Investment Firm

Preempting potential threats with greater visibility and proactive controls

Summary

For a long term equity investment firm Preempt is working with, reducing risk and maintaining the security of their organization is a top priority. The company has vigilantly built a robust security strategy and actively looking to stay ahead of the threat. Despite this, having the proper visibility to avoid potential breaches and insider risks was an area of concern.

The Challenge

The organization regularly shares sensitive financial data with clients. To continually stay on top of things, the security team had their work cut out for them. The organization had already deployed a multitude of solutions for detecting malware and protecting the perimeter. However, this amount of detection and protection was not enough to enable the security team to feel they had the visibility they needed to understand what was happening on an individual administrator, user, or endpoint level.

As their Manager of Network Technology explained, lack of visibility and understanding into which users and endpoints presented a risk was an area of focus for them. For example, they needed to understand what accounts were stale or had weak passwords. And gaining a better sense of whether privileged accounts were shared or being used according to best practices was important. "The manual process of following up on incidents and reviewing logs was too time consuming and didn't provide the level of user or endpoint visibility we required. We wanted to improve our effectiveness with a more active and dynamic solution to stop potential threats and gather continuous insights to help us better understand our changing users and network."

3 Immediate Benefits

Gain network visibility to reduce the attack surface.

Ensure that privileged accounts being used consistent with corporate policy.

Identification of potential security risk of users and endpoints before they are compromised.

The Solution

The Preempt Behavioral Firewall couples User and Entity Behavior Analytics (UEBA) and Adaptive Response to proactively protect their organization and reduce risk from attackers and malicious insiders. By learning the behavior of every user including privileged user, system account and endpoint in the network, Preempt establishes real-time behavior-based policies, user-driven security, risk scoring and fine-grained automated actions to eliminate threats without manual intervention from their security team. Preempt customers also appreciate that the solution is easy to install and provides quick time to value.

The Result

Preempt's automated, behavioral-based solution immediately demonstrated its value to the team. It was installed in less than two hours and within weeks of having the solution installed and learning their users and network, they were able to not only reduce the number of unnecessary and stale privileged accounts but also were able to correct shared privileged accounts with higher security risk. They were also able to quickly improve the overall strength of passwords among its users. The Organization understood that reducing the attack surface was one of the most effective ways to reduce the likelihood of breaches and Preempt helped them do so.

Now, with Preempt, they gain an unprecedented amount of visibility which enables them to automatically preempt possible threats. This is based on a flexible policy that integrates user risk scores, type of threat, type of user and a granular response capability. With Preempt Insights, they gain powerful analytics and real-time visual snapshots of their network for a better understanding of their insecure users and endpoints. This enables them to continuously monitor their security posture and quickly assess which users present the most concern.

Preempt also provides them significant insights of their privileged users, including whether they are complying with corporate security policy, using weak passwords, sharing endpoints and passwords, and more.

> "The Preempt Behavioral Firewall delivered **immediate value** to the team. Within weeks we were able to reduce our attack surface, improve our password strength and correct privileged accounts that had high security risk. "
>
> Manager of Network Technology

preempt.com

info@preempt.com

Preempt protects enterprises from security breaches and malicious insiders with an innovative and patented approach that couples User and Entity Behavior Analysis and Adaptive Response to provide the most effective solution for both detecting and automatically responding to security threats. This proactive approach allows organizations to preempt threats in real-time without engaging already overwhelmed security teams.