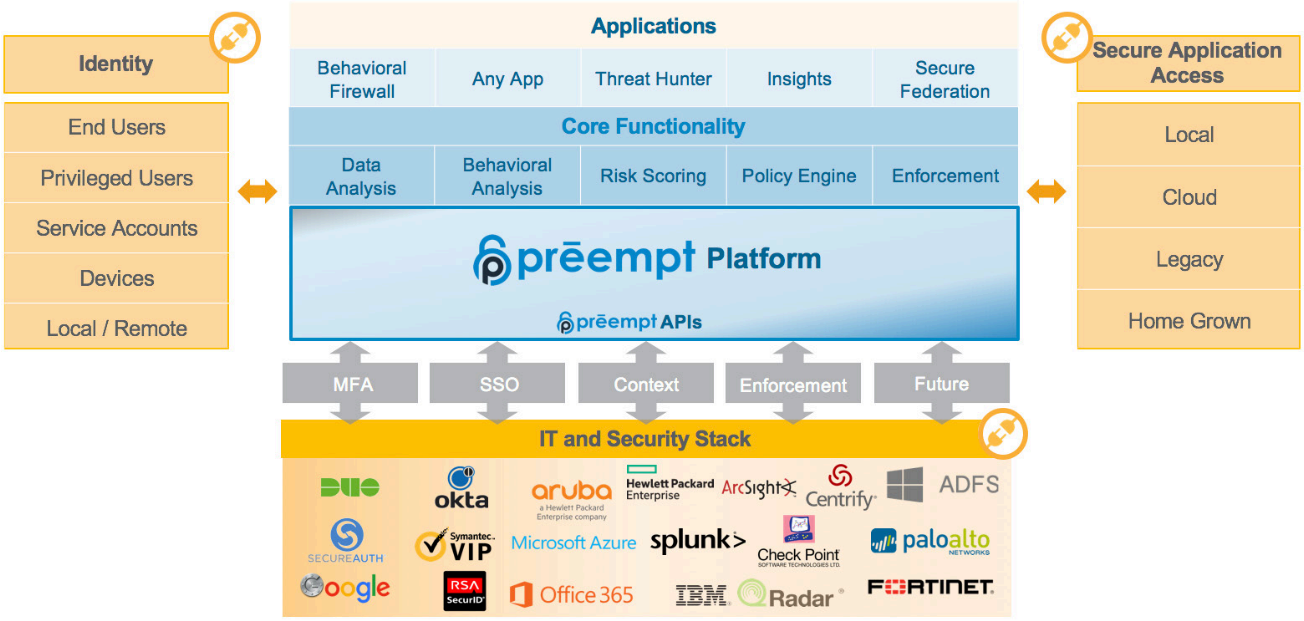
preēmpt

Comparing Preempt and Microsoft ATA and AATP

Preempt and Microsoft's Advanced Threat Analytics (ATA) and Azure Advanced Threat Protection (AATP) share some core similarities in that both solutions monitor an organization's directory infrastructure in order to find suspicious behavior and attacker techniques. However, closer inspection reveals Preempt and ATA/AATP to be vastly different solutions, with very different capabilities, roadmaps, and philosophies. This document will highlight some of these key differences and show how they have a material impact both on the security of an environment as well as the efficiency of security operations.

Note: Microsoft ATA is a locally deployed solution, while AATP shares a similar architecture, but deploys the central server in the cloud. The security functionality is virtually identical, and we will refer to ATA/AATP except when referring to architecture specifically.

The image below shows the high-level architecture of the Preempt Platform. While it isn't necessary to go into detail of each component of the architecture, we have included it here to illustrate that the behavioral analysis capability of ATA/AATP is only a component of the Preempt Platform. Even in this area of overlap, we will show how Preempt enjoys a clear advantage, while the additional areas allow Preempt to detect threats that ATA/AATP does not, while accelerating security operations.



Automated Adaptive Response vs Manual

Preempt recognized early on that behavioral analytics by itself was not enough. The industry was awash in analytics products such as ATA/AATP that could detect anomalies and abnormalities, but then required a human analyst to do the hard work of verifying an event and taking action. This is still the case with ATA/AATP today as evidenced by their Suspicious Activity Guide, which details the laborious process of sorting out false positives and taking corrective action.

Preempt pioneered the first solution to deliver automated and adaptive response. Suspicious behavior can be challenged by multi-factor authentication (MFA) or require an authorizer. A successful MFA response can automatically close the incident without staff intervention. Failures can force a password reset, reduce user privileges, or even block or isolate the host. In either case, Preempt uses the results to continually train detection algorithms over time.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Real-time adaptive response based on policy. + MFA, Authorizer, Demote, Force PW change, etc. + Blocks threats and prevents damage. + Automated protection for any application, server, or resource. + Algorithms continually trained based on supervised and semi-supervised feedback.	- Detection only, no prevention. - Requires manual investigation and response outside of the product.	Most analysts teams are already overloaded. Preempt allows organizations to automate triage and respond, which is customer accounts has proven to stop real threats while reducing incidents by 30%. By comparison, the ATA approach only works when a human analyst does additional work.

Risk and Impact Scoring

Preempt automatically scores all entities in terms of their risk to the network based on observed behaviors, traits, and identity in the network. Analysts can quickly focus on the highest risk users or see risk scores by organization unit, outliers, and the impact to the network. Policies then enable Preempt to trigger adaptive responses based on observed risk.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Risk scoring of all devices and users + Automated response based on risk + Risk scores by team or OU + Impact scores based on user traits such as delegated privileges, relationships, and role.	- No risk scoring	Analysts need to know where to focus, especially in a busy network. Preempts risk scoring lets analysts focus on the issue that have biggest impact to the business.

