications, services and *(eventually)* data, out of the enterprise than inside. Many visitor devices and BYOD(s) do not follow the organization’s hardening guidelines, your security teams will eventually turn blind to most of these devices connected to your own network. No

visibility to these devices, means no user identification, no evaluation of their security statuses, and hence, no monitoring and controlling their activities. As evidence, 34% of cyber attacks in 2018 were perpetrated by insiders *(Verizon Data Breach Incident Report 2019)*.

***Please note*:** The concept of *"Boundary control"* provides a decent level of protection to the enterprise internal network. Let's suppose you check into a hotel room and ask for a wi-fi connection. You get the login Id and passcode and connect to the hotel's wi-fi. You can connect to the public internet and simultaneously view the hotel's advertisement page. The public internet is completely unrestricted, and you can download anything, access any site, visit any webpage and face no restrictions. Having said that, you are unable to access to the hotel's intranet, their database with customer information, their applications with customer's membership points details, their payroll page, their employee(s) details and their future event plans. This is since you have been provided with an access to a proxy link, which directs you to a public internet, bypassing the hotel's own secured network.
Many hotels do this, but most of them are not aware of how many devices are connected to their proxy. A few good ones, restrict the number of devices connected to their proxy per login Id *(for instance, in Hyatt you can connect 2 devices on one check-in login Id/password, you try to connect the third one and the first one gets auto logged off)*, but a lot of them don't. As a result, many hotels do not have a visibility of how many devices are operating on their network. With an unrestricted internet access, a malicious non-monitored hacker strikes gold in due time. Many organizations with Guest accounts too have the same unrealized issue. Non-visibility of connected devices leaves your network security team handicapped.

2. Zero Trust comes to the rescue

Zero Trust is an alternative to the systematic failures of perimeter-focused security architecture failures. Gradually, Zero Trust has become a trustworthy model for enterprise security teams and have rightfully earned its place in the roadmap of security and hardening policy development. This was introduced in 2010 by a group of analysts from Forrester Research.

Zero Trust is a conceptual and architectural model, which instructs the security teams to redesign networks into secure micro-perimeters. Give more power to data security by limiting the risks associated with excessive user privileges and access. Break your network into segments and protect each segment individually. Improve security detection techniques and strengthen your incident response methodology with least manual intervention. Apply automation wherever there is a need of security incident analysis and response. This will make incident management techniques faster and more effective.

Zero Trust signifies that all devices, networks, security framework and architectures must be checked regularly. No trust at all. Even if your network design architecture is implemented with all the latest updates, your network components are thoroughly patched and upgraded and your devices are in the best of health, still do not trust anything applied and always keep an eye for potential gaps. Put as much perimeter controls as you can, to all devices and attain more and more visibility. Unlearn everything and start from afresh. The rule says, "you can't protect what you can't see". Have visibility across everywhere. Visibility is the foundation of Zero trust.

3. Evolution of Zero Trust Model

During early times, the Zero Trust model described very less about crucial security concepts related to "segmentation of network and hardening each segment" and "Mandatory controls based on least-privilege access". The Zero Trust model didn't provide any directions on how the described security controls could be leveraged in practical implementations. During the much-needed evolution phase of the Zero Trust model, Forrester Researchers came up with a theory of "Zero Trust eXtended (ZTX) Ecosystem".

The ZTX provides a framework to map relevant enterprise security technologies into seven key dimensions:

a. Networks
b. Data
c. People
d. Workloads
e. Devices
f. Visibility and Analytics
g. Automation and Orchestration

The ZTX framework performs the following basic services:

a. Implement protocols based on network isolation, segmentation and security
b. Data categorization, isolation, encryption and control
c. Secure network and network infrastructure resources from its users
d. Secure workload application stacks in public and private cloud
e. Automate and orchestrate Zero Trust controls and process across environments
f. Provide visibility and analysis across every part of the enterprise network.

ZTX framework enforces a security concept of "Default Deny", where enterprise systems and networks are isolated until a level of trust is established.

Please note: Nearly 99% of alerts notified out of any IDS are false positives. However, it is evident that even 1% of actual alerts are enough to put your business at risk. Automation and Orchestration makes sure that none of the IDS alerts go unnoticed and un-analysed.

4. Where do we need visibility?

To make Zero Trust a success, the following goals must be met:

a. It is crucial to "Discover" and "Classify" 100% of the devices connected to your network, not only those which are known, operational and installed with Endpoint agents.
b. Forced application of adequate least-privilege access policy based on the following:
    i) Granular analysis of the connected device
    ii) User identity and authorization
    iii) Software stack
    iv) Configuration compliance
    v) Security state of the device

To ensure optimum restrictive access policy, the network security team must be able to "see, access & control" everything on their network.

