

How Bella Vista POA Identifies and Stops Business Email Compromise Attacks in Real-Time

**INDUSTRY**

Real Estate

HEADQUARTERS

Bella Vista, Arkansas

COMPANY SIZE

50 employees

OVERVIEW

Bella Vista Property Owners Association (POA) is a private, member-based recreational community located in Northwest Arkansas. Spanning 36,000 acres, it offers an array of amenities including seven golf courses, seven stocked private lakes, miles of nature trails, swimming pools, a beach, parks, pavilions, an RV park, campground, and recreation centers. The POA manages these facilities for the benefit of property owners and members in the Bella Vista community.

OUR SOLUTION



“



Harmony Email and Collaboration's APIs seamlessly integrates with our collaborative cloud platforms and provides a transparent security layer that doesn't impede productivity.

Jack Brooks, IT manager at Bella Vista Property Owners Association

”

CHALLENGE

Business email compromise (BEC) attacks prey on our trust in digital communications. In this especially devious form of cybercrime, attackers impersonate executives, other insiders, or trusted partners by crafting convincing emails that trick employees into transferring funds or sharing sensitive data. These scams don't rely on malware or complex hacking techniques; they exploit human psychology and organizational processes to devastating and costly effect.

According to the FBI's Internet Crime Complaint Center, BEC attacks are among the top financially damaging Internet crime. In 2023, BEC and email account compromise (EAC) scams created about \$2.8 billion in global digital crime losses. That's up from \$2.4 billion in 2021.

Jack Brooks, IT manager at Bella Vista Property Owners Association (BVPOA), understands the risk. Recently, Brooks found that BVPOA was under attack -- an ongoing BEC attack. As Brooks explained, the company had recently witnessed several phishing and malware attacks, and he realized they were evolving in sophistication. "The reality is phishing attacks, smishing attacks, QR code scams, and other attacks can easily lead to operational disruption at any moment," Brooks said. As Brooks investigated with Check Point's Harmony Email and Collaboration security technology, they spotted the potentially costly BEC attack already underway.

Knowing that cybercriminals refine their tactics, organizations such as BVPOA must stay vigilant and adapt their security strategies to meet this persistent threat. During this time, Brooks realized that their existing email security defenses were not adequately protecting their traffic. He knew strategies against BEC attacks existed, such as employee training, email authentication protocols, and multi-factor verification for financial transactions, but human risk remained the security Achilles' heel. Brooks and the team then searched for an email security platform to provide the additional effective layer security they needed.

SOLUTION

Brooks and the BVPOA team contacted Check Point as part of their search. Following their initial discussions, the BVPOA team performed a proof-of-concept to determine if Check Point provided enhanced security over their current security defenses.



Having saved \$144,000 and prevented an administrative nightmare, BVPOA believes Check Point mitigates our cyber risks.

Jack Brooks, IT manager at Bella Vista Property Owners Association



Check Point deployed Harmony Email and Collaboration during that proof of concept. Check Point's Harmony Email and Collaboration provides comprehensive cloud-based security for businesses, protecting their email and collaboration tools against sophisticated threats like phishing, malware, and ransomware while simplifying management through a unified dashboard.

During the trial, the Check Point security analyst assisting with the deployment spotted an active machine-in-the-middle attack that had been missed entirely by their current security software. Having commandeered a BVPOA staffer's email during that attack, the attackers managed to read the financial emails and identified potential ways they could conduct their BEC attack. They then managed to insert themselves into an existing chain of emails and create a fraudulent vendor invoice based on the information they gathered. Thanks to the AI-based analysis within Harmony Email and Collaboration, which can capture and understand the context of BVPOA's environment, the system could spot the fraudulent BEC request for payment as it was well in-progress.

OUTCOME

Because Check Point Harmony Email and Collaboration caught the fraudulent invoice request just in time, the BVPOA's accounting team was able to stop the \$144,000 payment from being completed. While, as Brooks explained, BVPOA's accounting team typically verifies any requests for changes to financial transactions, because the attackers managed to make the request from someone inside the organization, the accounting team assumed the request was valid. "We got hold of the real vendor representative who told us they had requested no such change in payment and stopped the payment about 15 or 20 minutes before it would have gone through," said Brooks.

In addition to the fact that Check Point's solution picked up on an active attack, BVPOA's security team appreciates Harmony Email and Collaboration's ability to automate monitoring and some response levels, freeing the team to focus on other areas.

Additionally, the detection ability within Harmony Email and Collaboration detection self-improves as the system learns more about the environment and provides BVPOA semantic phishing analysis, more than 200 indicators of phishing model analysis, and extensive data security analytics that improve security.

Brooks finds those capabilities and Harmony Email and Collaboration's proven ability to identify sophisticated attacks underway all very reassuring. BVPOA appreciates how Harmony Email and Collaboration extends its protection beyond email and safeguards cloud collaboration tools such as Microsoft Teams and SharePoint. In the same way that Harmony Email and Collaboration scrutinizes email, it also analyses file shares, chat messages, and collaborative documents in real time as it hunts for malicious content, data leaks, and suspicious behaviors. "Harmony Email and Collaboration's APIs seamlessly integrates with our collaborative cloud platforms and provides a transparent security layer that doesn't impede productivity. It's particularly adept at thwarting phishing attempts via malicious links in Teams chats or documents shared in SharePoint while enforcing data loss prevention policies across the entire collaboration ecosystem," said Brooks.

In essence, "Harmony Email and Collaboration acts as a vigilant digital guardian, ensuring that the tools designed to enhance teamwork don't become conduits for cyber threats or data breaches. Having saved \$144,000 and prevented an administrative nightmare, BVPOA believes Check Point mitigates our cyber risks," said Brooks.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leading AI-powered, cloud-delivered cyber security platform provider protecting over 100,000 organizations worldwide. Check Point leverages the power of AI everywhere to enhance cyber security efficiency and accuracy through its Infinity Platform, with industry-leading catch rates enabling proactive threat anticipation and smarter, faster response times. The comprehensive platform includes cloud-delivered technologies consisting of Check Point Harmony to secure the workspace, Check Point CloudGuard to secure the cloud, Check Point Quantum to secure the network, and Check Point Infinity Core Services for collaborative security operations and services.

[LEARN MORE](#)

Worldwide Headquarters

5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters

100 Oracle Parkway, Suite 800, Redwood City, CA 94065

www.checkpoint.com

