cybereason® | CASE STUDY

Global Real Estate Development

GLOBAL DEVELOPER OF LUXURY REAL ESTATE

LOCATION
Dubai, United Arab Emirates

INDUSTRY
Global Real Estate Development

CYBEREASON SOLUTIONS
EDR, ENDPOINT CONTROLS, NGAV, MDR

> "The DNA of the company and the passion translate into the product, the features, and the customer success."
>
> DIRECTOR OF INFORMATION SECURITY AND GOVERNANCE

THE CHALLENGE

As one of the premier luxury real estate developers in the world, with operations in 38 countries, this global real estate development company has undertaken a digital transformation that is moving the operations and support for 1,600 employees and 3,300 endpoints to the cloud. But legacy anti-virus tools overwhelmed the four-person security team with alerts. The result was a mean-time-to-detect and a mean-time-to-respond (MTTR) of as long as five days.

They needed a security solution that could drastically improve detection and response times and provide robust Endpoint Controls and Predictive Ransomware Protection without busting the bank.

SOLUTION

- Combines advanced prevention and endpoint controls with rapid detection to leverage deep contextual correlations across all endpoints in real time.
- The operation-centric MalOp™ Detection Engine provided analysts the context they needed to be proactive, from root cause to every affected endpoint and user, with real-time, multi-stage displays of the complete attack details. Decreasing MTTR from 5 days to just a couple of hours.
- Cybereason NGAV helped them to move beyond signature-based malware detection to leverage 9 unique prevention layers capable of ending attacks earlier in the kill chain, stopping any form of ransomware, even those never before seen and achieving nation-state level prevention, without losing operational simplicity.

EFFECTIVE, EFFICIENT, AFFORDABLE, SCALABLE

Just 14 months ago, the company was at the beginning of a major enterprisewide digital transformation to the cloud. From a security perspective, the company had many challenges.

To ensure security during this time of great change, the security team set out to find a security platform that could meet the company's unique criteria. They needed:

- SECURITY CONTROLS DEPLOYED QUICKLY AND WITHOUT BREAKING THE BANK
- A CLOUD-FIRST SOLUTION WITH THE UTMOST CAPABILITIES AND AS FEW MAINTENANCE REQUIREMENTS AS POSSIBLE
- A SOLUTION THAT WOULD NOT OVERLOAD THEIR ANALYSTS WITH ALERTS
- CAPABILITIES TO SUPPORT A LEGACY ENVIRONMENT WHILE THE COMPANY MIGRATED TO THE CLOUD

THREE REASONS TO CHOOSE CYBEREASON

#1 THE PEOPLE

"What got us behind Cybereason was, first, the people," the Director of Security said. "Knowing Cybereason was built by people who are actually from the offensive side of security was important because they understand the adversaries like no other. They've been on the frontline, so they know the tactics, techniques, and procedures used by hackers in much more detail," he said.

#2 THE MALOP

Cybereason's MalOp Detection Engine consolidates alerts into a single operation. It makes sense of complex data relationships and behaviors to stitch together the separate components of an attack, including all users, devices, identities, and network connections into an operation-centric view.

The company's Director of Security used CrowdStrike for the better part of five years, and his experience was less than stellar. "We had to go through individual alerts," he said. "It took a lot of time to respond to an alert. So the MalOp really made sense, especially because our team is small, and we don't have the luxury of managing it completely."

#3 SUPERIOR TECHNOLOGY

Working with Cybereason, they were able to deploy, configure, and begin security monitoring on hundreds of endpoints in two weeks. "The policies took one call to configure, and to my surprise, the person who had not worked on EDR before got the hang of it and he was able to configure the policies himself for workstations and servers," according to the Director of Security. "In a matter of two calls, we were able to go online. We started off with 100 endpoints and then moved on to 300 and 500 servers and machines in two weeks."

The Cybereason Defense Platform demonstrated its muscle immediately. Before Cybereason, one member of the company's security team could manage only two platforms. With Cybereason, two people are able to manage 13 different technologies. "Even when I'm not in the office and some alert comes up we can connect from home, and take action. That really helped us to increase our response time ," the Director of Security said.