As per Forrester's analysis team, "Visibility is the key in defending any asset. You cannot protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the revealing signs of a breach in progress and to stop it."

For a successful implementation of a strategy like this, it is important that our conventional endpoint management system can capture devices connected beyond its reach. Some devices hard to detect and control are, but not limited to, the following:

I. Visitor and BYOD devices
II. Corporate end points with "disabled" agents
III. Rogue devices
IV. IoT devices
V. Network switches & routers
VI. Virtual machines in public cloud

5. Some solutions providing protection based on Zero Trust Principles

A. Forescout Platform:

The Forescout platform is utilized to identify all the unknown devices available in the network. Any network can have an extended version – proxies, VLAN, etc. The Forescout platform provides an agentless security solution *(Agentless security is a new, dynamic security solution that utilizes the resources of cloud technology to monitor computers and smart devices without the help of any physical agent or any deployable monitoring protocol)*, that dynamically *(the instance they are connected)* identifies and evaluates the network endpoints for all the devices connected to your extended or current network. Other than this, Forescout platform quickly determines the user, owner and operating system, along with its device configuration, software, services, patch state and the presence of security agents. Additionally, it provides remediation, control and continuous monitoring services for these identified devices.

Just imagine, your mobile device is connected to the office network and you get an email in some time to disconnect your Android OS, Samsung J10 Max, self VPN, xxxx patch version featured mobile device as it seems to be filled with downloaded malicious content, say an app. Moreover, you keep on receiving the follow up email in every 10 – 30 minutes till you haven't disconnected. The Forescout platform discloses every feature of your mobile, keeps a track of it and logs it for future forensic use, if any.

The following are the benefits of using Forescout platform:

I. It can be applied on managed corporate devices, unmanaged visitor devices, physical and virtual servers, network infrastructure, industrial operations and control systems and IoT systems.
II. It does not need previous device knowledge.
III. Can be implemented quickly into your existing network environment and needs no infrastructure changes, upgrades or endpoint re-configuration.
IV. It can work in physical, virtual and hybrid cloud environments.

A.1. Zero Trust network segmentation process

The Zero Trust network segmentation works in five phases

- Dynamic network segmentation
- Policy layer
- Control Orchestration layer
- Enforcement layer
- A Zero Trust access broker

I. Dynamic network segmentation:

Network micro-segmentation is the core process of Zero Trust framework. However, designing, applying and maintaining effective segmentation policies across distributed environments is known to be the most challenging part. Traditional segmentation solutions are hard to implement, along with a lot of manual interference *(inciting probable human errors)* and requires manual analysis for traffic flows and logs to understand traffic dependencies. This further leads to incidents such as inconsistent segmentation policies and consequent cases of business disruption.

Forescout comes to the picture with an impression that varied segmented network(s) have specific strengths, use cases and areas on the network they are deployed on. So, Forescout's segmentation strategy supports Application-centric, device / role centric and boundary centric approaches to Zero Trust segmentation spanning across all domains of enterprise network environments.

II. Policy Layer:

Forescout came out with a product named "eyeSegment" in order to speed up the process of designing, planning and deployment of dynamic network segmentation across the extended enterprise. The eyeSegment allows all organizations to implement Zero Trust principles for all "IP-connected systems". eyeSegment is capable of monitoring traffic flows, also, it helps in visualizing the traffic interaction between users, applications, services and devices. In lieu with this, it tries to understand its impact and changes brought by this unknown traffic on our network design by simulating and monitoring policies. Any changes or deviations noted in the network policies will be notified to the network security owner.

III. Control Orchestration layer:

It is important to integrate the Zero Trust process with various network devices *(switches, routers etc.)*. Forescout's eyeSegment enforces Zero Trust technology via implementation of network access controls. It provides policy-based network segmentation working in synchronization with switches, routers and other network components and enforcement points in campus, data centre and cloud environments.

IV. Enforcement layer:

Every network segment can be enforced with different policies. There is a constant need for coordination among these network segments across physical and virtual networks. With different controls for different network segments, Forescout's eyeSegment enforces coordination among multivendor enforcement points, enabling execution of segment across physical and virtual networks.

