preempt

WHITEPAPER

Defending the Enterprise with the Preempt Platform

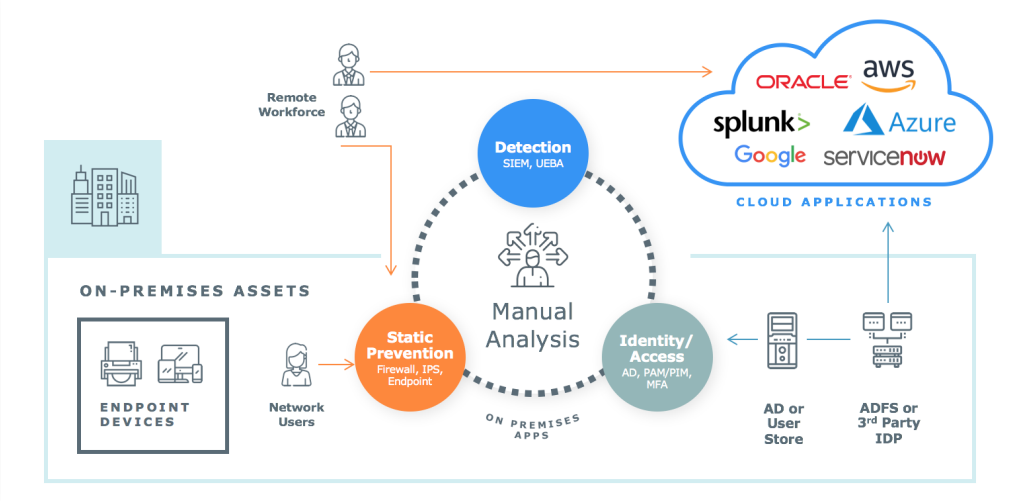
A Modern Approach to Access and Securing Identity

CONTENTS

Introduction

Security teams today struggle to find practical approaches to dealing with the threat of cyberattacks, breaches, and insider threats without disrupting their business or overloading analysts. Despite promises, many of today's security tools tend to generate many inconclusive alerts that require manual investigation. Traditional Identity and Access tools lack an understanding of threats and traditional enforcement methods remain limited to simple Allow or Deny responses that lack an understanding of behavior and risk-related context.

Additionally as organizations shift to the cloud, many security teams have lost consistent visibility into their users and assets. Teams often lack visibility and control over behaviors in the cloud, or in the best case, rely on separate and siloed solutions that lack context.



The Preempt Platform bridges these perspectives and enables organizations to deliver real-time conditional access and security controls that prevent threats based on identity, behavior, and risk. The solution pairs user behavior to detect threats with a contextual automated response that detects risky user behavior and proactively stop threats without disrupting the business. Policies take into account a user or entity's role, their behavior, and the target of their actions. Flexible response options can make gradual responses to changing risk, automatically close incidents related to benign anomalies, or block once a threat is verified.

This product white paper will dive deeper into the following areas:

- Key Concepts of the Preempt Platform
- Identity and Risk Insights
- Threat Detection and Analytics
- Conditional Access Anywhere
- Flexible Deployment and Journey

Key Concepts of the Preempt Platform

Preempt delivers a new approach to security that brings together identity, behavior, and risk into a unified security context. Instead of keeping security context siloed, Preempt introduces a new approach to access and identity security, which blends concepts of Identity and Access Management, Privileged Account Management, Behavioral Analysis, and Cybersecurity and Threat Prevention into a real-time approach to security that constantly adapts to changes in the environment.

Consistency Across the Enterprise

Preempt visibility and policy enforcement reaches across the enterprise including internal, on premise behavior as well as users and behavior occurring in the cloud. This lets security teams not only track all behavior across the enterprise, but also enables consistent policies, and track incidents that span on-premise and cloud assets.

Adaptive and Appropriate

Instead of simple “Allow” or “Deny” responses, Preempt enables far more nuanced responses that can gather additional information and adapt based on what it learns. This ensures that valid users aren’t prevented from doing their jobs. For example, if an administrator’s device begins acting strangely and attempts to access a critical server, Preempt could challenge with a second factor of authentication. If the admin fails the identity challenge, the connection could then be blocked, the user isolated via NAC, or other responses.

Extending Your Security Ecosystem

Preempt includes the option to integrate data from other solutions in the organization such as SIEMs, firewalls, VPNs, or SSO products. Preempt can ingest data from other sources such as reputation feeds, MDM solutions, or virtually any other type of security product. Preempt can also actively engages with other security solutions such as a multi-factor authentication products, and ticketing or orchestration systems.

Identity and Risk Insights

Data breaches often begin begin by an attacker finding an initial weakness or vulnerability in the target environment such as an employee using a weak or compromised password or a stealthy admin using an unmanaged endpoint just to name a few. In order to defend their environment, security teams need full visibility into their attack surface including all users and accounts.

