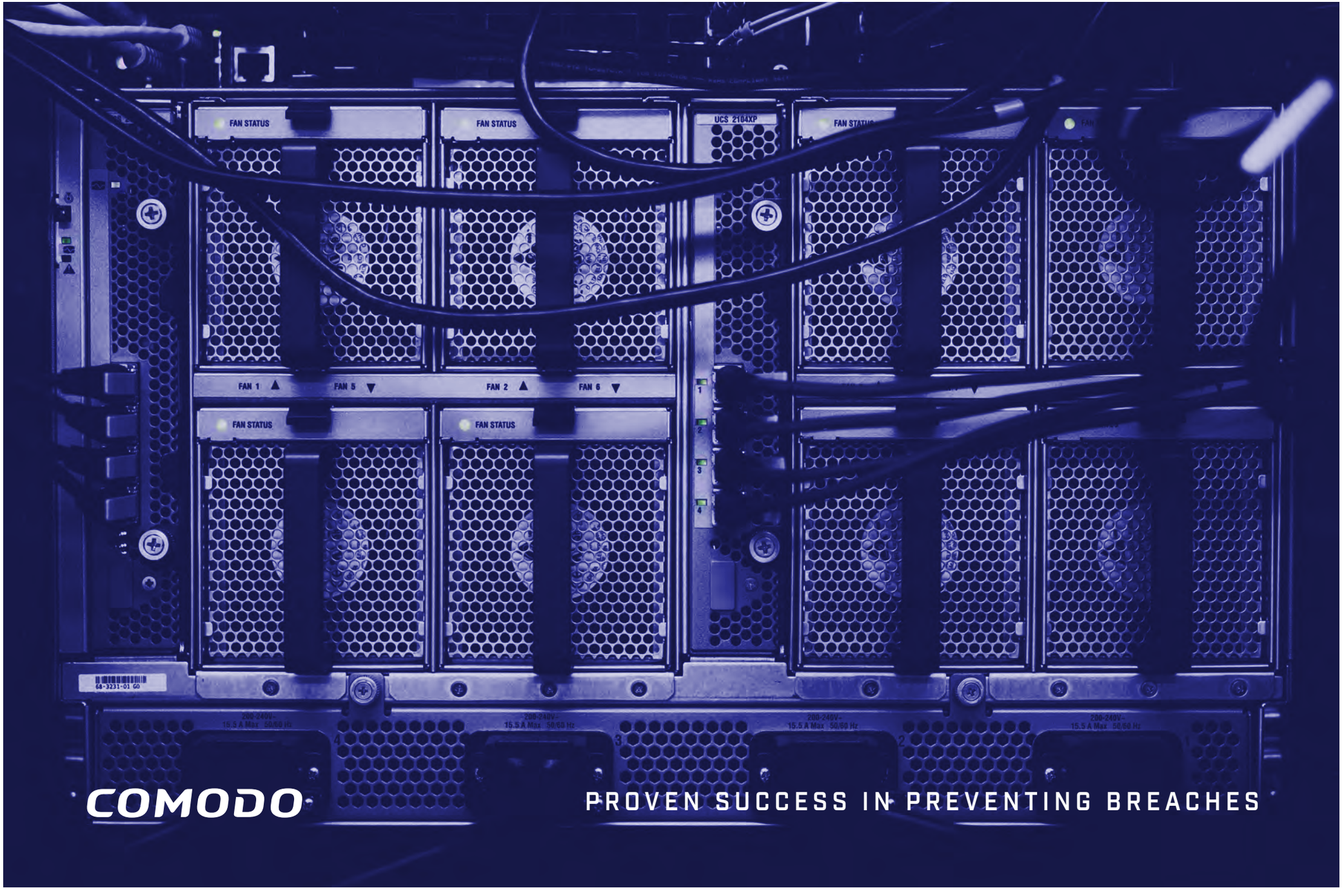
CASE STUDY: DATA PARTNER, INC.



CASE STUDY: DATA PARTNER, INC.

