# CS BBLS:
# Sender Domain Monitoring

October 18h, 2024

# Agenda

- Overview
- Demo
- Product Comparisons
- Beta Insights
- What’s Next
- Resources Available
- Q & A

validity

# Overview

Email systems are increasingly the target of malicious actors.

They want to publicly demonstrate their intrusion,

commit cyber-vandalism,

or use trusted, authenticated systems

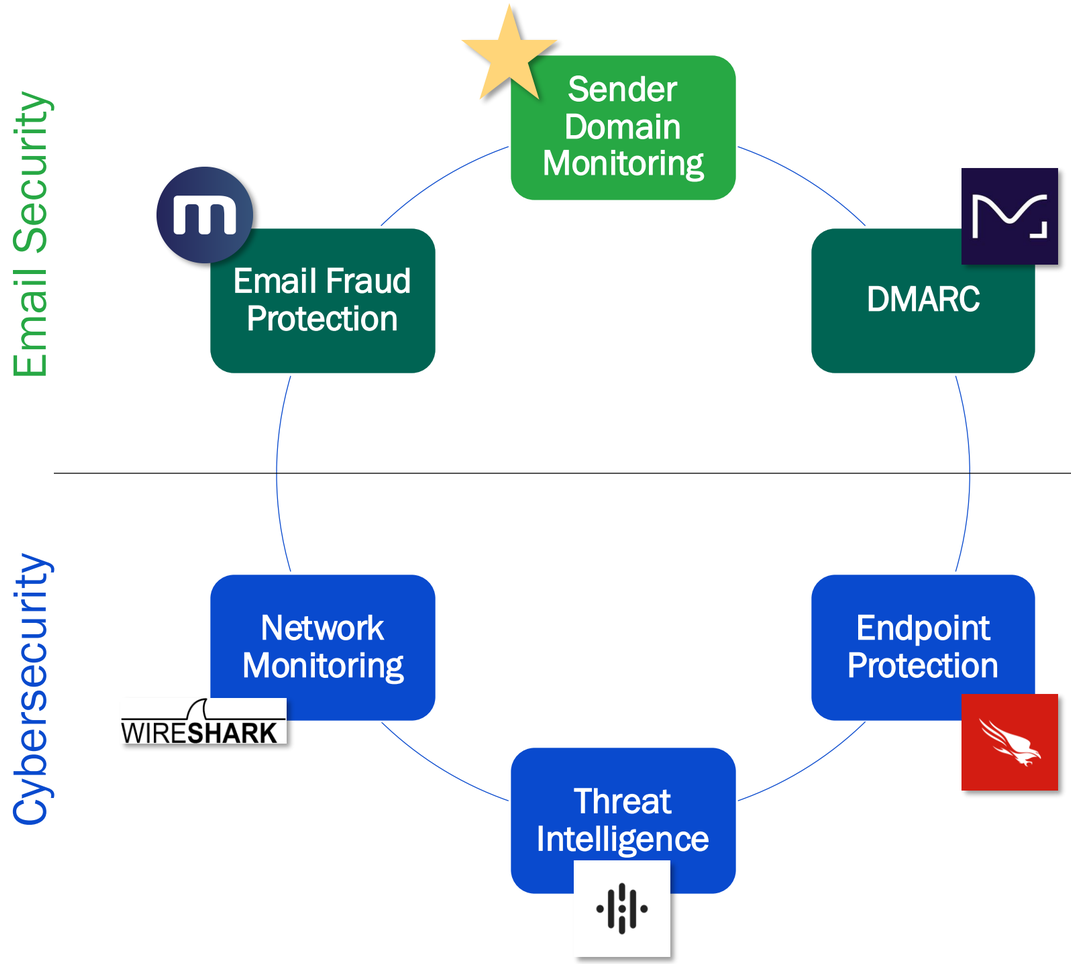
as a launching point for phishing attacks

and spreading malicious code.

Often the first sign of such a breach is people complaining on social media, or worse, it makes the news.

When malicious and abusive emails start going out, how do we spot this outside-the-firewall activity, and shut it down as quickly as possible?