Visibility Into All Accounts

Security staff need visibility into all of the accounts operating on the network. In addition to the traditional human users of a network, security teams must be aware of the many programmatic service accounts in use. These accounts often have high privileges and can be a valuable target for attackers. Preempt sensors can directly analyze traffic to reveal the true nature of an entity, such as a human attacker trying to use a programmatic account or a workstation masquerading as a server. This same type of analysis can be used for a variety of other classifications such managed and unmanaged devices, shared devices, and more.

The solution also understands the many types of users within an environment. The solution automatically identifies privileged users and administrators based on observed data. This intelligence includes the ability to reveal “stealthy administrators” who may have important privileges, but are not part of the official Administrators Group within Active Directory. The solution can also focus on high-value users such as executives who hare often targets of attackers. Visibility can likewise be aligned to users based on their functional role or organizational unit in the enterprise.

Risk Scoring

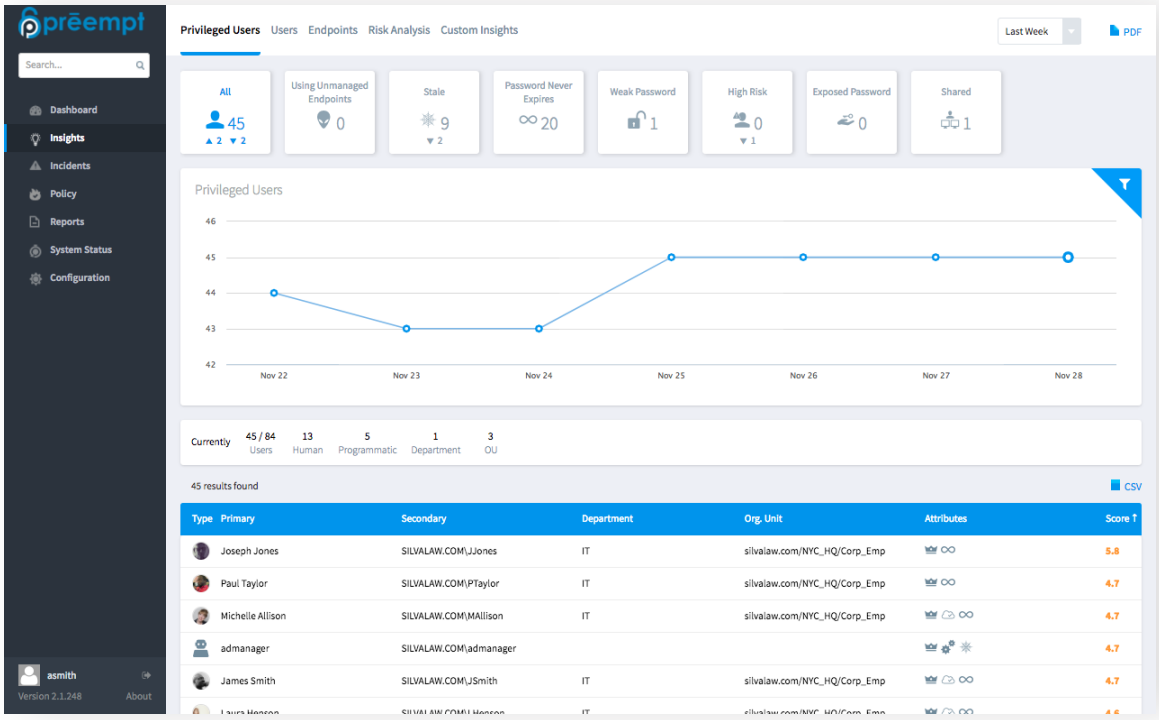
Preempt assimilates all of the available perspectives and context into an actionable risk score for every entity (user, account, device) in the network. This score is expressed as a number between 0-10 and represents the likelihood that the activities or posture of an entity can lead to a successful breach by a malicious attacker, or that an insider may be going rogue.

Preempt constantly evaluates inputs and changes scores up or down as appropriate. Some elements of risk score decay slowly over time while others can be resolved quickly. For example, when a user changes from a weak to a strong password, the user’s risk score decreases in response immediately. Additionally, some factors may lead to a boost in risk score, such as accounts with administrative rights, power users as executives, or even servers with specific critical roles. Risk scores are used throughout the Preempt solution to automate responses and enable staff to quickly investigate incidents or identify problem users in the network. Risk scores can even be used outside the Preempt platform by using the API to share Preempt risk context with other systems and orchestration platforms.

