Malwarebytes

CASE STUDY

Kraft Heinz scales and automates global endpoint incident response

Accelerated response time to minutes

Reduced the risk of a breach

Threats remediated transparently for the end user

Orchestrated automated security processes

Business profile

The Kraft Heinz Company is one of the largest food and beverage companies in the world with an unparalleled portfolio of iconic and new brands in retail and foodservice channels. With more than 38,000 employees across the globe and a large amount of intellectual property to protect, Kraft Heinz chose Malwarebytes Incident Response to automate its global endpoint security response and remediation process.

Challenges

Time consuming remediation processes
The SOC team applies a best practice approach of multi-layered security to safeguard the company's confidential data, as well as ensure global production remains online and operational. With business operations running in more than 40 countries across the globe, security operations is an around-the-clock function to keep the company's infrastructure protected and up and running, including more than 30,000 endpoints.

The SOC team was receiving consistent detections from its security layers that zero-day malware, potentially unwanted programs (PUPs), and other threats had slipped past the endpoint protection software. However, acting on endpoint malware detections and remediating the issue was presenting several challenges.

One of the biggest hurdles was identifying which employee endpoint was infected. For detections that said a user had introduced malware from a malicious site, the company's web security solution was only providing the IP address of the infected endpoint. By the time the information was sent to the team, the endpoint had gone off the network. Tracking down the right machine after it reconnected with a new IP address was a manual and time-consuming effort.

OVERVIEW

CUSTOMER
Kraft Heinz Company

INDUSTRY
Food processing

LOCATION
40+ countries across North America, South America, Europe, Asia

SOLUTION
Malwarebytes Incident Response

Kraft Heinz

> With Malwarebytes automating remediation, we can see it's working well. Job done. Endpoint remediation doesn't require any tickets or any of our security team resources. An incident response process that was previously taking us a lot of effort is now down to minutes.
>
> Chris Leonard, Senior Manager, European IT Security and Global Compliance
> Kraft Heinz

"From the start, it could take a week to receive the event information followed by lengthy time cycles to chase down which machine it was. Then, we'd need to coordinate with the end user to gain access. It could sometimes take a while to pinpoint the computer, gain access to it, and then remove the malware," said Chris Leonard, Senior Manager, European IT Security and Global Compliance at Kraft Heinz.

When GDPR compliance was introduced, it served as a positive catalyst for the SOC team to pursue an automated approach for incident response that would reduce malware dwell time. "We had a GDPR project to address any possible risk of a cyberattack taking data out of our environment. We looked at our incident response process and wanted to take proactive steps to automate endpoint remediation and remove the risk of a malicious attack," said Leonard.

How Malwarebytes solved the problem

Malwarebytes Incident Response
Leonard had long known Malwarebytes as a reputable product that provides fast and effective remediation. "As we started our investigation for a solution, we really liked that we could simply download Malwarebytes and do a free proof of concept. From that firsthand experience we knew, with confidence, that it worked. That positive trial experience lead us to select Malwarebytes," said Leonard.

Kraft Heinz also liked that the Malwarebytes API supported integrations with the company's existing security investments to enable its goal to globally automate incident response actions. After purchasing Malwarebytes, the security team used the Malwarebytes API to integrate remediation processes with their security incident and event management (SIEM) solution.

A fully automated process
Now, when the company's firewall or other security layers detect an endpoint malware issue, the SIEM receives the event information, which indicates that an end user's endpoint just got a malware infection. A fully automated process that pushes out the Malwarebytes non-persistent agent to the infected endpoint is then kicked off. Malwarebytes performs complete remediation to disinfect the machine, and then the agent is removed.

"With Malwarebytes automating remediation, we can see it's working well. Job done. Endpoint remediation doesn't require any tickets or any of our security team resources. An incident response process that was previously taking us a lot of effort is now down to minutes," said Leonard.

"The integration between Malwarebytes and our SIEM allows our security team to orchestrate a fast and effective process from detection to remediation that's fully automated and consistent across the globe," added Leonard.

> Malwarebytes' endpoint remediation is completely automated from the start right to the finish. Our security team doesn't even need to get involved. For us, it's a perfect solution—it just works.
>
> Chris Leonard, Senior Manager, European IT Security and Global Compliance
> Kraft Heinz

Incident response that just works

Even with ongoing end user security training, Leonard knows that it's impossible to stop employees from clicking on links and files. Therefore, the SOC team places importance on having a fast and effective endpoint remediation solution that's reliable across the company's global endpoints.

"Malwarebytes' endpoint remediation is completely automated from the start right to the finish. Our security team doesn't even need to get involved. For us, it's a perfect solution—it just works," said Leonard.

With Malwarebytes Incident Response, Kraft Heinz has an improved security posture, as well as peace of mind that confidential data is safe from a breach. Automating remediation with Malwarebytes also enables the company to demonstrate the rigor that it is applying towards GDPR compliance.

malwarebytes.com/business corporate-sales@malwarebytes.com 1.800.520.2796

Malwarebytes is a cybersecurity company that millions worldwide trust. Malwarebytes proactively protects people and businesses against malicious threats, including ransomware, that traditional antivirus solutions miss. The company's flagship product uses signature-less technologies to detect and stop a cyberattack before damage occurs. Learn more at www.malwarebytes.com.