SECURITY SOFTWARE CASE STUDY

Security Software Company Leverages Morphisec to Prevent Advanced Threats

Customer Profile

A leading provider of cloud and on-premises security solutions with numerous development locations across the globe and serving thousands of customers worldwide.

Challenge

The company is regularly targeted by advanced attacks, which posed an increasing threat despite a full complement of network and endpoint security tools. As a trusted cybersecurity provider itself, the organization's security must be watertight; a compromise or breach in the company means a breach in the trust of its customers. It is simply unthinkable.

The company's current endpoint stack included antivirus and a top-tier Endpoint Detection and Remediation (EDR) product but did not provide enough protection against the most advanced, in-memory attacks. Moreover, the EDR tool in place is time-intensive to manage and the company did not want to support another high- maintenance solution. While the company has a solid, highly-efficient SecOps team, its resources were stretched thin with false alerts and remediation tasks.

The company needed to optimize its endpoint stack on multiple fronts – cutting its threat exposure, simplifying management and minimizing the impact on systems and work. Anything that would interfere with providing a high-quality customer user experience would have been unacceptable.

"With Morphisec, we met our goal of securing our company against advanced attacks without adding staff resources, burdening security with false alerts or sacrificing performance."

— Security Officer, NASDAQ-listed Security Software Company

INDUSTRY

Cloud and on-premises security software

ENVIRONMENT

- 1300 endpoints
- Multiple networked development sites across the globe
- 30% of users work remotely
- Users have admin rights, increasing threat exposure

CHALLENGES

- Regular target of highly advanced threats
- Existing advance threat protection difficult to manage and not effective enough
- The company used a competitor's NGAV product in the past that caused conflicts and interfered with end users
- Zero-tolerance for breaches

SOLUTION

- Build an optimized endpoint stack including anti-virus, EDR and Morphisec for advanced threat prevention
- Secure company against advanced attacks without adding staff resources, introducing system latency or creating false alerts

MORPHISEC
Moving Target Defense

Solution

Of course, a company full of security experts is going to conduct extremely rigorous and thorough testing. They set up a test environment to run head-to-head comparisons of a long list of contenders, including incumbents, next-gen solutions and innovative start-ups. The trial environment allowed them to evaluate not only effectiveness in preventing threats but overall usability and disruption to its business operating environment. It threw the most evasive and sinister attacks at the candidates, both alone and as part of a full security stack. The company also tested its current stack for comparison control. Morphisec scored an order of magnitude higher. In the end, Morphisec was the one left standing, with top prevention efficacy and the lowest number of integration and compatibility issues.

Once the security team selected Morphisec, they proceeded with initial deployment on one hundred of its most complex endpoints. They experienced only a single compatibility issue, which was resolved immediately in close cooperation with Morphisec. After a short period of observation, with no problems arising, they decided to deploy the solution across the full enterprise. The team appreciated the very rapid time to value, with no waiting for database updates, rule setting, complicated configurations, or system learning requirements. One of its security specialists commented, "It's rare to work with such like-minded experts, who deeply understand our needs and challenges. Morphisec's commitment shows both in the way the product works and the way the Morphisec team responds."

Results

Since deployment, Morphisec has prevented multiple vicious, advanced targeted attacks, including a fileless Kovter variant delivered through Skype spam web links. The attack vector had been dramatically modified from previously seen versions and breached the defenses of many other companies, but Morphisec's built-in resiliency kept the customer fully protected without any update required.

With Morphisec running on the company endpoints, there has been a significant reduction in the attack surface and zero associated maintenance. The SecOps team is not distracted by false alerts and can instead focus on other initiatives. Most importantly, the department is fulfilling its commitment to protect company assets, preserve system uptime and performance and uphold customer confidence.

Schedule a demo now: demo@morphisec.com

MORPHISEC
Moving Target Defense

www.morphisec.com