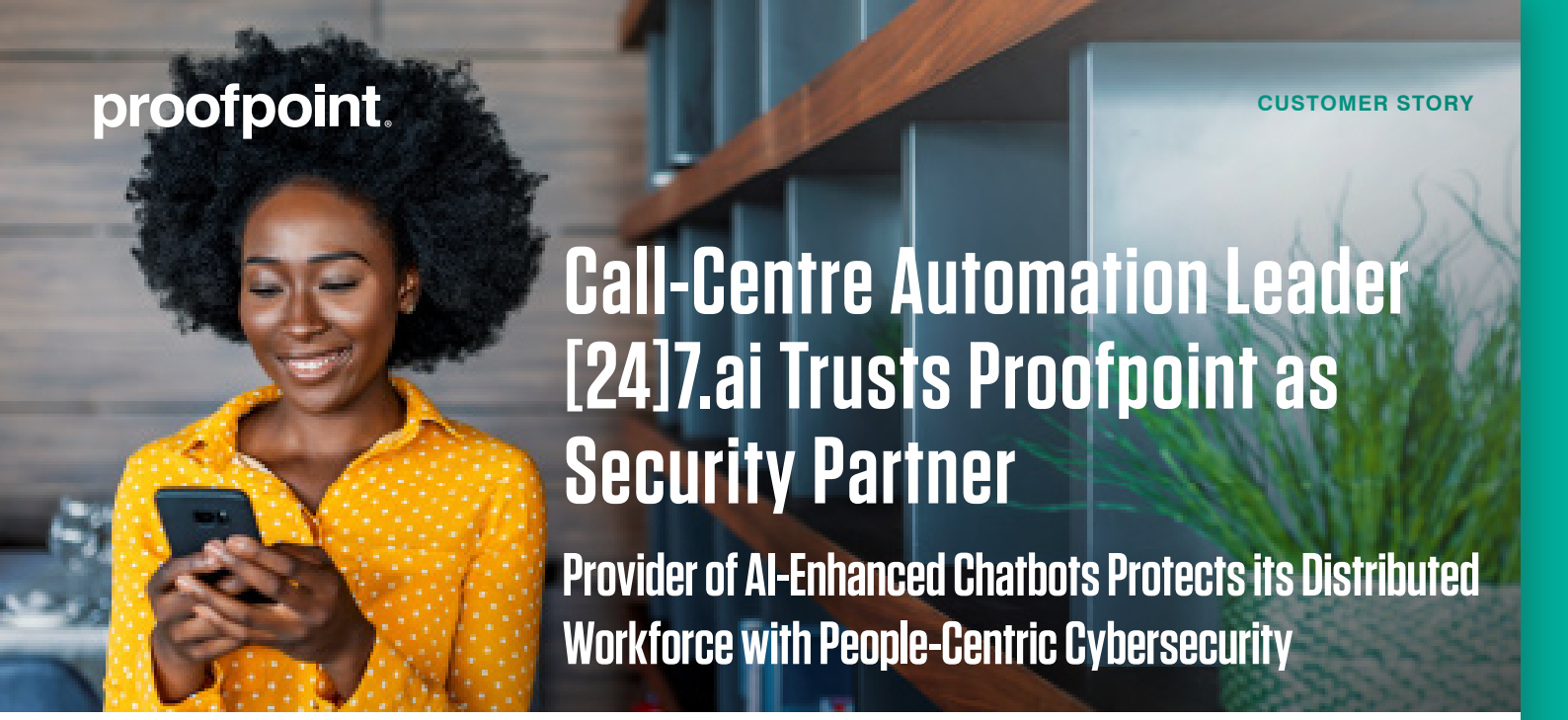


proofpoint.

CUSTOMER STORY

Call-Centre Automation Leader [24]7.ai Trusts Proofpoint as Security Partner

Provider of AI-Enhanced Chatbots Protects its Distributed Workforce with People-Centric Cybersecurity

THE CHALLENGE

- Safeguard intellectual property and customer data from a wide range of industries
- Protect a newly distributed workforce, including those working from home
- Scale up security capabilities without swelling budget

THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull

THE RESULTS

- Stopped a broad range of email threats
- Identified highly targeted users and departments in need of additional protection
- Secured remote workers and helped keep them compliant
- Augmented internal security team with outside threat intelligence and research

The Company

If you've ever felt trapped in a telephone menu tree, a nonsensical exchange with a chatbot, or even a call with a human customer-support rep who won't go off-script, [24]7.ai feels your pain.

The 20-year-old Silicon Valley company is on a quest to make customer service easier and more enjoyable—a mission that has grown ever more urgent amid a major shift to digital commerce and remote work. "If you have clients who go to your website and they can't find information very quickly and efficiently, they usually go away," says [24]7.ai Global CISO and Chief Privacy Officer Rebecca Wynn. "People don't have any patience anymore with that."

