



INDUSTRY

Industrial Goods, Industrial Electronics

PRODUCT

Area 1 Horizon Enterprise

SECURITY ISSUE

Phishing

CHALLENGE

Protect AVX from phishing threats company-wide

RESULTS

Area 1 scans AVX's inbound email to stop email-based phish, and integrates with their DNS servers to block web-based phishing campaigns.

- Over 1,000 phishing emails blocked per week
- Global reduction of cyber security risk
- Increased management confidence that inboxes are secure

CUSTOMER STORY

## Leader in electronic components manufacture turns to Area 1 Security to reduce global cyber security risk

BACKGROUND

Throughout the past 50 years, AVX Corporation has innovated, developed, manufactured, and supplied critical components and solutions for the global automotive, industrial, medical, military, consumer electronics, communications, and transportation markets, building a successful business with over \$1.5 billion annual revenue. Its vast suite of offerings includes capacitors, inductors, filters, resistors, couplers, diodes, and circuit protection devices, along with sophisticated sensor, control, interconnect, and antenna solutions. The company's sophisticated infrastructure comprises 29 research, design, manufacturing, and customer support facilities in 16 countries.

Customers look to AVX to deliver competitive advantages in a global marketplace. That means developing key delivery and production capabilities for go-to-market campaigns, optimized for each customer's unique requirements and business needs. For example, AVX makes new safety and control devices for automobiles; lifesaving treatment, imaging, and diagnostic devices for healthcare entities; and next-generation IT components for smartphones, networks, and data centers. AVX also drives the development of green energy solutions to preserve and protect the environment. This company's forefront thinking and creativity yield numerous patents for groundbreaking advances, making AVX a leading contributor to progress in this new century.

## CHALLENGE

AVX relies on its IT networks and systems, the cloud, and the Internet to process, transmit, and store operational and financial information, manage business processes, and support regulatory and tax compliance. The company's IT infrastructure is foundational to marketing and sales initiatives and integral for communicating with employees, customers, and suppliers worldwide.

Like other enterprises, AVX faces a growing menace from cybercriminals and state threat actors determined to nullify security and steal or corrupt proprietary information, interrupt services, and harm company reputations. AVX recognized the need to revisit cybersecurity to reduce the risk of cyber breach by threat actors targeting not only the company itself, but its customers, contractors, and suppliers.

The AVX IT infrastructure is globally distributed across many sites that use diverse, and in some cases aging technology to support the business, complicating cybersecurity. One successful breach anywhere on the network could quickly spread enterprise-wide, leading to unauthorized disclosure of confidential information and loss

or damage of intellectual property. This could hurt the company's reputation and brand for years to come.

To reduce the risk of a cyber breach, AVX formulated a goal to build a robust global cybersecurity program. With the challenge to build the program from the ground up, Global Head of Cybersecurity & Privacy, Zack Moody, sought a new, more intelligent approach to protect AVX from cyber threats company-wide.

**The team recognized that phishing attacks are the primary cause of cybersecurity breaches, and therefore placed anti-phishing as a top priority to reduce risk.**

AVX was currently using G Suite to provide company-wide office productivity applications, including email, relying totally on G Suite's security features to protect itself from email phishing attacks. Fortifying G Suite security not only defends against phishing attacks, but also helps to achieve the goal of reducing cybersecurity risk globally.

## SOLUTION

The AVX cybersecurity team reached out to a number of well-established vendors, including Proofpoint and Agari, but they were most impressed by Area 1 Security's anti-phishing protection capabilities. AVX appreciated Area 1's deep roots in the NSA, along with its sophisticated methodology for preemptively detecting and stopping threats and monitoring new domains.

**In an initial 30-day proof-of-value trial, AVX was convinced that Area 1 offered the most comprehensive, innovative, and effective anti-phishing strategy.**

The trial uncovered nearly 600 suspicious and malicious phishing emails that evaded existing Gmail defenses. Those attacks included emails with malicious attachments containing ransomware, emails with links to credential harvesting sites, and imposter emails trying to trick employees into responding to fraudulent executive requests. Any of these threats, if

clicked on by an employee, could result in a catastrophic cyber breach.

Area 1 offered AVX unique visibility in locating targeted attacks, as well as providing a rich API for manipulating data, enabling reporting and investigation, and easing integration with SIEM, EPP, and other security orchestration tools.

**“Additionally, Area 1’s team offered superior responsiveness and expertise in helping to investigate and deep-dive attacks to an unprecedented granular level.”**

All in all, Area 1's proactive threat hunting, coupled with superior expertise in detecting and disabling threats were AVX's key considerations in making its choice. Area 1 also offered unrivaled ease of implementation—needing only a 15-minute call to configure and test email flow.



## RESULTS

Area 1 Security is now scanning AVX's inbound email continuously to detect and block phishing attacks. In addition to protecting email, Area 1's recursive DNS feature is deployed globally with AVX's Windows DNS servers to block employee access to phishing sites and domains, further reducing cybersecurity risk from social and browser-based phishing attacks.

Today, AVX is better protected from cyber breaches than at any time in its history. Area 1's technology continuously crawls the entire web in a Google-like model to identify and deliver proactive early warning and defense from phishing attacks. This comprehensive approach delivers incalculable value in protecting AVX from the havoc of a successful phishing campaign.

**With Area 1, the AVX cybersecurity team now vigilantly monitors and reports on the number and type of threats caught and blocked company-wide, giving management critical insight and confidence that email inboxes are secure.**

**Over a recent three-month period, the Area 1 service scanned over 7.8 million emails for AVX and detected more than 12,000 phishing emails.**

That's over 1,000 phishing emails blocked from employee inboxes per week. Not only has this prevented damaging cyber breaches, it has also reduced the need for the cybersecurity team to spend time investigating and remediating incidents; the team is now free to support more new business initiatives.

**“With Area 1, AVX achieved its major objective of minimizing cybersecurity risk. The cybersecurity team now provides updates to executive management demonstrating how well they're protecting the organization by sharing the number of threats blocked and delivering ROI for security spend each quarter.”**

Next steps include integration of AVX's Splunk instance with the Area 1 service. This will help the team correlate security information organization-wide to visualize and analyze malicious activity and more efficiently investigate and respond to an incident.

AVX feels that they have gained a crucial partner in Area 1, proven by their recent renewal of the relationship for three more years.

---

## **ABOUT AREA 1 SECURITY**

The industry's most comprehensive anti-phishing solution, Area 1 Horizon identifies threat campaigns, attacker infrastructure, and delivery mechanisms to give an advance warning to stop targeted phishing attacks during the earliest stages of an attack cycle.

Backed by top tier investors, Area 1 Security is led by security and data analytics experts coming from NSA, USCYBERCOM, Cisco/IronPort, and FireEye who realized a pressing need for a proactive solution to targeted phishing attacks. Area 1 Security works with some of the most sophisticated organizations in the world, including F500 banks, insurance companies, and health care providers, to preempt and stop targeted phishing attacks at the outset, improve their cybersecurity posture, and change outcomes.

- ▶ **Learn more and get in touch with us for a free preview:**  
**INFO@AREA1SECURITY.COM**