preempt

CASE STUDY

Dan Hotels Improves Security for Uninterrupted Hotel Operations

Gains visibility and control over user privileges and reduces the mean-time-to-detect threats

1000+ Users

3 Domain Controllers

2000+ Endpoints

Microsoft AD, Azure AD

"The Preempt Platform uncovered the hidden security risks in many parts of our Domain Controllers, and gave us actionable insights on our organization's security risks and events, in real-time."

Igor Lishnevsky, IT, Dan Hotels

CHALLENGES

- Continuous Active Directory security
- Continuous visibility into user privileges
- Reducing the mean time to detect threats

12X Reduction in Time to Detect Threats

Reduced the time to search and investigate an incident from 60 minutes down to just 5 minutes.

Operational Simplicity

Unified visibility and control for on-premises AD and Azure AD, reducing operational overhead.

High-Fidelity Security Alerts

Real-time detection of credential attacks to secure access to critical systems, like Microsoft Exchange server.

< 1 Week

Simplified deployment, without reboots or business disruption, and faster time-to-value with actionable insights.

ABOUT DAN HOTELS

Dan Hotels is a chain of Israeli luxury hotels.
Established in 1947
Employees: 5000
Rooms: 3500+ (International)
www.danhotels.com

SOLUTION

Real-time threat detection with the Preempt Platform

The design & implementation of the project was done by 10Root Cyber Security, Preempt's global partner.

"Preempt's real-time threat detection is not noisy. This means that we are confident about the accuracy of incident alerts and the actionable insights to remediate threats without any guesswork, saving us time and effort"

Yossi Gabay, VP of Information Technology, Dan Hotels

Continuous Active Directory Security — Across On-Premises & Clouds

Being a hotel with thousands of employees and operations in multiple countries, Dan Hotels wanted to have the right controls in place to ensure that their Active Directory environment stays secure – on-premises and clouds. The hotel's security and risk teams wanted to have a clear and holistic understanding of the events from their Domain Controllers (DCs) and their Active Directory policies and audit the authentication traffic hitting their on-premises AD and Azure AD. Preempt's unified visibility, without siloed use of tools, is especially useful as Dan Hotels ties in the authentication happening on Azure AD back to their on-premises AD.

Continuous Visibility into User Privileges

Being a dynamic hotel with 24x7 operations across multiple locations, Dan Hotels required complete visibility into what their users are doing - where are they logging in from, what they're accessing, and if they're accessing what they are supposed to access, deviations from normal behavior, and so on. With Preempt, Dan Hotels gained in-depth visibility into user privileges, behavior analytics, stealthy credentials, and risk scores of every human and service account that is accessing applications on-premises or in the cloud.

Reducing the Mean Time to Detect Threats

With the increasing sophistication of attacks, Dan Hotels realized that they needed a solution that would empower their security and identity teams to prioritize risky authentication activities in real-time (for example, detecting credential scanning attacks over NTLM). Dan Hotels understood that potential risky activities using NTLM, Kerberos, and RDPs to their DCs had to be discovered in real-time, instead of looking back into the logs and analyzing them. With Preempt's real-time threat detection and behavioral analytics, Dan Hotels was able to accurately pinpoint a credential attack happening on one of their on-premises Microsoft Exchange servers. The security team resolved this potential risky activity in under an hour.

About Preempt

Preempt secures all workforce identities to accelerate digital transformation. Since 80% of all breaches involve compromised credentials, Preempt unifies security visibility and control for on-premises and cloud identities. Threats are preempted and IT policy enforced in real-time using identity, behavioral, and risk analytics. Preempt protects 4M+ identities across 400+ enterprises.