Allegheny Millwork

Case Study

Allegheny Millwork & LUMBER

Challenges

- An increase in malicious employee impersonation emails
- Industrial devices that expand the attack surface
- Phishing threats coming from supply chain vendors

Solution

- AI-powered anti-phishing capabilities through the IRONSCALES platform
- Regular phishing simulations and email security educational campaigns

Results (Weekly)

- 91,428 emails remediated (deleted, moved to the spam folder, or flagged with an inline message)
- 10,813 resolved incidents, 8,631 of these being phishing
- 5709 hours of remediation time saved

About Allegheny Millwork

Allegheny Millwork is a leader in the custom millwork industry, providing clients with the highest quality manufacturing and construction services for over 40 years. The Allegheny Millwork group comprises four companies, spanning eight locations and employing around 300 professionals across the US. The organization's projects are solely commercial, predominantly providing design, engineering, and installation services to high-end hotels, casinos, museums, and resorts nationwide.

The Problem

Email is one of the biggest vectors for cyber-attacks; 94% of all security incidents with malware occur through the use of malicious emails, and phishing attacks are increasing year on year. Allegheny Millwork's risk of attack is exacerbated by its production facilities' use of robotic equipment and Industrial Internet of Things (IIoT) devices, which streamline maintenance, quality control, and inventory management. This larger attack surface makes systems a perfect target for hackers, who can use phishing emails to gain remote control of industrial systems.

The organization was also at risk of being affected by phishing attacks from trusted partners up and down the supply chain. With a large network of smaller vendors, Allegheny Millwork needed a way to effectively identify malicious emails, even when they were coming from a trusted external source. And with a small team heading up security across all four of its companies, phishing detection and remediation was becoming an overwhelming task.

After receiving multiple phishing attempts targeting the company, including employee impersonation emails, the Allegheny Millwork security team felt that getting a handle on email security was a top priority.

> " A lot of our vendors are much smaller companies, so many of them don't have a dedicated IT department. Just yesterday a vendor's account was breached and they were sending us phishing emails. Luckily IRONSCALES caught them."
>
> MIKE SHORTS, IT MANAGER AT ALLEGHENY MILLWORK

Solution

The team at Allegheny Millwork was looking for a three-pronged approach to email security: a solution that could identify malicious emails, remediate incidents, and educate users on what an attack looks like. When researching solutions, IRONSCALES was the only platform that provided all three of these crucial factors at a competitive price.

Allegheny Millwork's security staff were so impressed with IRONSCALES' capabilities that they decided to install the full solution immediately after a demo in June 2019. The installation was quick and seamless, rolling out the solution to 256 users across the four companies with just one click.

"When we were installing IRONSCALES, I logged into the portal, synced it with my Office 365, and it just brought all the emails over straight away. It was beyond easy." said Mike Shorts, IT Manager at Allegheny Millwork

Outcomes

Since installing IRONSCALES the Allegheny Millwork team has seen a drastic reduction in phishing and spam emails hitting user inboxes. This, in turn, has had a positive effect on employee productivity, with staff able to work more efficiently without having to deal with junk and malicious emails. In the three years since implementation, IRONSCALES has used AI to automatically remediate over 90,000 emails and resolve over 10,000 email incidents, 8,000 of which were phishing attacks. This equates to over 5,000 hours of remediation time saved for the internal security team, who now use this time for other critical department activities. For a small security team like Allegheny Millwork's, taking the responsibility of remediation away from the human team has afforded them greater peace of mind.

"As the Head of IT, it's a weight off my shoulders to have that support with detection and remediation. My first month at Allegheny Millwork was pretty nerve-wracking given the number of malicious emails we were receiving. I definitely started sleeping better at night when I brought IRONSCALES on board." said Mike Shorts, IT Manager at Allegheny Millwork

In addition to their simple-to-navigate dashboard, IRONSCALES provides a mobile app for remediation on the go. The flexibility offered by the mobile app has been invaluable to the team, giving them greater control over the organization's email security, no matter where they're working from.

> "When I first came on board three years ago and saw the number of phishing emails we were receiving, I knew that getting a handle on email security was my priority. You can't fool a computer, but you can fool a person."

MIKE SHORTS, IT MANAGER AT ALLEGHENY MILLWORK

As well as securing user inboxes, Allegheny Millwork is taking advantage of IRONSCALES' integrated phishing simulation and training tools. Sending out a phishing simulation once a month, the security team has noted a marked improvement in overall user awareness and knowledge. And by altering the style of their simulations each time the team can keep users on their toes when it comes to the latest techniques and industry trends. Three years on, the Allegheny Millwork team feels that the monthly training has started long-term, positive conversations between staff about phishing, creating stronger email security that's become a part of the company's culture.

Looking Ahead

After using the IRONSCALES solution for three years, and adopting new features as the platform evolves, Allegheny Millwork is looking to further tailor its phishing simulations to different departments. With four separate companies within their employee base, there are more opportunities to personalize phishing simulations to each company and the departments within them. And after a recent increase in malicious emails spoofing HR and Accounting employees, the team is looking to focus training on these specific areas.

About IRONSCALES

Every day criminals launch billions of new phishing attacks. No company is immune. Legacy solutions can't keep up & cloud providers struggle to stop advanced attacks with native controls. IRONSCALES' powerfully simple email security solution helps you fight back fast and keeps your company safe in today's cloud-first world.

Incubated inside the world's top venture program for cybersecurity and founded by alumni of the Israeli Defense Forces' elite Intelligence Technology unit, we offer security professionals an AI-driven, self-learning email security platform that provides a comprehensive solution to proactively fight phishing attacks.

To learn more about IRONSCALES' award-winning anti-phishing solution, please sign up for a demo today at Ironscales.com/get-a-demo/

> " I'm happy to recommend IRONSCALES to others, in fact, our sister company recently onboarded the solution based on my recommendation. If a company is looking for an anti-phishing or user training solution, IRONSCALES is definitely the way to go. I have no complaints!"

MIKE SHORTS, IT MANAGER
AT ALLEGHENY MILLWORK

---

www.srccybersolutions.com   +91 120 232 0960 / 1   sales@srccybersolutions.com

ABOUT SRC CYBER SOLUTIONS LLP

At SRC Cyber Solutions LLP, we provide Next Generation, Automated and User-Friendly solutions in partnership with AUTOMOX for Patch and Endpoint Management, IRONSCALES for Comprehensive Email Security and Anti-Phishing Protection, THREATX for WAAP (WAF++) with an Attack-Centric approach for Web Application and API protection and Project Ares for Online Gamified Simulation-based Cyber Security Training.

Learn how working with IRONSCALES makes us Safer Together. www.ironscales.com

Everything is just a click away, from initial installation to threat identification and removal.