DARKTRACE | BIOMERICS

Biomerics

0

Novel attacks have reached inboxes since deployment

14+

Global facilities protected with unified AI email security

Biomerics partnered with Darktrace to stop sophisticated email threats that were evading traditional filters — protecting critical medical device manufacturing while giving the IT team time back to focus on strategic work.

The defender: Playing whack-a-mole with high stakes

Joshua Wilson is a cybersecurity defender on the front lines. As IT Operations Manager at Biomerics — a medical device manufacturer with 14+ facilities and 3,200 employees — he protects manufacturing operations where production downtime can cost millions. "When we get production down, the potential is for not just hundreds of thousands, but potentially millions [in losses], depending on the outage," explains Wilson.

Wilson's team built a layered defense strategy, including endpoint protection, network scanners, Microsoft security tools, and email filters. But he describes the job as "a really nasty game of whack-a-mole." Once they locked down one area, threats emerged somewhere else. Email remained the persistent weak spot — and the problem wasn't volume, it was sophistication.

Business email compromise attacks targeting vendor relationships were slipping through. The attacks worked like this: A trusted partner's account gets compromised. The attacker reads past conversations, understands the relationship, then inserts convincing requests that pass all authentication checks — like suddenly asking to change banking information in what looks like a normal conversation. Traditional filters checking SPF, DKIM, and DMARC couldn't catch these threats because they looked legitimate on the surface.

"There have been times where we've actually seen our partner companies become compromised," Wilson says. "It's a legitimate company emailing us that we work with, but it's a bad actor on their side."

> "Darktrace learns how we normally communicate and flags deviations in real time — shifting us from reactionary defense to proactive protection."
>
> ■ **Josh Wilson**
> IT Operations Manager, Biomerics

For Biomerics, these attacks posed two critical risks. Fraudulent banking changes could drain hundreds of thousands of dollars before detection. Worse, if malware entered through a trusted vendor email, it could spread across manufacturing systems, triggering the million-dollar production shutdowns. Meanwhile, Wilson's small team was stuck chasing down these incidents — investigating, alerting partners, patching gaps — instead of strengthening defenses.

"When you read the email, it's very clear that there's something wrong here. But no amount of fine tuning on our email filters would catch those," Wilson explained. The attacks he describes as "they did a really good job here" kept getting through.

How Darktrace changed the equation

Wilson represents the cybersecurity defenders Darktrace builds for — those who should be championed for blocking novel threats before they become breaches. He needed a solution that could spot subtle behavioral changes signaling a compromised account, even when technical indicators looked normal.

With a background in machine learning —- "I did research with my professors on applying machine learning to logic games" — Wilson was skeptical of AI hype. "AI means very little to me," he admits. "I have to understand what it's actually doing on the back end."

What convinced him was how Darktrace's Self-Learning AI works. Instead of relying on known threat signatures, it learns normal communication patterns for Biomerics and its user. When something deviates, like a vendor suddenly requesting banking changes in a conversation that typically discusses product specifications, Darktrace flags it in real time.

During the proof of value, Wilson tested the accuracy himself. "You guys have your anomaly score. You're telling me directly from baseline, this is how far off we think this is," he notes. "Every time I saw a 100, I would review it [and say] 'yep, this is not what we want.'"

The consistent accuracy gave him confidence the AI was genuinely learning Biomerics' communication patterns, not generating false positives.

> "The Darktrace approach, as opposed to these other systems, is it wasn't just looking for what I'd call your key indicators. While the system will take that into account, it's also just looking at the contents of the email."
>
> **Josh Wilson**
> IT Operations Manager, Biomerics

The results: Stopping threats and gaining time back

Since deploying Darktrace / EMAIL™, Biomerics has seen dramatic changes:

Stopping sophisticated attacks: The novel phishing and business email compromise attempts have been nearly nonexistent. "We're not seeing those now," Wilson says. "And that has been a breath of fresh air."

Containing security events: When incidents do occur, they're isolated fast — affecting one to three users instead of spreading across the company.

Freeing the team for strategic work: Wilson's team is no longer stuck in reactive mode. "Talking about that whack-a-mole game, we've really hammered down one of those holes," he says. "It gives me some availability to go tighten things up in another place."

Productivity gains beyond security: Darktrace filters out more noise than previous solutions, reducing the time employees spend sorting legitimate emails from threats. The team can focus on their actual work, not email triage.

Reducing alert fatigue: Wilson's external communications have changed too. He used to be the one calling partner companies to warn them about compromises. "I'm not seeing stuff coming through," he says. "I'm not the red canary saying you might have a problem anymore...my problem is making sure my company is safe. And this tool is doing that job for us."

The layered defense Wilson built now works as designed — each layer reinforcing the others, not compensating for email's gaps. Darktrace / EMAIL™ is part of the Darktrace ActiveAI Security Platform™, which extends the same Self-Learning AI approach across network, cloud, endpoint, identity, and OT security.

A strong foundation for the future

For a medical device manufacturer operating under strict ISO 27001 and FDA compliance frameworks, the shift from reactive to proactive is essential. The ability to contain threats before they impact production lines protects not just revenue, but the healthcare supply chain that depends on Biomerics.

Wilson sums up the transformation: "The Darktrace approach is, we're going to see how you normally talk to people, we're going to establish a baseline for you, and when things go away from that, that's when we're going to raise the red flag. That's the difference for us...it's not reactionary, it's proactive."

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.