Insights

Finding and preemptively resolving weaknesses is one of the most important aspects of strong cybersecurity. However, weaknesses can come in a variety of forms - user specific traits such as password issues, device configuration problems, support for outdated and weak protocols, Active Directory settings, and vulnerability to a wide range of attack techniques. Preempt's Insights page is dedicated to tracking the security posture of the network, while making it easy to find and monitor the users, devices, and accounts in the network that pose the greatest risk.

This includes finding devices that share the same local admin credentials, users with weak passwords, devices that allow RDP or RPC from the local user, accounts being shared by multiple users, and many more. This visibility allows organizations to reduce their attack surface where possible, and closely monitor any assets that could be inviting to an attacker.

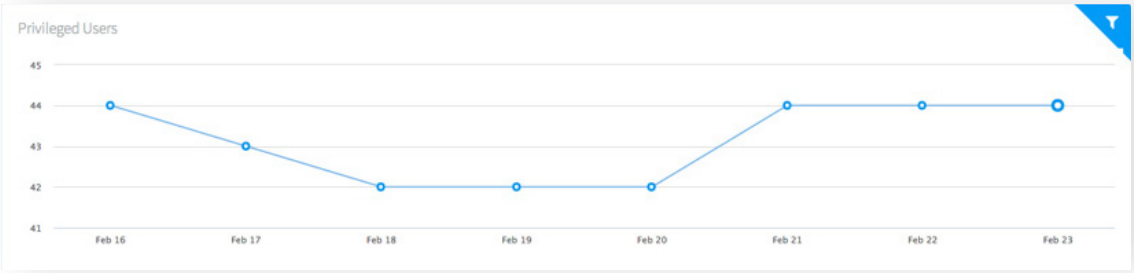


The Insights page contains a variety of pre-built views for seeing risk. Staff can immediately jump to views dedicated to Privileged Users, End Users, Endpoints, as well as a Risk Assessment of all entities. Alternatively, views are available to analyze Active Directory Hygiene or to view the full attack surface of the network or a particular segment.

Each view is interactive, making it easy to drill down into additional information. The list below includes just some of the weaknesses that Preempt can automatically identify:

- A user or admin using an unmanaged endpoint
- Stale privileged account
- Device compatible with versions of NTLM
- SMB signing is disabled
- Devices vulnerable to skeleton key attack
- Multiple devices with the same local administrator
- Accounts only using a DES key
- Password that never expires
- Stealthy administrators
- Using a weak password
- Has a high risk score
- Using an exposed password

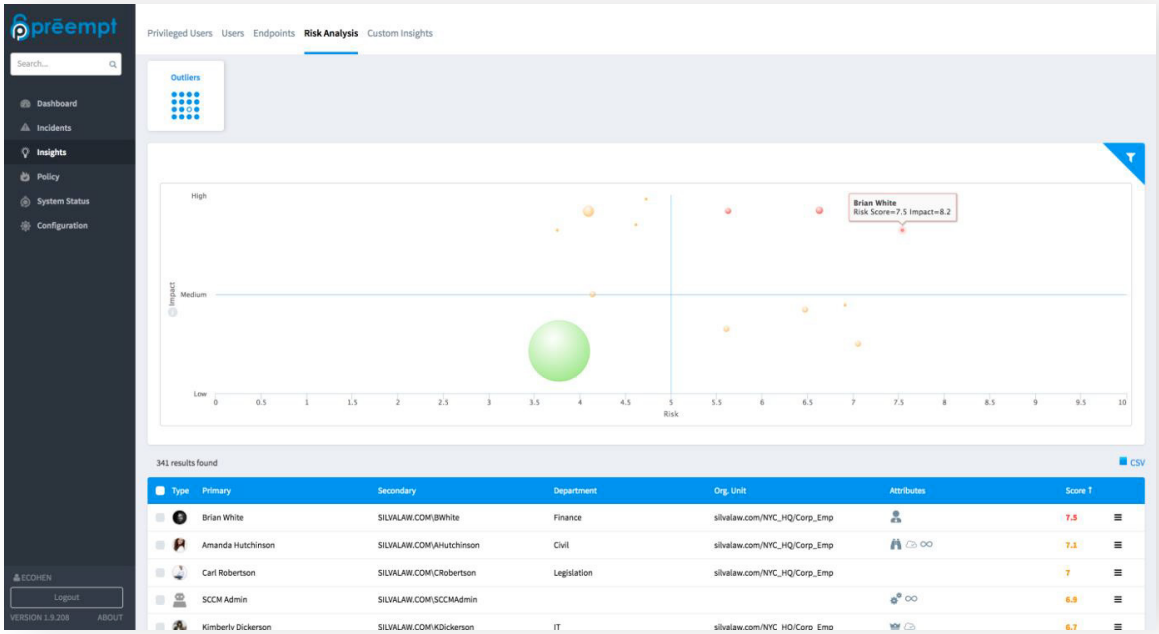
The Insights page also lets staff easily track changes over time. The 'Privileged Users' view could easily reveal when new administrative accounts have been created that otherwise may have been missed. Similarly, in the 'Endpoints' tab, staff can easily see if more unmanaged endpoints have entered the network over a particular period of time.



