preempt

Executive Brief

Zero Trust With Zero Friction

Introduction

A hybrid cloud world, massive remote working population, and acceleration of digital transformation all require enterprises to have a Zero Trust (ZT) initiative. While CISO's have knowledge of ZT technology and principles, the implementation path can create tremendous complexity, cost, and user friction if not done carefully.

The key pillars of ZT (as defined by its creator Forrester) include security technology for users, devices, networks, applications, automation, and analysis. Fundamentally what this means is that every resource accessing another resource must have continuous assessment and action of risk and policy implementation for every transaction.

> "Zero Trust is not a single architecture but a set of guiding principles for workflow, system design and operations ... to improve the security posture ..."[1]

A typical approach to ZT involves acquiring vendor solutions in each of these pillar areas and assembling a security stack. This stack, with the complexity in integration and management, creates friction for both IT and the end-user. In addition, the migration to a ZT approach itself takes time, effort, and capital. Deployment of software, conversion of current policies into a ZT solution stack, and finally the operational effort in getting everything working and running continually.

So how can ZT be implemented, but without the friction?

Forrester's Best Practice Principles of Zero Trust

BEST PRACTICE PRINCIPLE	COMMENTS	PREEMPT ZERO FRICTION
Micro-segmentation	Several approaches are encouraged, including identity-based segmentation. With 80% of threats involving identity, micro segmentation by identity is most effective.	Identity-based segmentation deploys very quickly without infrastructure changes, works in real-time, and covers on-prem and cloud deployments.
Enforce Policy Everywhere	Policy creation must be automated (one of the key pillars) and dynamic. This includes legacy systems which have their own identity policies and systems.	The policy can be system-defined via Machine Learning and also user-defined. Attributes are collected from static and 100+ dynamic analytics. This approach reduces the resources required for changes and maintenance.
Identity Beyond IAM	Identity must provide the risk of both human and application (service) accounts to provide the complete context.	Provides real-time, continuous risk analysis. Can be deployed with or without an end-point user agent when connected to SSO.

Table: Based on Key Principles from Forrester on Zero Trust[2]

Beyond Zero Trust

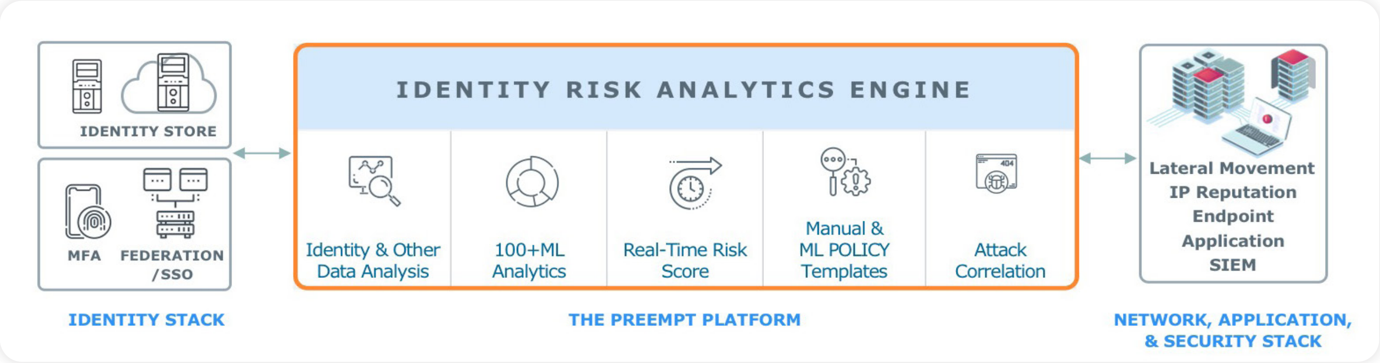
> "Identity-driven approaches also work well for enterprises that use cloud-based applications/services that may not allow for enterprise-owned or -operated Zero Trust security components to be used (such as many SaaS offerings)."[3]

While Forrester may have started the framework, there are several others also feature real-time risk analysis based on identity for a perimeter less architecture.

Gartner - Gartner's CARTA model emphasizes the continuous aspects of trust/threat analysis (i.e. real-time and not log-based). Preempt works by looking at real-time identity traffic from any location (on-prem or cloud) and creates a risk score that feeds into a policy to determine action.[4]

IDSA - is an industry standards organization that focuses on identity-related topics. Preempt covers the key elements in IDSA's architecture as Preempt can provide triggers on policy for any MFA. And this can work with both humans and applications (service accounts) as both require ZT for resource access. [3]

NIST - Several publications from NIST support the idea of identity being a key and effective method for enabling a ZT approach. Since the government has disparate systems, including legacy systems, NIST emphasizes the importance to provide ZT without a complete lift and shift approach to existing systems.[5]



Preempt ZT Framework

Conclusion

While ZT may be discussed by many companies, focusing on a strategy for easy user experience for both IT and end-users will become the most successful. After all, no one wants to be secure if they cannot freely do their core business function.

[1] NIST FIPS 199
[2] Forrester Wave: Zero Trust Extended, Oct 2019
[3] IDSA: The Path To Zero Trust Starts With Identity Aug 2020
[4] Gartner July 2020: User Auth Report
[5] NIST Special Publication 800-207 Zero Trust Architecture

About Preempt

Preempt secures all workforce identities to accelerate digital transformation. Since 80% of all breaches involve compromised credentials, Preempt unifies security visibility and control for on-premises and cloud identities. Threats are preempted and IT policy enforced in real-time using identity, behavioral, and risk analytics. Preempt protects over four million identities across 400+ enterprises. Learn more: www.preempt.com.