ABOUT DATA PARTNER

CYBERSECURITY SOLUTIONS PROVIDER

Established in 2001, Data Partner, Inc. has been providing businesses worldwide with complete IT solutions focusing on key critical elements. Over the years, Data Partner, Inc. has evolved their business model alongside the growing need for increased security and simplicity that today's IT world demands. Data Partner, Inc. utilizes their teams' years of experience to learn the details of their customers' environments and offers customers a state of the art, custom, and cost effective long-term solution to meet all their business needs.

Headquartered in Bloomfield Hills, Michigan, Data Partner, Inc. manages around a total of 230 clients and internally manages 50 employee endpoints. Eric, Lead Solutions Architect at Data Partner, Inc. has been with the company for over two years and manages endpoint protection for Data Partner, Inc. employee devices.

230+
CUSTOMERS WORLDWIDE

Michigan
BLOOMFIELD HILLS HEADQUARTERS

TWO
DECADES OF BUSINESS

CASE STUDY: DATA PARTNER, INC.

THE CHALLENGE

FINDING AN ENDPOINT SOLUTION THAT IS MORE THAN AI AND ML

When Eric joined Data Partner, Inc., Crowdstrike Endpoint Protection was deployed on internal Data Partner, Inc. devices and was also being promoted to their massive client base. As Eric managed this solution to prevent breaches for Data Partner, Inc., he realized Crowdstrike is not transparent at all. Eric mentioned, ***"With Artificial Intelligence and Machine Learning solutions, you don't know what it's learning and you have to trust that it's doing well. These solutions have the capacity to learn from bad behaviors, which leads to an influx of false positives."***

On the search to find a solution that he could truly trust, Eric spent a weekend writing a zero-day threat to test various leading solutions. He created the zero-day threat and did a fifty-times encrypted package. He then inserted some typical strings from a couple of known "good" programs to trick solutions he was testing. He created the loader, used the reversed unicode character to make it look like a text file and then he put it onto a USB stick. When executed, the zero-day threat opens a reverse pcp listener and gives Eric full access to that endpoint. Once Eric gains full access of that endpoint, he is able to take screenshots, take mouse control, turn on the microphone and camera and pretty much do whatever he wants on that endpoint.

He uploaded his zero-day threat to VirusTotal and it passed all 28 virus checks, including vendors like Crowdstrike and Cylance. Eric took a device that he could test this threat on and when the device was offline and off the network, he ran his USB loader on it. From an end-user perspective, a text file opened up and when the file was closed by the user, it ran an invisible powershell script in the background and the user didn't notice any harm immediately. Eric then began taking control of the endpoint and was able to capture screenshots of the device remotely from his office. Because Eric's zero-day threat passed VirusTotal checks, Eric was not confident in what endpoint protection platform he was going to move forward with for Data Partner, Inc, as well as his clients.

Limited
VISIBILITY
OF UNKNOWN THREATS

False
POSITIVES
CONSTANTLY

Traditional
ANTIVIRUS
PROTECTION

CASE STUDY: DATA PARTNER, INC.

THE SOLUTION

SELECTING AN EPP THAT RECOGNIZED ERIC'S ZERO-DAY THREAT

During Eric's search for a more robust EPP solution, he came across Comodo. He participated in a demo of Comodo's Advanced Endpoint Protection and began testing the solution on a test device. After he uploaded his zero-day threat to VirusTotal and did not receive promising results, he decided to run his zero-day threat on his Comodo test device. After leading vendors did not pass his test, he did not know what the outcome would be with Comodo.

Eric ran the zero-day threat on his Comodo test device and Comodo's Advanced Endpoint Protection immediately recognized that the notepad file may not be safe and put notepad into a container, even though notepad had nothing to do with the code string that was deploying. Advanced Endpoint Protection realized that notepad was the first part of a chain of executables. It let notepad open, however it put notepad into a container, which restricted the zero-day's write privileges to the memory, causing the powershell to fail and preventing the damage that could have occurred from Eric's zero-day threat.

Ultimately, the fact that Comodo's Advanced Endpoint Protection prevented damage from the zero-day threat Eric created, swung the decision to Comodo. However, that was not the only reason Eric decided to move forward with Comodo. Along with choosing Comodo's Advanced Endpoint Protection, Eric also gained access to additional IT management tools at no additional cost in one centralized platform. Eric leverages Comodo Remote Monitoring, Patch Management and Mobile Device Management. He also likes the Comodo Platform for asset management and mentioned that it is a nice inventory tool that allows him to view everything.