The Insights page then provides a detailed list of each relevant user or device for further investigation. This list is called the Entity Table and provides deep insight into each entity. The table shows if the entity is human, programmatic, or a device along with organizational unit and risk score. The table can then provide a wide array of additional detailed traits based on the particular entity. For example, the system could distinguish a particular user as being an executive, a watched user, or a user with multiple devices. A device could be further identified as being an App Server, or a DNS server, or a device with a vulnerable OS. Staff can also create their own customized Insights based on virtually any attribute tracked by the Preempt solution.

Risk Analysis

The Insights page also provides staff with a dedicated risk analysis view. This visualization shows risk scores in relation to the impact on the network. For example a user may have a high risk score, but if that user has relatively limited privileges on the network, then the impact could be low. The graph is broken into quadrants with the top-right section representing entities with both high risk as well as high impact. This again provides a very helpful way for staff to hone in on the users that need the most immediate attention.



The Risk Analysis page also breaks out risk by Group and Organizational Unit. This allows staff to easily identify the groups and individuals that are contributing the most to the risk of the enterprise. The Outliers view provides additional detail by showing the risk of individual users or entities in the context of impact. For example, a user may have a high risk score based on a series of unusual or potentially malicious behaviors, and also have a high impact score based on access to a high-value database or application.

Reporting

Preempt provides built-in and customizable reporting for virtually all of the many traits tracked by the platform. This can vastly simplify the sharing of information within the organization while improving the speed of regular tasks such as compliance reporting. Reports can configured based on time (weekly, monthly, etc), and can be emailed or downloaded in PDF format.

Threat Detection and Analytics

Preempt Sensors allow for the direct analysis of traffic traveling to and from the authentication infrastructure. This allows the platform to directly detect a wide range of threats in the environment and to continuously track the behavior of all entities over time. Preempt automatically learns normal behavior patterns for each entity and identifies risky or anomalous behavior.

Enhanced Entity Classification

In addition to information from Active Directory, Preempt performs direct analysis of traffic. This lets Preempt classify every entity with certainty and also recognize when an entity is being impersonated such as a human user impersonating a service account. This level of analysis also reveals a wealth of context such as being able to associate specific endpoints and device traits with user accounts, such as being able to find an administrator who is using an unmanaged device.

Anomalous Behavior

Preempt continually learns and tracks the behavior of every user, device, and account in the environment in order to recognize any abnormal behavior. Anomalous behavior is not necessarily malicious behavior, but it can often be the first indicator that something is wrong in the environment. For instance, an end-user accessing unusual resources, from an unusual location, or at an unusual time can be a sign that the user is potentially compromised by an attacker or malware. By learning normal behavior across a wide variety of traits, Preempt can flag anomalies, score the user's level of risk, compare it to peers behavior, and then challenge the user to confirm identity to ensure that the behavior is valid.