# Email and Cybersecurity Landscape




**Email Security** falls into two buckets:

- Outbound Email Authentication (e.g. DMARC)
- Inbound Mail Protection (eg Mimecast)

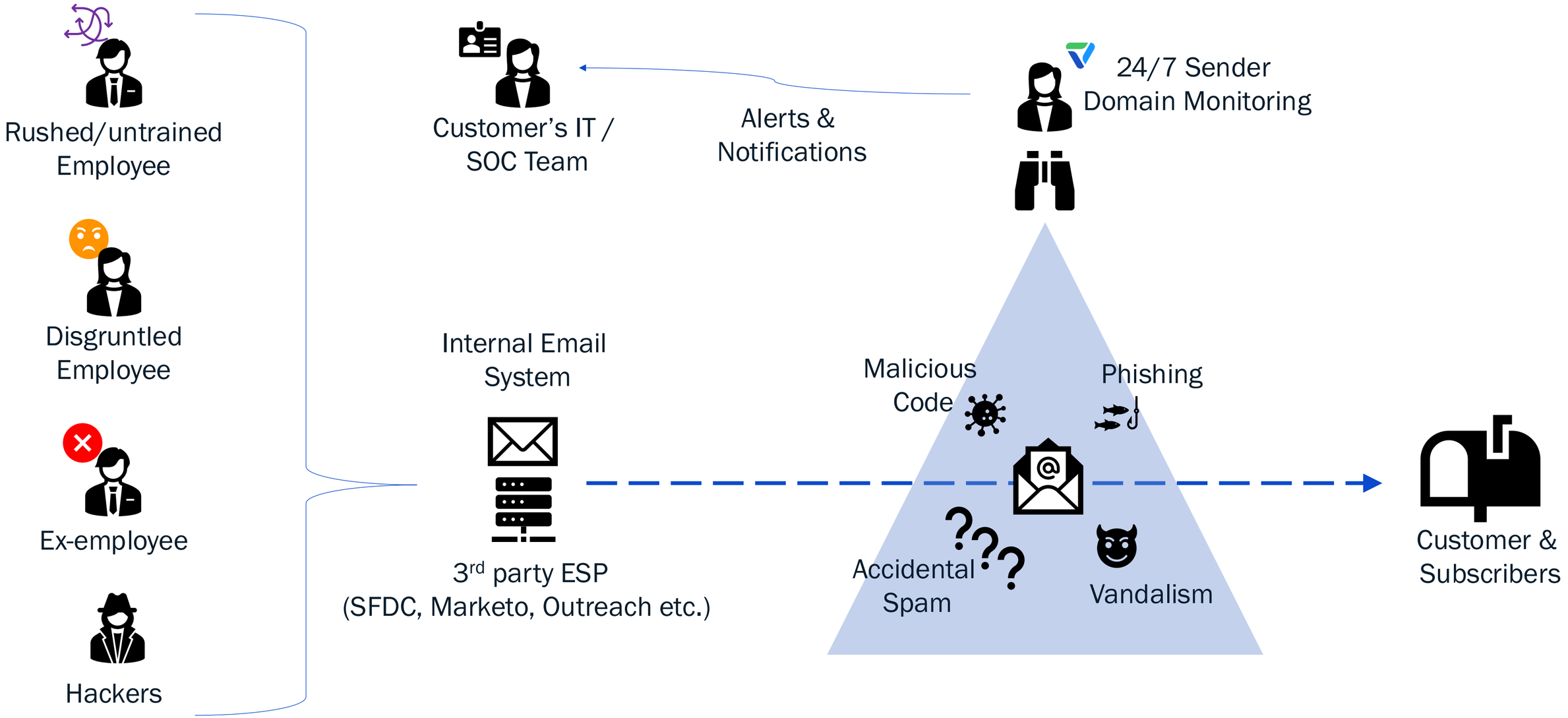
*… but neither of those tools can detect authentic mail being sent by a compromised system.*

**Cybersecurity** relies on a layered strategy:

- Educated humans
- Internal detection and monitoring
- Perimeter and endpoint intrusion prevention
- Aggregate industry alerts of malicious actor signatures

*… but today they cannot monitor external activity for indicators of compromised systems*

# Sender Domain Monitoring



# Who it’s for

Security/IT Professional – require advanced, multi-layered threat detection and response solutions to safeguard information systems

Email Marketers – require tools to identify phishing and spoofing attacks, improve deliverability, and maintain brand integrity.

