

# Coca-Cola Beverages Northeast

>1 million

Emails autonomously analyzed  
each month by Darktrace / EMAIL™

3,000

security analyst investigation  
hours saved over 10 months

<1 minute

for Darktrace's Cyber AI Analyst to inves-  
tigate and respond to potential threats

Coca-Cola Beverages Northeast is a leading bottler and distributor of Coca-Cola products, serving communities across New England and upstate New York.

See how Coca-Cola Beverages Northeast (CCBN) seamlessly protects operations from AI-driven, email-based cyberattacks, experiencing zero email-based incidents since using Darktrace while achieving significant efficiency and productivity savings.

## Today's email attacks don't stand out. They blend in.

Coca-Cola Beverages Northeast (CCBN) plays a critical role in delivering iconic beverages to millions. With over 3,500 employees, email is not just an office tool but a critical business enabler for executing sales, coordinating distribution, connecting with suppliers, and keeping frontline teams and leadership aligned.

**It's also one of the most common paths attackers use to try to exploit trust and infiltrate organizations.**

"Darktrace gave our users the most control and the most context."

■ **Eric Bixby**

Director of Infrastructure and Security

## Phishing and impersonation threats

"In the cyber world, we're prime real estate," explains Eric Bixby, Director of Infrastructure and Security at CCBN. "Attackers study our brand, our partners, our vendors, and our people. They craft messages that look familiar, feel genuine, and quietly try to slip into busy inboxes."

Like many organizations, CCBN faces a constant stream of impersonation attempts, credential harvesting, and vendor-based fraud that traditional tools aren't designed to catch, including:

- Partner payment scams, where a seemingly legitimate request to update banking information could redirect funds to an attacker
- People and culture scams, where convincing HR-themed messages attempt to lead employees to fake login pages
- Vendor invoicing scams, where malicious attachments or links arrive through trusted supplier relationships

## High-volume email traffic

Email traffic at CCBN operates at enterprise scale. More than one million emails flow through the organization each month, which can translate into tens of thousands of potential alerts, far too many for a lean security team to manually investigate in real time.

### But one click is all it takes.

CCBN encountered a moment years earlier that underscored the importance of rapid email security. "That was a turning point," says Bixby. "Back then, we didn't have what we needed in place to stop it quickly. Today, we're focused on making sure something like that does not happen again."

# Choosing a Self-Learning AI defense

CCBN selected Darktrace / EMAIL™ to add a layer of AI-driven defense that could identify subtle anomalies, stop threats that bypass traditional filters, and respond autonomously at scale at machine speed. “Attackers are using AI to craft faster, smarter, more convincing messages, so we need AI working for us too,” explains Bixby.

Darktrace’s leadership in AI for cybersecurity, demonstrated success with global organizations, and performance against other solutions during proof-of-concept testing contributed to the decision. “We had the best results with Darktrace,” says Bixby.

He particularly appreciated Darktrace’s emphasis on user enablement through insights, which supports CCBN’s corporate goals for continuous cybersecurity education. “Darktrace gave our users the most control and the most context. Using the analysis view they could see why something was blocked and what factors drove the decision. That context builds awareness in the moment while reinforcing good habits.”

## Understanding what’s “normal”

A key differentiator was Darktrace’s Self-Learning AI, which models “normal” communication patterns for the organization and for individuals, then detects when something does not fit. This is especially valuable when threats arrive through trusted relationships, where static rules and reputation-based controls may not be enough.

Bixby says he saw Darktrace catch things other defenses did not. “Even when an email comes from someone a user would typically trust, Darktrace can recognize when something is anomalous and hold it.” He emphasizes, “People have relationships. AI doesn’t. It doesn’t play favorites. It just looks at what is normal and what is not.”

For example, an employee may receive an email from a trusted partner they frequently interact with that includes a “Download” button for an invoice. While the interaction itself isn’t unusual, Darktrace may identify a phishing link hidden behind the text.

## Helping every team focus on what they do best

Another decision factor was Darktrace’s ability to protect the business without adding friction for employees. Instead of relying solely on blanket blocking, CCBN can apply proportional controls based on risk, including holding suspicious messages, locking links, and applying clear warnings when needed.