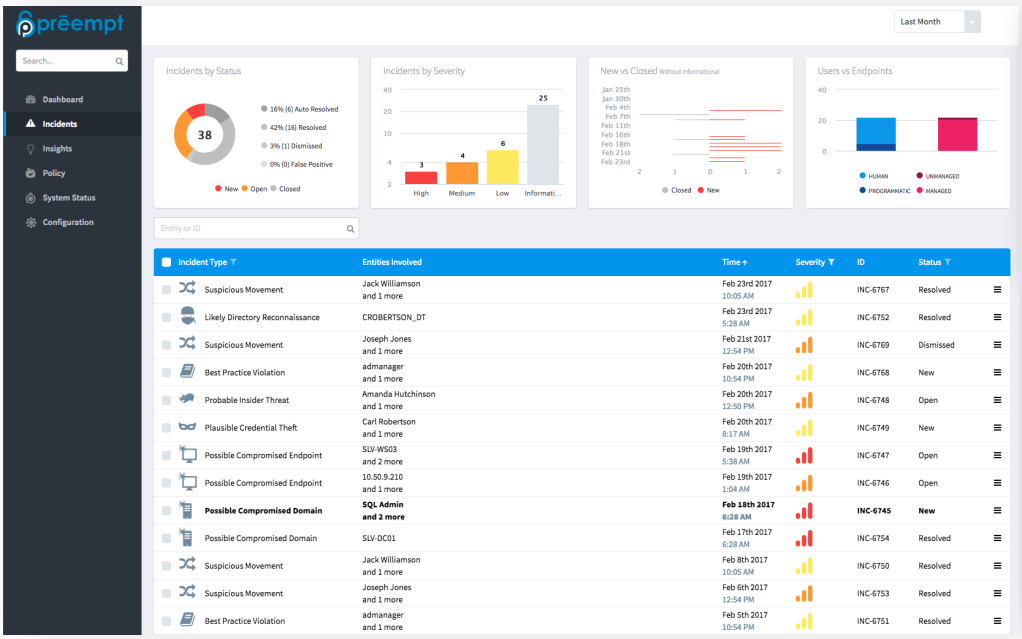
Malicious Behavior

Preempt directly reveals malicious actions and techniques used by attackers to move laterally within a network and extend the intrusion. This includes techniques such as Pass-the-Hash, Golden Ticket Attacks, Active Directory Harvesting, and attempts to elevate privilege via forged Privileged Account Certificate (PAC) just to name a few. This analysis also reveals the use of common attack tools such as Mimikatz or the use of insecure protocols such as NTLM. These detections can be particularly valuable as they can reveal a more deterministic sign of attack. It is also important to note that detecting these actions often requires direct analysis of network traffic provided by the Preempt Platform and can not be detected based on log traffic analysis alone.

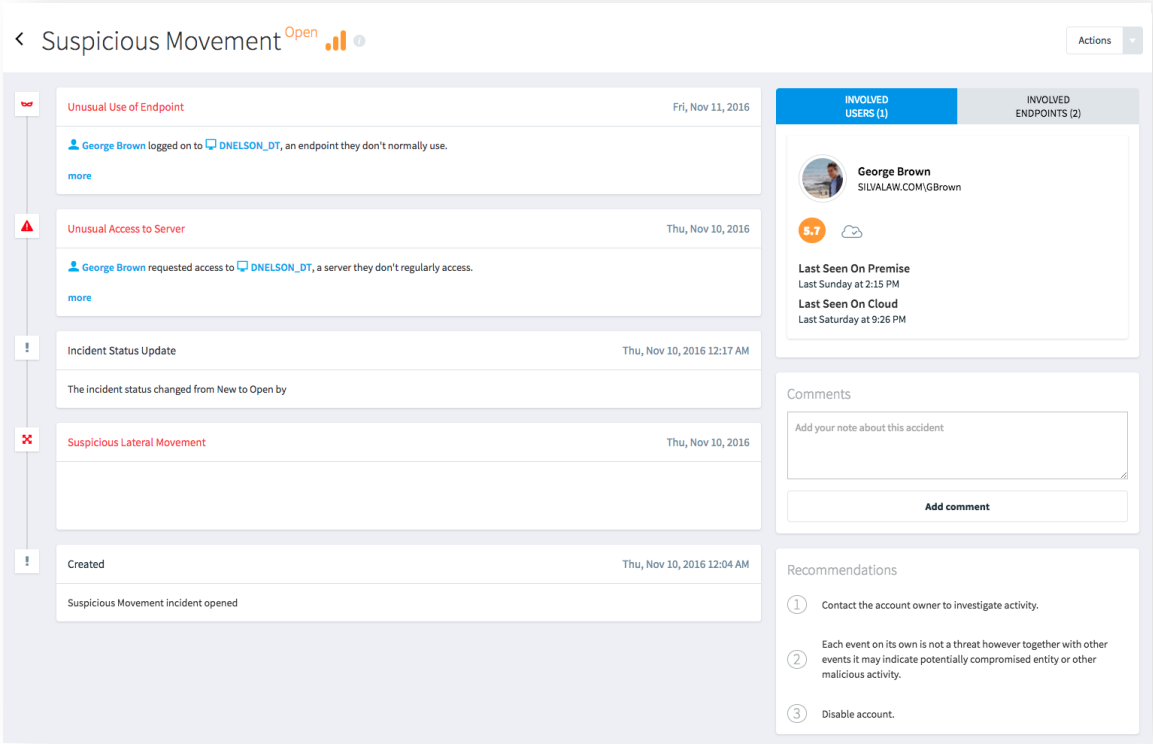
Malicious Behavior	Anomalous Behavior	Entity Classification	Security Posture
++ Brute Force	++ Assets accessed	++ Human vs programmatic	++ Weak password
++ Account Scanning	++ Applications or services used	++ Workstation vs Server	++ Exposed password
++ Pass-the-Hash /Ticket	++ Time	++ Managed vs unmanaged	++ Shared account
++ AD Harvesting	++ Location	++ Etc...	++ Stale privileged accounts
++ Forged PAC File	++ Device		++ NTLM use
++ Etc...	++ Etc...		++ Etc...

