prēempt

CASE STUDY

Fortune 500 Enterprise Preempts Future Breaches

Remedying breach leads to embracing a holistic view of identity and proactive enforcement

Summary

A Fortune 500 company discovered an internal threat with significant ramifications for company financials and brand reputation. The breach involved a hacker moving laterally within their environment, with nearly unfettered access to proprietary and other confidential data. Despite having a robust security strategy, the organization lacked the visibility and real-time response capabilities to prevent these types of threats from taking a foothold in the organization.

Executive leadership requested Preempt to initially assist with the breach investigation. Based on early results, leadership identified Preempt as the solution to address the current gaps in their security posture, remediate the breach and avoid future breaches and internal threats while reducing their risk.

The Challenge

Prior to the breach, the company had significant exposure to a variety of hacks, from simple password exploits and phishing attempts to zero-day exploits. Due to a large global footprint, the company has a diverse, global and complex group of authentication ports numbering in the six figures. This globally distributed and initially disorganized variety of ports presented a significant challenge to organizational security. Once the company discovered the breach, they found the hacker's access to private data had the potential to adversely affect the company's financial standing, brand reputation and other business-critical factors such as customer loyalty and enterprise relationships. In sum, the company's lack of visibility into their network, inability to respond in real-time and disorganized password, access and authentication policies left them unable to respond and prevent a business-critical breach.

Immediate Benefits

- Now able to preempt threats and incidents in real-time
- Provided critical insights for breach investigation
- Gained control of privileged users
- Identified security vulnerabilities and risk of users and endpoints

The Solution

The organization chose to implement the Preempt Platform not only to help with the breach investigation and response but to provide them with a more holistic view of identity, greater visibility to reduce risk and real-time response capabilities to prevent future threats. Preempt detects and challenges anomalous or risky behavior and malicious tools, taking adaptive, automated action before access is granted. This in turn allows organizations to preempt incidents and threats in real-time. Preempt's team worked closely with the organization's Security Operations Center to address the threat at hand and analyze security incidents to focus on critical vulnerabilities first and foremost. With a globally renowned technical and engineering team, Preempt quickly became a top trusted advisor and partner to the enterprise, investigating and remedying the breach, while also putting into effect measures to preempt future intrusions.

The Result

The Preempt Platform immediately demonstrated its value. Without specific guidance from the customer on the presumed source of the breach, the Platform identified the source of the breach within 24 hours. Additionally, Preempt's platform from day one learned the organization's users and network and identified many areas to be addressed, including major vulnerabilities in their Active Directory and Active Directory services, presence of stealthy admins, users with passwords that did not expire, machines with vulnerable operating systems, users with SPNs and a lack of encryption.

Additionally, the organization used Preempt to find critical insights related to the investigation, including an exposed password belonging to a privileged account - despite deploying a leading Privileged Account Management (PAM) solution. Preempt subsequently linked the exposed password to one of the most significant threats. Within a week, the team quickly discovered the extent of the breach, including the internal threat's lateral movement within their environment for an extended period of time - which started with a single credential compromise. For traffic-related findings, the Platform located interactive logins by service accounts and LDAP Simple Bind clear-text authentication, all of which had contributed to the incident.

Since being deployed, the enterprise's IT management has been able to increase their use of Preempt by tenfold following a brief ramp-up and training period. With real-time response, they are able to continuously preempt threats by focusing on control of privileged users and unifying visibility across all accounts and platforms, allowing them to remediate incidents and reduce time and resources required to manage their security policy. In addition, the organization reduces and continuously monitors the number of unnecessary and stale privileged accounts, improve the overall strength of passwords among its users, and remediate vulnerabilities which helps them prevent accounts from being compromised.

preempt.com

info@preempt.com

Preempt protects organizations by eliminating internal threats and security breaches. Threats are not black or white and the Preempt Platform is the only solution that delivers identity and access threat 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