“What may be normal activity for one user may be anomalous for another,” notes Bixby. “Darktrace recognizes that distinction, even when the user doesn’t, and takes action.”

“Attackers are using AI to craft faster, smarter, more convincing messages, so we need AI working for us too,”

### ■ Eric Bixby

Director of Infrastructure and Security

# Faster response, measurable savings, and zero incidents

Since implementing Darktrace / EMAIL™, CCBN has strengthened its resilience against email threats while significantly reducing the manual burden on its security team. “We haven’t experienced a single email-based incident since using Darktrace,” says Bixby.

## Security at scale

The platform scales effortlessly to the organization’s email environment, analyzing roughly one million messages each month without slowing business operations. That scale enables Darktrace to proactively reduce CCBN’s exposure to risk. Tens of thousands of junk or potentially harmful messages are neutralized or kept out of employee inboxes each month, limiting opportunities for phishing, impersonation, and fraud before they can take hold.

## Increased resilience, improved efficiency

Darktrace has transformed the threat investigation process, allowing the security team to respond faster while avoiding time-consuming manual triage. Of the thousands of investigations Darktrace performs annually, the platform autonomously resolves approximately 95 percent of those incidents, often within seconds, escalating only 5% to analysts for further review.

By automating routine investigation and response, Darktrace has freed the team to focus on higher-value security work. Over a recent 10-month period, CCBN estimates the platform helped save more than 3,000 analyst hours that would otherwise have been spent reviewing alerts and chasing false positives.

With fewer email-driven disruptions, the impact extends beyond security operations. Teams across sales, operations, supply chain, and leadership remain productive while reducing exposure to account compromise, fraud, and business interruption.

## Different roles, different risks, different benefits

Bixby praises Darktrace’s ability to protect CCBN’s distributed workforce by adapting to different working styles and technology needs. “Users don’t have to change how they work,” he says. “No matter what someone’s role is, Darktrace helps minimize disruption and keep business moving.” For example, Darktrace enables:

- **Sales & Field Teams** to avoid account lockouts on the road, protect customer trust, and keep presentations and sell-ins moving.
- **Operations & Manufacturing** to reduce chances of downtime from a risky attachment or link.
- **Supply Chain & Logistics** to prevent shipment delays and partner disruption caused by hijacked vendor threads.
- **Corporate & Business Services** to lower exposure to payroll or invoicing fraud and data leaks.
- **Leadership** to minimize business interruption, brand/reputational risk, and regulatory headaches.



## Keeping people in the loop and staying proactive

“We’re in this together. AI is powerful, but it’s the combination of innovative tools, regular training, and human awareness that makes the difference.”

■ **Eric Bixby**

Director of Infrastructure and Security

Proud of the cybersecurity approach his team has built, Bixby declares, “We’re in this together. AI is powerful, but it’s the combination of innovative tools, regular training, and human awareness that makes the difference.”

Looking ahead, CCBN plans to continue reinforcing cyber awareness through quarterly training, internal communications, and introducing practical tools to help employees make better decisions in the flow of work. The goal is not only to respond to threats faster, but to proactively reduce risk across the organization as attackers continue to evolve.

Bixby and CCBN remain vigilant, realizing operational impact can begin with a single compromised message. In 2025, cyber incidents increasingly caused material operational and financial impacts across the sector, including one global beverage producer that experienced major disruptions to ordering and logistics, loss of sensitive data, and significant revenue loss due to a cyber-attack.

For CCBN, strengthening email security with innovative technology and ongoing education is a practical way to reduce the likelihood that one click will become a major business interruption.

“With the right tools, we are confident we can stay ahead and protected,” says Bixby. “But we never want people to assume technology means they can stop thinking. The best results will continue to come from partnership between people and AI.”



■ **About Darktrace**

Darktrace is a global leader in AI cybersecurity that keeps organizations ahead of the changing threat landscape every day. Founded in 2013 in Cambridge, UK, Darktrace provides the essential cybersecurity platform to protect organizations from unknown threats using AI that learns from each business in real-time. Darktrace’s platform and services are supported by 2,700+ employees who protect nearly 10,000 customers globally. To learn more, visit [www.darktrace.com](http://www.darktrace.com).