Investigating Incidents

The Incidents page provides administrators with quick access to the information they need to get work done. Administrators can customize the time range and then further filter based on severity, status (new, open, resolved), and type of user (human or programmatic) or device (managed vs unmanaged). Staff can also search of incidents of specific type or identify incidents that involve a specific user, account, or device.



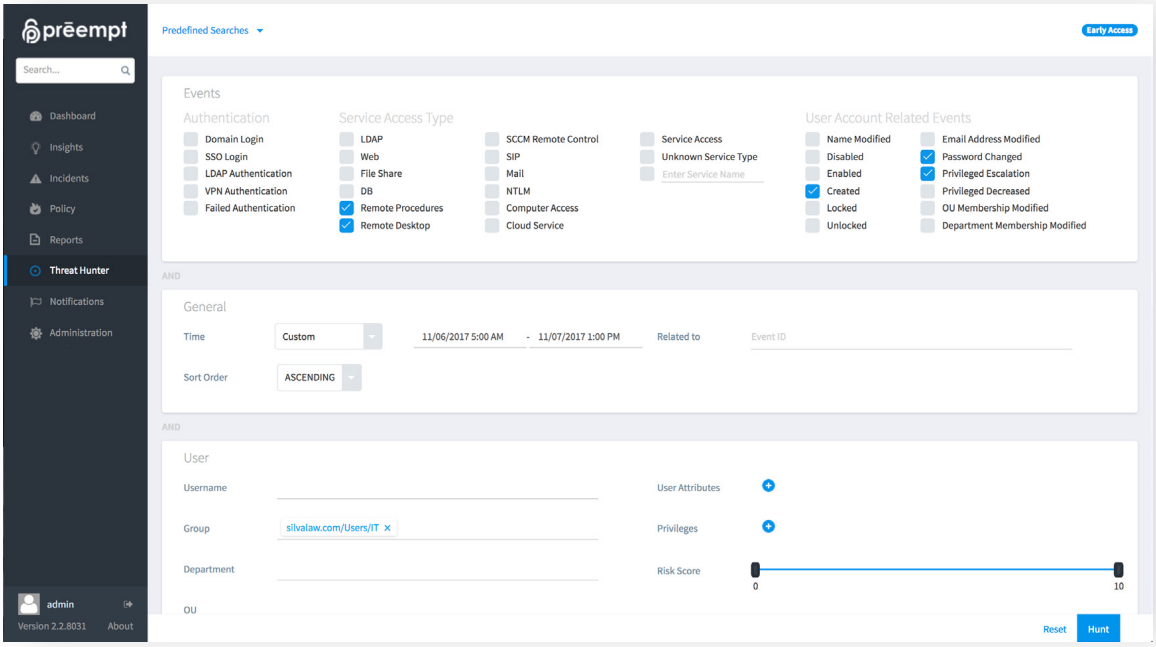
Clicking on a particular incident provides a detailed narrative of the incident and its progression over time. For example, in the Suspicious Movement incident shown below, the detail shows when the incident was created and that a particular user was observed accessing and unusual server, and then the next day using an unusual device. Staff can click to learn more about a particular event within the Incident details. The right-hand side of the screen also shows details about the users or devices involved in the incident along with their overall risk score and last time seen. This view also provides recommendations on next steps and provides a place for administrators to leave comments on the incident.



Once an event is investigated, staff can further manage the incident by marking it as resolved, dismissed, or as a false positive. Dismissing an incident will suppress the incident, although Preempt will continue to track the event in the background. If the same event occurs in the future, the incident will be generated again. If an incident is marked a false positive, will learn that the behavior is allowed and will not generate new incidents in the future.

Threat Hunter

The intuitive Threat Hunter interface lets analysts query and correlate across any combination of attributes and network traffic events tracked by the Preempt Platform. Analysts are free to follow their own intuition and ask open-ended questions that cut across user and device attributes, access and authentication methods, account changes, time, location, and more. When analysts see something interesting, Threat Hunter can provide any related events and a chronological view to put the details of the hunt into full context.



