CASE STUDY

Analog Devices automates its threat response process

Malwarebytes Incident Response improves remediation and reporting

Manual remediation costing $1,000 per endpoint

Powerful detection uncovers malware lurking on endpoints

Automated attack response provides prevention against a breach

Business profile

Analog Devices (ADI) is a Fortune 100 company and a world leader in the design, manufacture, and marketing of high-performance analog, mixed-signal, and digital signal processing (DSP) integrated circuits (ICs). The company's products are used in all types of electronic equipment. With more than 20,000 employees worldwide and a large amount of intellectual property to protect, Analog Devices chose Malwarebytes Incident Response to help automate its security response and remediation process.

Business challenge

Accelerating response and remediation

Analog Devices' innovative signal processing solutions are used by more than 100,000 customers worldwide. The company's products play a fundamental role in converting, conditioning, and processing real-world phenomena into electrical signals that are used in a wide array of electronic devices.

To protect its intellectual property and manufacturing processes, Analog Devices has built a formidable security infrastructure. Air-gapped and segmented networks create barriers to access in some areas. Multiple firewalls, perimeter security solutions, DLP, IPS, forensics tools, audit management software, endpoint antivirus, a threat hunting solution, and a Splunk SIEM create an arsenal of defense for other Analog Devices systems. The SOC team protects endpoints, such as desktop, laptop, and mobile devices, as well as mission-critical manufacturing systems running on Windows XP. Production simply cannot stop, and upgrading the Windows XP environment would require replacing hundreds of millions of dollars of equipment. In addition, the team did not want to add additional client software to systems.

OVERVIEW

INDUSTRY
Technology

BUSINESS CHALLENGE
Remediate threats that other systems miss and increase visibility into threats targeting the organization

IT ENVIRONMENT
Microsoft SCEP, IPS, Splunk, other layered enterprise security

SOLUTION
Malwarebytes Incident Response

> Malwarebytes is a huge help in automating attack response. Weather it's reducing the number of reimaged systems or providing valuable information for preventing a breach, Malwarebytes will make a significant difference in our security ROI.
>
> Bob Chadwick, Senior SOC Manager
> Analog Devices

"We were seeing a high number of endpoints that required reimaging, in spite of the controls in place," said Bob Chadwick, Senior SOC Manager at Analog Devices. "Many factors contribute to those numbers, but many were not remediated by Microsoft SCEP and we suspected that some cases were misdiagnosed malware."

When threats evaded the endpoint antivirus and other security controls, they infected systems before being discovered by RSA threat hunting software. With 20,000 endpoint systems globally, it is difficult to document each reimaging case, so the team lacked visibility into causes of infection. Reimaging is costly—each system costs approximately $1,000 to reimage, so Bob began looking for a way to significantly reduce the number of reimaged systems.

The solution

Malwarebytes Incident Response
Bob and his team evaluated the company's entire threat management process—from detection to remediation. After evaluating a range of potential solutions in the context of the existing environment, they decided to try Malwarebytes Incident Response.

"I had used Malwarebytes for many different purposes," said Bob. "When we took a look at Malwarebytes, everything fell into place."

Analog Devices wasn't looking for a single, end-to-end solution. Instead, the team liked Malwarebytes' flexibility to fit into their existing processes—in particular, the Malwarebytes Breach Remediation tool. Breach remediation is an agentless, lightweight tool that can be deployed and integrated with existing third-party tools.

Bob also liked the fact that Analog Devices could share threat information and collaborate with Malwarebytes and other Fortune 100 clients. They launched a proof of concept and chose it as an integral part of their automated response processes.

In the new process, Malwarebytes works with the company's existing SecureWorks, Microsoft System Center Endpoint Protection (SCEP) and other systems. If a threat evades other security measures, the team deploys Malwarebytes using Microsoft System Center Management. Malwarebytes Breach Remediation runs, cleans up infections, saves logs, and deletes itself, leaving no trace or resource-grabbing artifacts. All threats that Malwarebytes finds and remediates are documented in the company's Footprints ticketing system to provide metrics. Systems are only reimaged as a last resort.

Flexibility for systems around the world
Analog Devices engineers rely on compute-intensive applications, and any extra software on a system noticeably affects performance. Bob's team needed a solution that could be instantly deployed for remediation without disruption to users. When Malwarebytes is needed, the team can quickly install it, run it, and then delete it from the system.

"Our initial goal is to use Malwarebytes on infected machines," said Bob. "Eventually, we plan to install it permanently on a subset of systems to easily run ad hoc scans and then scale deployment over time."

Threat visibility for proactive defense

The SOC supports Analog Devices help desk teams globally. Every malware ticket generated is captured in the Footprints ticketing system. Monthly SCEP reports detail issues that were detected and remediated by SCEP. From the Footprints system, Bob can pull up reports of malware and junkware that SCEP missed and Malwarebytes remediated.

"Malwarebytes shows us malware that wasn't otherwise detected," said Bob. "Even if it is just PUPs or PUMs, those could affect system productivity for the user, or worse, be weaponized later and used to breach the network."

Malwarebytes Breach Remediation data is also forwarded to the Splunk SIEM for correlation with other log data using the Open IOC threat-sharing framework and giving Bob even greater visibility across the infrastructure. This capability is especially valuable for Analog Devices. As a Fortune 100 company working with large enterprises and government accounts, Analog Devices receives Indicator of Compromise (IOC) data alerting it to changes in the threat landscape. Malwarebytes gives Analog Devices a solution to have in place, just waiting to scan and remediate a system with the touch of a button.

"Malwarebytes is a huge help in automating attack response," said Bob. "Preparedness becomes return on investment. Whether it's reducing the number of reimaged systems or providing valuable information for preventing a breach, Malwarebytes will make a significant difference in our security ROI."

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.

Copyright © 2020, Malwarebytes. All rights reserved. Malwarebytes and the Malwarebytes logo are trademarks of Malwarebytes. Other marks and brands may be claimed as the property of others. All descriptions and specifications herein are subject to change without notice and are provided without warranty of any kind.