Continuous Audit of Security Posture

Preempt continuously assesses every device and user in the environment across dozens of security-relevant traits. For example, Preempt reveals the use of weak or compromised passwords, stealthy administrators, users who are sharing passwords, using unmanaged endpoints, and much more.

Preempt	Microsoft ATA	Why it Matters
+ Continuous audit of all users, computers, service accounts including password and device policies. + Dedicated Insights page to highlight, analyze, and remediate potential weaknesses	- No user or device audits	Preempt's Insights allows organizations to proactively manage their attack surface, and address weaknesses before they can be exploited by attackers.

Management of Privileged Accounts

Preempt performs an autodiscovery of privileged accounts based on actual traffic and analysis of detailed permissions. This allows Preempt to identify "stealthy administrators" whose permissions allow them to behave as or control an admin even without being in an official admin group. Microsoft ATA/AATP only identifies privileged accounts if they exist in a static list of administrator groups in Active Directory or are specified manually.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Continuously analyzes traffic and permissions to identify stealthy admins. + Track, manage, and even demote all privileged users in a dedicated Insights page. + Can set adaptive policies (MFA, Authorizers, etc) for privileged users.	- Only identifies users as privileged if they are in pre-defined admin groups - No active management	Users are often granted temporary privileges that are never revoked, or permissions where the full impact is not obvious. Preempt uncovers the hidden chains of privileges, and provides adaptive responses to ensure those privileges can't be used to damage the network.

Hardware and Resource Requirements

While Microsoft will often give away the ATA license as part of a bundle, the product carries hidden hardware costs. Comparing the two solutions, the sensors and agents for both ATA and AATP requires more CPU cores, memory, and disk even though Preempt processes and stores more data points. This combined with ATA/AATP's need for extensive care and feeding from analysts gives the solution an ongoing operational cost that negates the value of the initial free license. While AATP removes the need for a central hardware server, it does also require the customer to open many inbound and outbound ports to their data center.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Low CPU, memory, and disk requirements. + Removes work from analyst via adaptive response and automated resolution of false positives.	- High hardware requirements - Requires extensive manual analysis and response from staff.	While Preempt does not give away its product, the total cost of ownership can easily less than ATA/ATP when operational costs and the cost of analyst time is considered.

Data Enrichment and Integration

Preempt naturally integrates with the rest of an organization's ecosystem, both to enrich data and provide adaptive responses and feedback to other systems. This includes integration with perimeter firewalls, single sign-on (SSO), MFA, VPNs, SIEMs, NAC, and more. Preempt's open syslog handler allows the solution to ingest data from virtually any vendor. Microsoft's SIEM integration is limited to accepting 8 types of Windows events.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Open syslog connector to work with any vendor + Prebuilt connectors for SSO, VPNs, Firewalls, MFA, more. + Robust API allowing other tools to consume Preempt data (e.g. Risk scores) + Visibility into users with cloud access.	- SIEM ingestion for 8 Windows events only - VPN support for 3 vendors - No adaptive response	Preempt acts as a natural glue connecting your various security investments, helping it all to work together in real time. ATA/ATP represents yet another data silo for analysts to manage individually.

Threat Hunting and Investigation

Preempt aims to automate as much work as possible, but it also provides the tools to investigate quickly and in depth when analysts need it. The dedicated Threat Hunter interface allow analysts to query across any of the many dozens of attributes tracked by the Preempt Platform. Analysts can then easily pivot to related events and see and complete chronology of related events. ATA/AATP provides no query interface and shows a simple high-level summary of event progression.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Dedicated Threat Hunter interface. + Query and correlate across any attribute. + Find connected events and pivot on the fly.	- Basic event summary - Option to download details such as related IP addresses for manual investigation.	The speed and depth of investigations directly impacts how many investigations a team can perform in a day. Preempt gives puts analysts in full control of their data and investigate intuitively.

Focus and Execution

The ATA product was born from Microsoft's acquisition of Aorato in 2014. Aorato had no customers at the time, and since being acquired, the solution has seen almost no feature updates, and key talent has since left the organization. Preempt, on the other hand, is solely focused on cybersecurity, and continues to deliver on an aggressive development roadmap and boasts and has one of the most prolific security research teams in the industry.

Preempt	Microsoft ATA/AATP	Why it Matters
+ Dedicated security focus + Led by the best minds from Israeli defense forces + CEO led industry's first IPS product	- Enterprise security is not a priority for Microsoft. - No new features - Lost core talent including leadership and R&D.	Cybersecurity is constantly evolving and security products will quickly become outdated and ineffective without ongoing focus and execution.

Summary

This document highlights some of the key functional differences between the Preempt Platform and Microsoft ATA/AATP, but is not an exhaustive list of all differentiators. We are happy to provide a more customized analysis based on your unique environment and needs. Simply contact the team here at Preempt and we would be happy to help.

About Preempt

Preempt protects organizations by eliminating insider threats and security breaches. Threats are not black or white and the Preempt Platform is the only solution that delivers identity & accessthreat prevention that continuously preempts threats based on identity, behavior and risk. This ensures that both security threats and risky employee activities are responded to with the right level of security at the right time. The platform easily scales to provide comprehensive identity based protection across organizations of any size. Learn more about us at www.Preempt.com