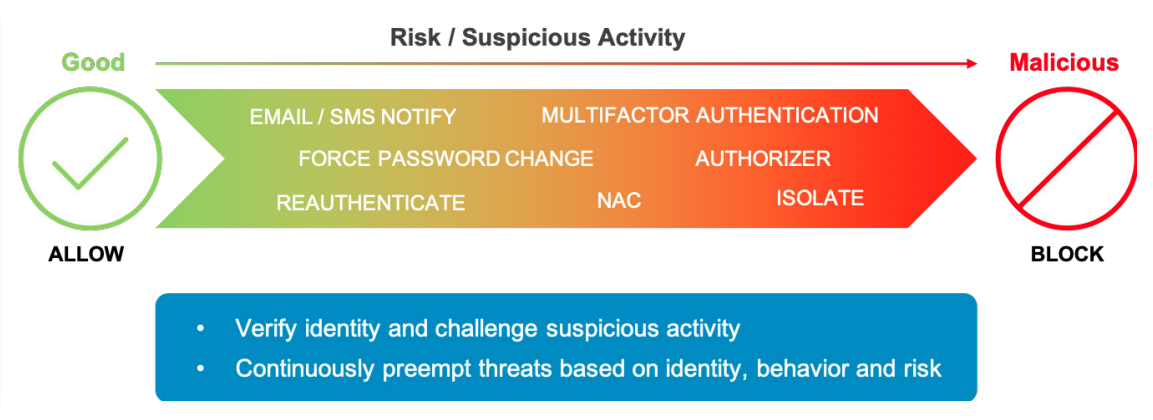
Conditional Access Anywhere

Detecting threats is obviously a critical component of the Preempt Platform, but ultimately the solution is about turning this intelligence into business-appropriate action. The overarching goal is to deliver responses that are automated without requiring analyst time or impacting valid end users. To deliver on this goal, Preempt leverages a highly adaptable policy engine that can block, challenge users, verify threats, and deliver a variety of real-time graded responses. This enables organizations to build powerful conditional access policies that align a wide range of security contexts to real-time and business-appropriate responses.

The Preempt Policy Engine

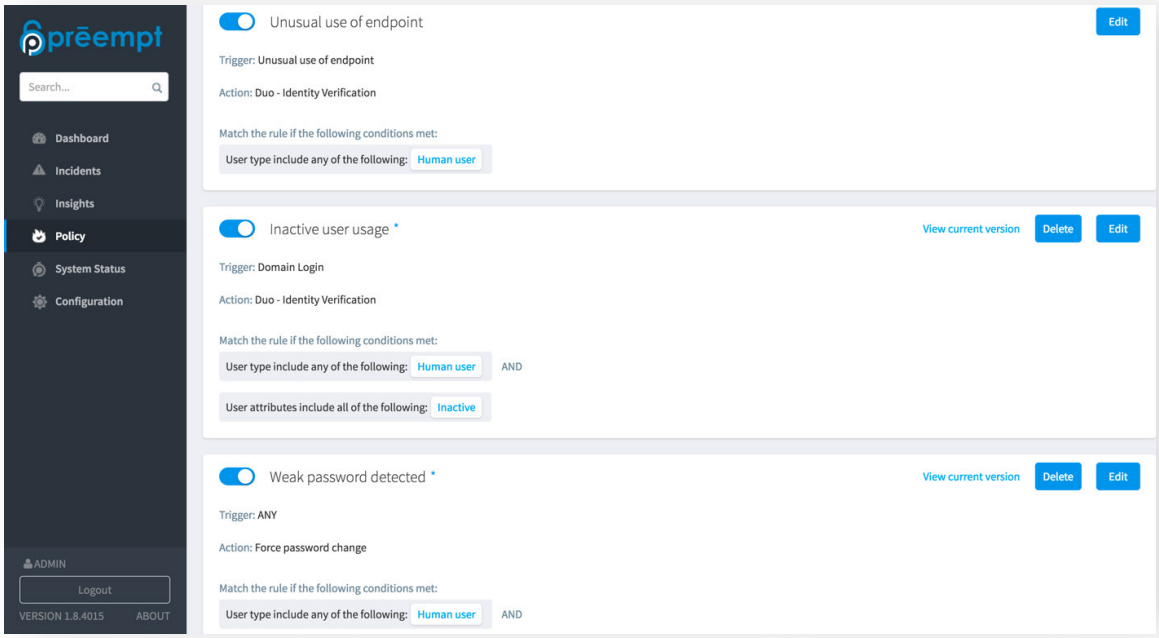
The Preempt Policy Engine is the key to conditional access. It brings observed behavior, user role, risk scores, the target being accessed, access method, and many other factors into a single action-oriented context. Just as importantly, policies have the ability to gain new information and adapt over time. When Preempt detects abnormal or risky user behavior, the Policy Engine can automatically challenge users to confirm their identity. Then based on the response, the policy engine could take further action such as isolating the user via NAC, blocking access, or notifying staff. This real-time and adaptive approach to conditional access ensures that actions remain appropriate to the situation without requiring constant attention from analysts.

The Policy Engine takes in a variety of inputs such as any detection rules, user defined rules or changes to an entity's attributes. Responses can include the ability to block a user, force a password change, or challenge a user with multi-factor authentication. The results of a challenge can likewise change the user's risk score and also drive further responses. This allows the policy engine and the organization's response to logically interact with the user and adapt to the situation.