Companies usually come to [24]7.ai when they realise their customers are not happy with their online experience and are not completing sales. Think of it as the online equivalent of a shopper leaving their half-filled trolley in a supermarket aisle.

Even online, customers want a personal experience. That's inherently difficult for companies to scale. For [24]7.ai, the answer is a blend of artificial intelligence and human insight to predict and personalise customer experiences. The idea is to give digital interactions a more human-like touch by using artificial intelligence to better understand what help customers need and getting it to them quickly. This AI-powered conversation can adapt based on what device the customer is using, whether it's a laptop, smartphone, messaging service or a call to a live agent.

The company, originally named [24]7 Customer, began as a business process outsourcing (BPO) firm, or call centre. Clients relied on the company to outsource customer service functions, says [24]7.ai Vice President of Marketing Lisa Matherly.

The company's big pivot to AI was a natural outgrowth of its work with its customers. They were always looking for ways to make their customer support operations more efficient, voice agents more productive and the whole experience better for customers. [24]7.ai used what it learned in the process to build a portfolio of products that help automate many customer service tasks—and knows when to bring in people for things that need a more human touch.

[24]7.ai helps clients provide customers with a more personal and effortless experience. Its AI-powered digital and voice automation anticipates customers' needs for faster, better service. The company also offers self-service tools that allow clients to easily build, automate and optimise their own sales and customer service journeys.

The Challenge

Two critical aspects of [24]7.ai's business are protecting its intellectual property and keeping clients' information private.

The company has more than 200 patents approved or in process along with intellectual property that it keeps more closely held. Its customer data is just as important to protect. Some chat sessions, for instance, might include credit card numbers or personally identifiable information.

[24]7.ai's customer base runs the gamut of industry sectors. Many of those—such as healthcare, finance and government—are highly regulated. [24]7.ai must keep customer data out of the hands of cyber criminals and compliant with a growing myriad of regulations.

> "I look for who can be a good partner with me, who can be a great augmentation of my staff. We are in a cyber war and I need people who can be in that cyber war with me."
>
> **Rebecca Wynn**, Global CISO and Chief Privacy Officer, [24]7.ai

"Cybersecurity plays a big, big role in what we do," Wynn said. "We're fighting a cyber war with people who are behind another keyboard and who are trying to harm us all."

That fight has grown more complicated in the wake of Covid. The global pandemic has scattered workforces, pushed commerce to the web and created new security and compliance risks.

Fortunately, [24]7.ai was prepared. It had already begun making the shift to remote work when the pandemic hit, so it was better prepared than most to make the sudden switch. (A majority of its 10,000 employees now work from home; others collaborate at microsites designed to comply with local social distancing rules.)

It met with its key vendors, data centre operators and top customers to discuss how the pandemic might affect operations and map out how it can respond. As the company assembled a business continuity team and raced to reassure customers, new security implications took centre stage.

Data privacy is just one example.

"Who is a trusted person in the home?" and "What is a safe environment?" she said. "If your loved one comes over and says 'hi,' they might inadvertently see something on your screen."

The Solution

For [24]7.ai and other companies, the new working environment is really more like thousands of new working environments. Unlike an office, which offers uniform workspaces under easily controlled conditions, each home environment is unique. Companies must deal with countless combinations of device and networks—all out of reach of the IT, security and compliance departments.

To help manage the chaos, [24]7.ai crafted new acceptable-use agreements for corporate resources. In some cases, it even had employees send pictures of their working environments so the company could assure customers that their data is being properly managed and protected.

Remote work also meant doubling down on a people-centric approach to cybersecurity. While cyber attackers have long focused on people rather than traditional IT infrastructure, keeping them protected remotely can be even harder, Wynn says.

"I can't be a ghost in everyone's house," she said. "So what can I do to have the same security and privacy controls when they're on their computer?"