V. A Zero Trust access broker:

Forescout platform performs device control measurement through network infrastructure. It provides a centralized mechanism for provision of network access based on its integrated view of user identity, role, authentication and device state. It performs a local integration of more than 30 switches and wireless vendors and provides direct integration with routers which run on the Linux operating system. This technology is capable of changing VLAN assignment, add an ACL or disable a switch port while working at a network switch. While working on a wireless device, it can blacklist a MAC address or change the role of a user. Additionally, this technology can restrict remote VPN users.

B. Check Point Software Technologies (Check Point Infinity)

In order to implement a Zero Trust Model to any enterprise system a complete rebuilding of security infrastructure is required. This security infrastructure rebuilding may lead to complex deployment and inherent security gaps. To avoid these inbuilt issues, Check Point came up with a more holistic and practical approach to implement Zero Trust. This approach offers a single consolidated cyber-security architecture, Check Point Infinity. Absolute Zero Trust Security, provided by Check Point Infinity, offers a complete, efficient and preventive implementation of the Zero Trust Model.

The Check Point Infinity consolidates a wide range of security functions and solutions that enable you to implement all the seven principles of the Zero Trust Extended *(here referred as Extended Zero Trust Security)* Model:

a) **Zero Trust Networks**: *"Check Point Security Gateways"* creates granular network segmentation across public/private cloud and LAN environment, providing you with a detailed visibility into the users, groups, applications, machines and connection types on your network. This allows you to setup and enforce a "Least Privilege" access policy, so only the authorized users and devices can access your protected assets.

b) **Zero Trust Workloads:** These particularly work on the public/private cloud. *"Check Point CloudGuard Iaas"* and *"CouldGuard Dome 9"* provide security to workloads, particularly those which are running in the public cloud. These technologies provide integrated services with any public or private cloud infrastructure, giving full visibility and control over these dynamic environments. Dynamic environments including AWS, GCP, Microsoft Azure, Oracle Cloud, IBM Cloud, Alibaba Cloud, NSX, Cisco ISE, OpenStack, etc.

c) **Zero Trust People:** To ensure that the access to your data is granted only to authorized users, *"Check Point Identity Awareness"* and *"Check Point CloudGuard SaaS"* is offered. Once implemented, the user's identity is strictly authenticated using Single Sign-On, Multi-Factor Authentication, Context-Aware policies *(such as time and Geo-location of the connection)* and anomaly detection.

d) **Zero Trust Data:** Check Point Infinity provides data protection at different layers in order to protect data from theft, corruption and unintentional loss.
   i) Data Encryption: Technologies used are *"Check Point Full Disk Encryption"*, *"Check Point Media Encryption"* and *"Check Point IPsec."*
   ii) Data Loss Prevention: Technologies used are *"Check Point Data Loss Prevention"*.
   iii) Data Management Categorization and Classification: Technologies used are *"Capsules Docs"* and *"Capsules Workspace"*.

e) **Zero Trust Devices:** If any trusted device gets infected, Check Point solutions allows you to block them from accessing corporate sensitive information and assets. These devices can be employee's mobile phones and workstations, IoT devices and Industrial Control System. The technologies *"Check Point SandBlast Agent"* and *"SandBlast Mobile"* protects employees' devices all the time by enforcement of corporate security policy on untrusted network.

f) **Visibility and Analytics:** Multiple Check Point solutions technologies are available for various aspects of Visibility and Analytics. *"Check Point Smart Event"* provides full visibility to your entire security posture, so the cyber security agents can quickly detect and mitigate threats in real-time. *"Smart Log"* enables users to view and analyse billions of logs records. *"Cyber Attack Dashboard"* lets users to investigate events with real-time forensics. *"Check Point Compliance"* enforces compliance with corporate policy and Data Protection Regulations.

g) **Automation and Orchestration:** Check Point Infinity provides an automated integrated solution, including a rich set of APIs *(Application Program Interface)*, with the organization's IT environment to enable speed and agility, improved incident response, policy accuracy, and task delegations.

Please note: All technologies discussed are centrally managed by Check Point solution's *"Check Point R80 Centralized Security Management"*. Security teams can manage all aspects of security, from access

policy to threat prevention – across the entire organization – on both physical and virtual environments, with a single console.

Preventive Zero Trust:

Check Point Infinity provides solutions for users who focus more on threat prevention instead of detection. To provide protection against known and unknown threats across all networks, Check Point Infinity uses 64 different security engines. These security engines, apart from being implemented on network, can be enforced on endpoints, cloud, mobile, and IoT. How do they do it? These solutions leverage globally shared threat intelligence powered by *"ThreatCloud"* to provide threat prevention technologies with the industry's best catch rate.