How the Policy Engine Works

Preempt policies are built on a combination of triggers, conditions, and actions. Triggers are the core activity of the policy rule such as an unusual use of an endpoint. Conditions allow the policy to be targeted to a specific situation or use case. For example, a policy for an unusual use of endpoint could specifically look for unusual behavior of devices belonging to executives. Actions specify the automated response or security control to be used when a rule is matched.



Incorporating identity, role, target and behavior into the Policy Engine ensures business processes can continue while containing security threats. The table below provides just a few example of conditional access policies that can easily be created using Preempt.

Action	Condition	Trigger	User
Approver required	Any or Specific	Login from new Location	Third Party Vendor, Consultant
Isolate using 3rd party NAC	Any	Risk score > 9	Any
Add user to SSO risk group to limit access to cloud applications	Any	Pass-the-hash detected in on-premise network	Any
Block	Workstation	Remote Desktop	Admin
MFA - Verify identity	Critical Server group	Login	Any user not from jump host
Change password on next login	Any	Weak password detected	Employee

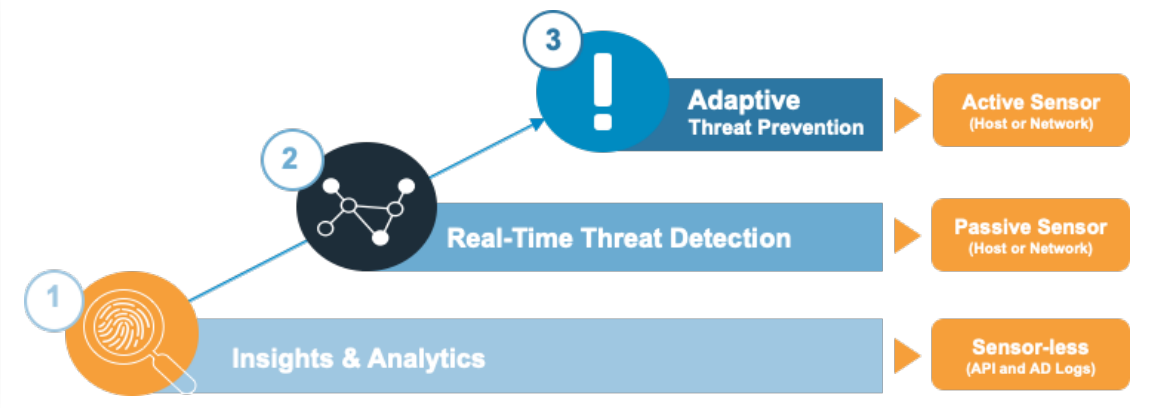
Extending MFA to Any Resource

Preempt allows organizations to extend multi-factor authentication to virtually any resource in the enterprise. Using Preempt's network-based approach, teams can add conditional access and MFA controls to custom, legacy, and home-grown applications without making any changes to the applications being protected. Preempt can also add MFA controls to assets such as databases or workstations without the need to install agents on the devices being protected. Additionally, by integrating with Active Directory Federation Services (ADFS), Preempt can protect any federated services accessed via web browser such as Office 365 or even applications configured for single sign-on (SSO).

Flexible Deployment and Journey

The Preempt Platform provides customers with enormous flexibility in terms of how the solution is deployed. At the highest level, Preempt can be deployed in three different ways:

- **Sensor-less Deployment -** In this configuration, Preempt gathers information by querying Active Directory servers for important security-related traits and integrating logs from other enterprise sources via APIs. This option provides insights and analysis into user accounts, identifies privileged users, stealthy admins, and a wide variety of password-related issues.
- **Passive Sensor Deployment -** This option leverages a passive Preempt Sensor, which can be deployed in the network or on the Active Directory servers themselves. This approach allows Preempt to directly analyze traffic traveling to and from the Active Directory infrastructure. This approach includes all the insights of the sensor-less approach, and also adds the ability to analyze user behaviors and detect active threats in real time such as lateral movement, attack tools, and dangerous protocol use.
- **Active Sensor Deployment -** This is the most robust deployment option and includes all of the previous described functionality as well as the ability to enforce conditional access policies such as adaptive MFA, blocking of threats and more. An active sensor can be deployed as an in-line network sensor or directly on the Active Directory server.



Only one of these options is required at a time. This flexible architecture means that Preempt easily aligns to the needs of any environment while retaining the option to grow as needed. Many customers will deploy initially using active sensors to leverage all features of the platform, while others can begin with insights and analytics, which requires little more than active directory credentials.

Conclusion

Hopefully this paper has helped to introduce some of the key concepts of the Preempt Platform. However this paper is certainly not an exhaustive of the solution's capabilities. We encourage you to continue to learn more by either seeing a demo or testing the solution in your environment, where we can show in detail how Preempt can help the unique needs of your network.