HOSPITALITY INDUSTRY CASE STUDY

Dan Hotel Group Secures Its VDI From Advanced Threats

Customer Profile

Dan Hotels is the largest luxury hotel chain in Israel with 13 hotel properties, as well as other business interests including apartments, commercial space and two vocational schools.

Challenge

The Dan Hotel group, like most luxury hotel chains, knows the importance of technology for streamlining operations, expanding opportunities and providing an outstanding customer experience. However, it also understands the enormous risks that come with digital adoption. It's no coincidence that Dan Hotels' VP of IT, Yossi Gabay, comes from the IDF's infamous 8200 security unit.

"It's not just a matter of compliance. As the leading hotel brand in the country, security here means to secure our name. We have a mandate to protect our customers' personal and financial information and the level of service they receive," says Gabay. "Whatever happens, operations cannot stop, 24 hours per day, 7 days a week."

Dan Hotels utilizes a VDI system across its properties that brings consistency, control and efficiency but also increases threat exposure. A breach in one endpoint could put the entire infrastructure at risk. Assessing the threat landscape, Gabay saw that the company's classic security stack of network security and antivirus left it increasingly vulnerable to advanced attacks. He knew he needed a technology that could tackle all the newly emerging advanced threats before Dan Hotels became another entry in the long list of hotel breaches.

A VDI environment, however, poses particular challenges – any security solution must be extremely lightweight so that it doesn't lower consolidation ratios. It also can't rely on signatures or other methods that require updates as this impacts system load times.

INDUSTRY

Hotels

ENVIRONMENT

- 1000 endpoints, the majority running as VDI terminals
- Distributed environment including hotel properties, corporate operations office and call center
- AV and network security in place

CHALLENGES

- Protect sensitive financial and personally identifiable information
- Bookings via third-party OTAs increase risk exposure
- Zero tolerance for breaches or disruptions - must be operational 24/7
- Protect brand reputation

SOLUTION

- Deploy Morphisec across all VDI terminals and other endpoints
- Protect the entire enterprise from advanced attacks without adding to the IT burden with maintenance requirements or false positive alerts

MORPHISEC
Moving Target Defense

"The effectiveness of Morphisec's endpoint protection is unequaled. This is the first security product I have ever seen that does its job as advertised and is literally an 'Install & Forget' solution."

— Yossi Gabay, VP of Information Technology at Dan Hotels

Solution

Gabay heads a dedicated team that deals with all aspects of IT operations, user support, and security. He has built a robust environment backed up by efficient processes and tools to handle operations vital to the business. He abhors unnecessary complexity and seeks cutting-edge technologies that adhere to this principal.

In researching the latest security solutions, Gabay came across Morphisec's Moving Target Defense approach and was immediately intrigued by its ability to prevent advanced threats without relying on any prior knowledge. Its minimal footprint also made it uniquely well-suited to Dan Hotels' VDI environment.

After extensive comparison testing, Gabay selected Morphisec Endpoint Threat Prevention. "I was impressed not only with Morphisec's groundbreaking technology but with the extremely high level of expertise I encountered," says Gabay. "I could trust that the product would perform as promised. And it does."

Once the selection was made, implementation proceeded quickly and easily. The solution was rolled out in three phases: first on the dozens of virtualized servers, next the higher risk endpoints and then the remaining end-points. All prevention functionality kicked in at the moment of installation, with no configuring, learning, database connections, tuning or rule setting.

Results

Dan Hotels' entire VDI is now protected from zero-days and advanced attacks like evasive exploits, browser-based attacks, fileless threats and backdoor, supply-chain attacks. Since installing Morphisec, the hotel group has had no breaches or operational disruptions from security incidents. Gabay and his team appreciate that Morphisec has zero associated maintenance, no false alerts and minimal to no interaction with the end user. Most importantly, the hotel group can be secure in its commitment to be operational 24/7 for its customers and protect their sensi-tive information.

Schedule a demo now: demo@morphisec.com

MORPHISEC
Moving Target Defense

www.morphisec.com