Customer Case Study

# Domino's Rolls Out Stronger Communications Security with Behavioral AI

## Abnormal is a key ingredient in the company's mission to deploy future-proof solutions for efficiency, security, and trust.

**Industry**
Retail & Hospitality

**Headquarters**
Ann Arbor, MI, USA

**Protected Mailboxes**
4,400+

The Domino's brand is synonymous with pizza worldwide, with locations in more than 90 countries serving more than a million customers per day. Growing from a single store in Ypsilanti, Michigan to the largest pizza company in the world, Domino's has put technology at the center of its business model. "We classify ourselves as a technology company that delivers pizza," said John Roeser, Senior Manager, Information Security.

### The Domino's Email Security Challenge

Domino's has a huge communications ecosystem to protect. In addition to Microsoft 365's security features, Domino's had a secure email gateway (SEG), but it didn't stop advanced spear phishing, BEC, and account takeover attacks.

A team of six security analysts was spending an outsized amount of their time investigating and responding to system and user-reported emails. "We were receiving 500 tickets a day regarding potentially malicious emails," said Jonas Turner, Manager of Engineering, Information Security. "We also had analysts educating executives and teams," Roeser said. However, new AI-generated attacks were exceeding the ability of even security analysts to spot them.

### Customer Key Challenges

- Reallocate security team time spent on email management to other projects.
- Stop advanced attacks that the legacy SEG couldn't catch.
- Manage human behavior by keeping threats and graymail out of inboxes.

### Abnormal Solution Impact

- 41 security analyst team hours saved per day on manual email investigations and remediation, enabling analysts to focus on other critical security needs.
- Secure communications with no false positives and fewer questionable emails delivered, resulting in more user trust in their inboxes.
- 488 hours of time savings across the organization in 30 days identified for graymail filtration.

"Human behavior has always been a big email security factor that attackers exploit. With Abnormal's behavioral AI keeping attacks out of end users mailboxes, human error risks are reduced and we're much more secure."

John Roeser
Senior Manager, Information Security

# Customer Case Study

**98%**
Reduction in user-reported malicious emails.

**488 hrs**
Potential companywide savings on graymail in 30 days.

**355%**
More BEC attacks detected and remediated compared to industry averages.

## The Abnormal Security Solution

The SEG didn't stop threats and it created work for the team. "Managing the SEG can be very time consuming, so we're always looking for ways to automate," Roeser said.

Turner heard about Abnormal from a colleague with the Information Systems Security Association (ISSA). Intrigued by Abnormal's API architecture and autonomous AI capabilities, Domino's requested a proof of concept. "The integration was fast and the POC could turn into production," Roeser said.

Equally important is Abnormal's ability to detect threats across platforms beyond and connected to email. "We have Teams and Slack and other SaaS applications, and the fact that Abnormal can protect those as well is something we are looking at closely," said CISO Andy Albrecht.

## Domino's Gains Time and Insights with Abnormal

"Abnormal's automation gives our analysts time back to work on other projects, and the fact that it's API-based gives us flexibility to tie in other applications and their data," Roeser said. By saving the security analyst team 41 hours per day on manual email investigations and remediation, Abnormal has enabled Roeser to pivot the analysts onto more critical security needs. He added that the data provided by Abnormal is helping the security team understand the business better.

Domino's may soon save more time with Abnormal. It's testing the Email Productivity module for graymail filtration, and Abnormal has identified 488 hours of potential time savings across the organization in 30 days. "A lot of graymail gets through our SEG, so I'm excited to see the amount of promotional email that will disappear from users' mailboxes when we roll it out," Turner said.

## A Behavior-Based Solution for Efficiency and Trust

Abnormal has also helped Domino's advance toward one of the CISO's long-held goals. "We want our people to trust what they're opening in their inboxes. The more trust people have, the faster they can go through their messages, and the more they can accomplish," Albrecht said.

That level of trust requires technology that lets people engage without putting data at risk. "Abnormal has really helped reduce the potential for compromises caused by human behavior," Turner said.

> "Abnormal's differentiator is its behavioral AI. Abnormal knows the company's normal patterns of emails, conversations, and business practices. Understanding human behavior through AI will allow our protection platforms to stay ahead of threats that target our organization."
>
> Andy Albrecht
> CISO

**Abnormal Products in use:**

- Inbound Email Security

abnormalsecurity.com →

Abnormal