Case Study

Polymer manufacturer turns to Binary Defense MDR after breach

Business:

Global polymer manufacturer in multiple market verticals

Challenges

Three-person IT team has competing priorities

Outdated antivirus software presented a security risk

Security breach occurred and IT team needed to mitigate damage

Results

Binary Defense Managed Detection & Response installed quickly to determine source of breach

Binary Defense works as an extension of the Chemence IT team

Customer values personal relationships with Binary Defense experts and support team

---

"The ease and speed of [Binary Defense MDR] deployment helped us find out that the source of our breach was out of date antivirus across the network. Binary Defense gave us the insight into the attacks that were happening and prompted us to lock down the network more than ever before." -Zac Valentine, IT Director, Chemence

Global polymer manufacturer faces cybersecurity challenges
Atlanta, Georgia-based Chemence® specializes in polymerizable technology and serves multiple industries, including medical, industrial, cosmetics and consumer adhesives. Founded in 1983, the company has grown to have global reach and is continuously innovating in the area of polymers. Chemence employs over 200 people in three offices in the United States, and is planning to grow into a fourth facility soon. With proprietary research and data around the innovations taking place at the organization, keeping information secure is a top priority.

Zac Valentine is the IT Director for Chemence, tasked with a multitude of duties, including network infrastructure, servers, security, hardware and software purchasing, configurations, and strategizing for process improvement, reducing cost and reducing the company's footprint. His team consists of one full-time staff member and an outside consultant who is brought in for larger projects/troubleshooting. In addition to the full plate of responsibilities, "the three of us juggle reviewing security notifications," Valentine said. "The challenges of the day often supercede planning to guard against the theoretically possible future."

This scenario is not unusual—many small-to-medium-sized businesses (SMBs) are understaffed and have competing priorities. 62% of SMBs don't have an up-to-date or active cybersecurity strategy in place. SMBs are increasingly becoming targets for cyberattacks, with 1 in 3 SMBs reporting a breach within the past five years.

One day, the odds caught up to them. Chemence was breached.

When a breach occurred, Binary Defense was the answer
Chemence was using a basic Gateway UTM configuration and an antivirus program that was several years old. Valentine had researched several cybersecurity platforms over the years, but had never found the right fit for his organization.

Once the breach occurred, Valentine had to act quickly to get to the source and mitigate the damage. He found that the outdated antivirus program was ultimately what led to a breach getting through and knew that he needed to find a cybersecurity vendor partner to work with moving forward. Binary Defense was that partner, and Managed Detection & Response (MDR) was the solution.

Having MDR is like having active surveillance for your organization's network. Once MDR was installed, the Security Operations Center (SOC) at Binary Defense's home office in Ohio began to monitor each endpoint (e.g., laptop, desktop computer, server, etc.) in the Chemence organization. The SOC watches for abnormal behavior 24 hours a day, seven days a week.

Binary Defense MDR

No need for big IT budget or additional staff

Keeps your business secure and builds customer trust

Flexible packages, scalable

Binary Defense SOC

Your proxy cybersecurity team

Dedicated, US-based security analysts

Around-the-clock monitoring of your business

Can detect known malware as well as abnormal activity immediately

---

"Binary Defense has proven its salt and I trust it with my domains implicitly."
-Zac Valentine

Suspicious activity will trigger an alarm, which is reviewed by an expert security analyst. This information is then shared with the customer or its Managed Service Provider, if applicable.

"The ease and speed of [Binary Defense MDR] deployment helped us find out that the source of our breach was out of date antivirus across the network. Binary Defense gave us the insight into the attacks that were happening and prompted us to lock down the network more than ever before," Valentine said. "I was taken aback by how helpful everyone involved [from Binary Defense] was, willing to go above and beyond to help us."

That was a year ago.

Today, "network breaches aren't keeping me up at night, because I know Binary Defense is filtering through all the data passing each of my endpoints," Valentine said. "Trust is a difficult thing to gain and even harder to hold, but for over a year now, Binary Defense has proven its salt and I trust it with my domains implicitly."

An extension of the Chemence team
Valentine is extremely pleased with the support he receives from Binary Defense. "Binary Defense is my favorite vendor and platform," Valentine said. "I rarely have to call Binary Defense these days, but when I do, I know I am going to reach MY technician and they are going to know exactly what is going on with my network and my machines. I don't have to update anyone when seeking my own answers."

Valentine and his team still juggle multiple areas of responsibility, and he feels he still does not have enough time in the stay to keep up with all the latest variants, attack vectors and malicious activity that could be impacting the company. He credits the Binary Defense team and their insights on the current threat landscape for helping him stay informed. "I like getting [the Threat Watch emails] every day to catch a glimpse of new threats on the rise," he said. "It helps keep security at the forefront of my mind so I don't take for granted that everything is running fine. Knowing that Binary Defense knows what's going on is a real assurance."

"Defense in Depth" is best practice for cybersecurity
Chemence's story is not unusual—many companies find themselves in the same situation. An organization's IT team can only handle so much in a day, and cybersecurity isn't on their radar because nothing "bad" has happened.

Proactive measures are recommended to detect, contain and protect your organization's assets. Antivirus software, paired with an MDR solution, or even a SIEM, can help to ward off a breach. Multiple "layers" of security is known as "Defense in Depth" and is considered a best practice for cybersecurity.