Preempt

Delta Dental Plans Association

Preempting potential threats in real-time

DELTA DENTAL®

About DDPA

Delta Dental Plans Association (DDPA) is a not-for-profit organization with some for-profit affiliates as member companies. Delta Dental offers national dental coverage through 39 independent member companies. As America's largest and most trusted dental benefits carrier, maintaining the security of the organization is a top priority. As the Plans Association, DDPA drives IT security best practices and assists member companies with guidance, advice and partnerships for deploying their security infrastructure.

The Challenge

Despite having a SIEM solution, DDPA lacked the visibility and capacity to prevent credential misuse by attackers or insider threats in real-time. To solve this, the security team started looking at both Privileged Access Management solutions and User and Entity Behavior Analytics (UEBA) tools so that they could get visibility into privileged users, stale accounts and systems accounts to detect potential threats or risky behavior. The challenge they found was that while many of the UEBA players could provide them with visibility, they didn't have the ability to automatically block access requests in real time in response to threats. Additionally, they would have needed to spend a lot of time and effort building out the orchestration and multi-factor authentication capabilities not native to those UEBA solutions.

As Paul Soriano, Manager of Security Architecture at DDPA explained, lack of visibility into users and endpoints and not having the ability to quickly respond to possible threats presented a significant risk to the organization. In particular, they didn't have a sense of what privileged users were doing or whether privileged accounts were shared or being used according to best practices. "The ability to make sure that users are who they say they are, particularly privileged users, is extremely important. Active Directory is an important asset so having identity verification before they gain access to the system is critical to maintaining security."

3 Immediate Benefits

☑ Detects and blocks suspicious activity in real-time

☑ Ensures privileged accounts are being used consistent with corporate policy

☑ Identifies potential security risk of users and endpoints before they are compromised

The Solution

Preempt provided DDPA with the Preempt Platform, a real-time conditional access and threat prevention solution, to gain more visibility, insights, protection and security team effectiveness. This is achieved by combining continuous behavioral analytics to detect suspicious behavior along with real-time automated response that securely authenticates the user and redirects risky user behavior and proactively stops threats without disrupting the business. Smart security controls such as multi-factor authentication, re-authentication, block, allow, isolation, notify and more can be implemented based on behavioral risk scoring or policy.

> "We looked at least four other solutions and none of the other solutions allowed us to be able to block and respond to threats in real-time. This was the driving factor for us selecting Preempt."
>
> Fred Kwong, CISO at DDPA

The Result

Preempt's automated, behavioral-based solution immediately demonstrated its value. 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 get better visibility into users, privileged users, unmanaged endpoints, weak passwords, and more. They can very easily see what's going on now. "The visibility gives us a lot of comfort," stated Soriano. "In particular, being able to have better visibility into my privileged users and what they are doing is very important because of the data and systems they have access to. I want to make sure that the person logging into Active Directory is who he says he is. It's very important and seeing it in action is great."

Preempt has not only simplified following up on incidents, but the number one feature that DDPA gets the most value out of is Preempt's ability to respond in real-time to suspicious behavior and policy. "We looked at least four other solutions and none of the other solutions allowed us to be able to block and respond to threats in real-time. This was the driving factor for us selecting Preempt," stated Fred Kwong, CISO at DDPA.

The ability to have adaptive response based on risk allows them to add stronger enforcement where they need it along with the ability to auto-resolve many alerts and false positives, which is important for a small security team with limited resources. Preempt allows them to be able to ensure security without business disruption.ensure security without business disruption.

preempt