proofpoint

BENCHMARK ELECTRONICS SHORT-CIRCUITS THREATS

CUTS PHISHING LINES AND DEPLOYS PROACTIVE PROTECTION

CHALLENGE

- Stop impostor emails (business email compromise)
- Easily distinguish between legitimate senders and malicious email
- Prevent advanced threats from reaching employee inboxes
- Add a layer of protection to existing security infrastructure

SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection

RESULTS

- Prevented 90% of phishing and spoofing incidents
- Gained immediate visibility into attempted phishing attacks and user clicks for proactive investigation
- Saved staff time, reduced rack space, and simplified operations with cloud-based protection

Benchmark Electronics' mission is to design, develop, and deliver advanced technologies for defense and aerospace companies. However, the fight against impostor emails, phishing campaigns, and other malware was diverting valuable IT resources. The Fortune 1000 company was ready to do whatever it took to succeed.

With global operations, Benchmark Electronics employees around the world are targeted by cyber threats. Since 2007, Benchmark has seen volumes of email spam, malware, and other threats steadily increase. Before 2007, 1%–2% of the three to four million emails it received per day were suspicious. Today, 10–12 million emails traverse the network every day, and 8%–10% of them are malicious, aiming to steal employee credentials. That puts Benchmark at risk, in addition to threatening intellectual property related to customers' projects.

"We've seen a lot more phishing campaigns in just the past two years," said Michael Krogstad, Corporate IT Manager, Security and Governance at Benchmark Electronics. "We see it in the whole enterprise with malicious links and attachments that our antivirus and web filters were not catching."

IMPOSTOR EMAILS ADD UP FAST

Impostor email, or BEC, was a particular problem. Almost daily, employees received impostor emails that supposedly came from the CEO's office. Phishing campaigns increased, and they became more sophisticated. Impostor attacks started coming from supposed Benchmark suppliers demanding wire transfers of funds or from HR services organizations requesting W-2 forms. Some emails included malicious attachments disguised as invoices. Thanks to strong financial controls, no funds were lost. But the IT team was spending hours trying to distinguish between authentic and impostor emails and fighting off phishing campaigns.

"Benchmark does business with a large number of third-party companies that send email to us using our corporate email address," said Shawn Feezel, Senior Systems Administrator, IT Infrastructure and Operations at Benchmark Electronics. "If their email is hosted on a public cloud service, that complicates everything. I can add them to my safe list. But if I allow that specific cloud service, I allow everyone else that hosts mail through them, including spammers, phishers, and impostors."

CHANGING TACTICS

Around the same time, Benchmark was upgrading many of its IT systems, including security. Its aging IronPort systems were due for replacement, and IT wanted to add new layers of protection.

"We have enterprise-class solutions in place for filtering, firewalls, and intrusion prevention on the edge of the network," Krogstad said. "We also have antivirus on our endpoints. But that's only part of the solution because it's reactive. We needed proactive defense to keep the threats out."

SLAMMING THE DOOR ON THREATS

The security team contacted Proofpoint to learn more about Proofpoint Email Protection and Proofpoint Targeted Attack Protection (TAP). They learned how Proofpoint Email Protection defends against unwanted and malicious email, while Proofpoint Targeted Attack Protection (TAP) protects from advanced threats in email that use malicious attachments and URLs. During a

"With Proofpoint, more than 90% of email attacks are stopped before they reach employee inboxes. We went from seeing about 20 incidents per month to only one or two, and we haven't had a major targeted attack."

Shawn Feezel, Senior Systems Administrator, IT Infrastructure and Operations, Benchmark Electronics

four-week proof-of-concept test, the team saw how Proofpoint detected and stopped the impostor emails they were receiving, and they saw how it successfully blocked a cryptolocker attempt. A few weeks later, Benchmark rolled out the solutions across the organization's 10,000 mailboxes.

"Proofpoint just plugged into the middle of our infrastructure," Krogstad said. "It was really quite seamless."

PHISHING AND IMPOSTOR EMAILS SHARPLY REDUCED

"We've seen a huge reduction in phishing and impostor emails," Feezel said. "With Proofpoint, 90% or more attempts are prevented. We went from seeing about 20 incidents per month to only one or two, and we haven't had a major targeted attack."

Feezel also gained insight into email header information, so that he can identify impostor emails more easily. If a user clicks on a malicious URL, Proofpoint TAP can later block access to it. If something gets through, Feezel knows immediately.

SMART SEARCH ZEROES IN

Feezel also uses the Proofpoint Smart Search feature in Email Protection. With this advanced message tracing capability, he can quickly pinpoint hard-to-find log data and drill down into an individual email for a detailed view. For instance, when a user reported a problem with sending and receiving emails, Feezel looked at Smart Search and found that there was no route to the host. Right away, he knew what the issue was, and quickly resolved it.

VISIBILITY TURNS THE TABLES

"I'm a team of one, and our operations team includes 13 people," Krogstad said. "Proofpoint gives us breathing room. It's been performing so well that team members have been redeployed to work on more strategic projects. I haven't yet completely tapped into what's possible with Proofpoint."

Before Proofpoint, the IT team only knew about a phishing email if a user reported it. With TAP, they know when an attack occurs and whether or not the user clicked. Feezel said that when an executive received a phishing email, they knew immediately and were able to quickly check his machine to make sure that nothing malicious was installed.

CLOUD-BASED BENEFITS

"One reason we moved to Proofpoint was to benefit from a cloud-based solution," Feezel said. "We didn't have to deploy hardware on site, so I don't have to maintain or manage appliances at our locations."

The cloud-based solution also fit nicely with Benchmark's drive to upgrade and simplify IT. The team saved rack space in its data center and new disaster recovery site. It also reduces power requirements and saves time for the operations staff.

ALL SYSTEMS GO

New, best-in-class protection has made a big improvement in productivity for the internal IT and security organizations. Even though threats will continue, Benchmark can prevent them from reaching its employees.

"We'd rather not let threats in," Krogstad said. "When I can keep it from coming through the front door, that's always the best."

For more information, visit www.proofpoint.com.