THE RESULTS

COMODO IS DATA PARTNER'S GO-TO ENDPOINT SECURITY VENDOR

Eric successfully deployed Comodo Advanced Endpoint Protection internally on all devices within Data Partner, Inc., consisting of majority Windows devices, but also some Androids, iPhones and Linux servers. Because of Eric's confidence in Comodo's Advanced Endpoint Protection, Comodo will be the only endpoint security vendor that Data Partner, Inc. recommends to their clients moving forward. Leveraging the additional IT management tools in Comodo's Platform enables Eric to help Data Partner, Inc. clients save money, which they would be spending otherwise on expensive IT management tools.

Currently, Data Partner, Inc. is a reseller to their clients, however they are striving to be a Managed Security Service Provider (MSSP), managing security and IT management for their clients. Data Partner Inc. will be creating a security bundle that they will offer as an MSSP, including Comodo Advanced Endpoint Protection as their leading solution.

CASE STUDY: DATA PARTNER, INC.

ABOUT COMODO

In a world where preventing all cyberattacks is impossible, Comodo Cybersecurity provides Active Breach Protection with its cloud-delivered cybersecurity platform. The Comodo Cybersecurity Platform provides a zero trust security environment that verdicts 100% of unknown files. The platform renders an almost immediate verdict on the status of any unknown file, so it can be handled accordingly by either software or human analysts. This shift from reactive to proactive is what makes Comodo Cybersecurity unique and gives us the capacity to protect your business – from network to web to cloud – with confidence and efficacy.

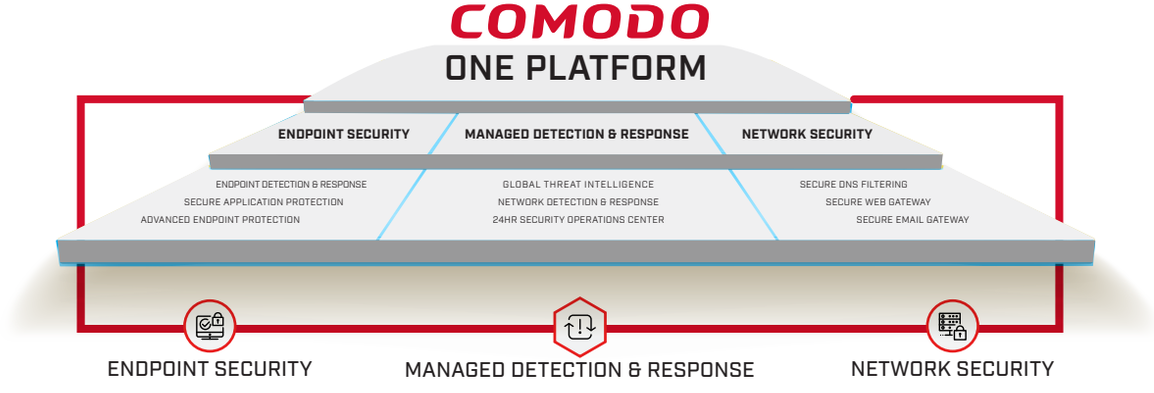
Comodo has experts and analysts in 185 countries, protecting 100 million endpoints and serving 200,000 customers globally. Based in Clifton, New Jersey, Comodo Cybersecurity has a 20-year history of protecting the most sensitive data for both businesses and consumers worldwide.

ACTIVE BREACH PROTECTION PREVENTS DAMAGE WITH THE INDUSTRY'S LEADING ZERO TRUST ARCHITECTURE

PROTECT THREAT VECTORS WITH OUR ZERO TRUST SECURITY POSTURE

ENABLE CYBERSECURITY SOLUTIONS FROM OUR ONE CENTRAL PLATFORM

ELIMINATE ALERT FATIGUE WITH CLOUD-NATIVE ARCHITECTURE & THREAT DETECTION



COMODO CORPORATE HEADQUARTERS
1255 BROAD STREET, CLIFTON, NJ 07013 USA

Experienced a breach? Contact us at (888) 551-1531
Visit **comodo.com** for your free 30 day trial

COMODO

PROVEN SUCCESS IN PREVENTING BREACHES