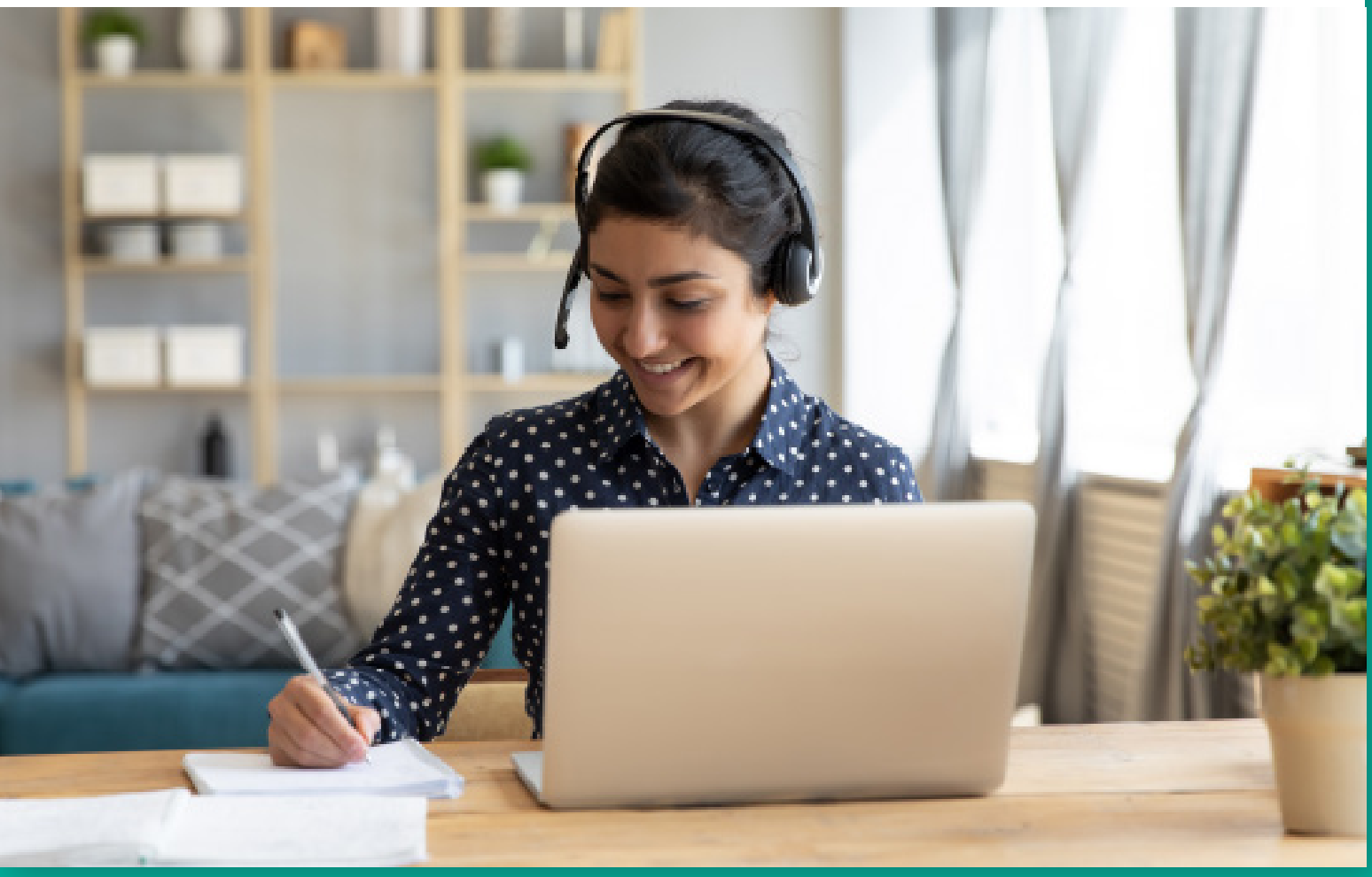
To meet the challenge, Wynn enlisted the help of Proofpoint, a cybersecurity vendor she calls a strong ally in her fight against cyber threats and compliance risks.

"One of the things that I look for is who can be a good partner with me, who can be a great augmentation of my staff," she said. "We are in a cyber war and I need people who can be in that cyber war with me."

The company uses Proofpoint Email Security to stop a wide range of cyber threats—in most cases, before they ever reach users' inbox. The award-winning solution stops spam, malware and attacks that use social engineering to exploit human nature rather than technical vulnerabilities.

These non-malware threats include email scams such as business email compromise (BEC). In BEC, attackers impersonate trusted colleagues, business partners and brands. And they do so in ways that aren't always easy to detect with conventional email defences.

When something gets through or turns malicious after being delivered, Proofpoint Threat Response Auto-Pull automatically removes the message—along with any copies that have been forwarded to other users.



The Results

The Proofpoint deployment has enabled [24]7.ai to take a people-centric approach to cybersecurity by providing visibility into the company's most heavily targeted users, or what Proofpoint calls Very Attacked People™.

"I can see which people, in which departments, are getting what kind of attacks," she said. "This allows me to see whether I need to do additional training or meet with people one-on-one. And it better prepares me to protect the whole company."

According to Wynn, one of the factors that makes Proofpoint such a valuable partner is its wide-ranging threat intelligence. Like [24]7.ai itself, Proofpoint works across many industries. That means Proofpoint can spot potential cyber threats against industries that [24]7.ai serves.

Wynn says Proofpoint has helped her become more efficient by becoming an extension of her internal security team. Thanks to Proofpoint investments into research and development and the scale of its threat intelligence, Wynn can redeploy her team to focus on security issues best managed internally.

"You guys are my team," Wynn says.

Having access to Proofpoint's cybersecurity data and insight gives [24]7.ai critical information in as close to real time as possible for it to make better decisions—making her team more efficient and her company more protected.

"Proofpoint allows me to sleep at night because of what they are doing for me," she said.

LEARN MORE

For more information, visit **proofpoint.com**.