# The Benefit:
# Case Study – Consumer Technology Provider

## Security Compromise – Bot Attack

### The Breach

- An attacker circumvented their bot detection systems.
- They created user accounts containing inappropriate material.
- These profiles followed each other and legitimate accounts.
- **Over 2,000 fake accounts were created.**
- **Over 1.5 million *unauthorized* emails were sent from their *authorized* IP.**

### The Response

- Validity's 24/7 monitoring team identified the compromise of the Customer's Certified IP
- **Validity immediately de-Certified their IP, automatically re-engaging mailbox providers' spam, phishing, and malware protections.**
- The Customer was provided sample emails and metadata to identify the affected accounts.

### The Outcome

- Customer disabled the bot accounts, preventing them triggering further emails.
- **New email sends were tested and evaluated, which met Validity's Certification requirements.**
- Validity re-Certified their IP, and customer resumed their normal email practices.

# The Benefit:
# Case Study – Event Ticketing Platform

## Security Compromise – Phishing

### The Breach

- An attacker circumvented their security protections.
- They accessed the email management system.
- They created an email about a fictional event and sent it out.
- **The email contained a phishing attack.**
- **~3,000 unauthorized emails were sent from *authorized* IP**

### The Response

- **Validity's 24/7 monitoring team identified the compromise of Customer's Certified IP within 5 min of the first email being sent.**
- Validity immediately de-Certified their IP, automatically re-engaging mailbox providers' spam, phishing, and malware protections.
- The customer was notified with examples of the phishing email.

### The Outcome

- Customer purged the intruder's changes to their event system.
- **New email sends were tested and evaluated, which met Validity's Certification requirements.**
- Validity re-Certified their IP.
- Customer added additional metadata to emails to further body to further authenticate email campaigns as legitimate.

validity

# Demo

validity

# Validity Product Comparison

# VS Other Common Solutions

- **VS Everest**
  - SDM leverages our Reputation Network complaint and trap feeds, and any threat is reviewed by a human prior to notifying the customer.
  - Everest uses our Domain Sensor Network (aka Threatwave & Mailbox Park) and suspicious activity is not reviewed by a human.
- **VS Sender Cert**
  - SDM provides compromise detection and identification via suspicious email activity originating from a specific domain and all the IPs sending from that domain, including shared and dedicated IPs.
  - SC that only detects activity on dedicated IPs.
- **VS DMARC authentication tools (e.g. Valimail)**
  - These tools protect you from malicious actors hijacking your domain, making it appear as if their emails are coming from your brand. They provide no benefit if your systems are compromised – your systems will send out emails that DMARC will believe are authentic.
- **VS other cybersecurity technology**
  - Does not provide compromise detection and identification through monitoring outbound email activity.
- **VS inbound, anti-spam, and email filtering technologies (e.g. Mimecast)**
  - These tools protect you against inbound email threats and cannot detect internal compromised or misused systems sending outbound emails.

validity

# Beta Program Insights

# Beta Timeline

| | |
|---|---|
| September 10-16th | **Closed Beta Program Awareness** |
| September 18th | **Closed Beta Applications Close** |
| September 23rd | **Closed Beta Program Starts**<br>**Help Center Articles Live** |
| **October 11th** | **Follow-up Email w/Survey** |
| **October 23rd** | **Closed Beta Program Ends** |

validity

# Beta Participants

59 applications received

- ClickDimensions
- Robly Digital Marketing
- Frontdoor, Inc.
- Experiom
- ICF Technology
- Lululemon USA, Inc.
- Happily Family
- Human Rights Campaign
- Origin Energy
- Multi-View, Inc.
- Generic Publications Pty Ltd
- Zoho Corporation Private Limited
- Qualtrics LLC
- The Access Group
- Sanofi Aventis Group
- Tide Platform Ltd.
- Amgen U.S.A. Inc.
- 1440 Daily Digest
- Windstream
- National Collegiate Scouting Association LLC
- Morris Printing Group, Inc.
- Zuri Group
- HR Acuity
- Uplight
- Constant Contact
- Virgin Atlantic Airways Ltd
- Cox Communications Inc
- Open Text Corporation
- Feeding America National Organization
- General Mills
- Saint Leo University
- HelloFresh SE
- J.Jill, Inc.
- Renault SAS
- Loews Hotels & Resorts
- LPL Financial

validity

# Participant Feedback

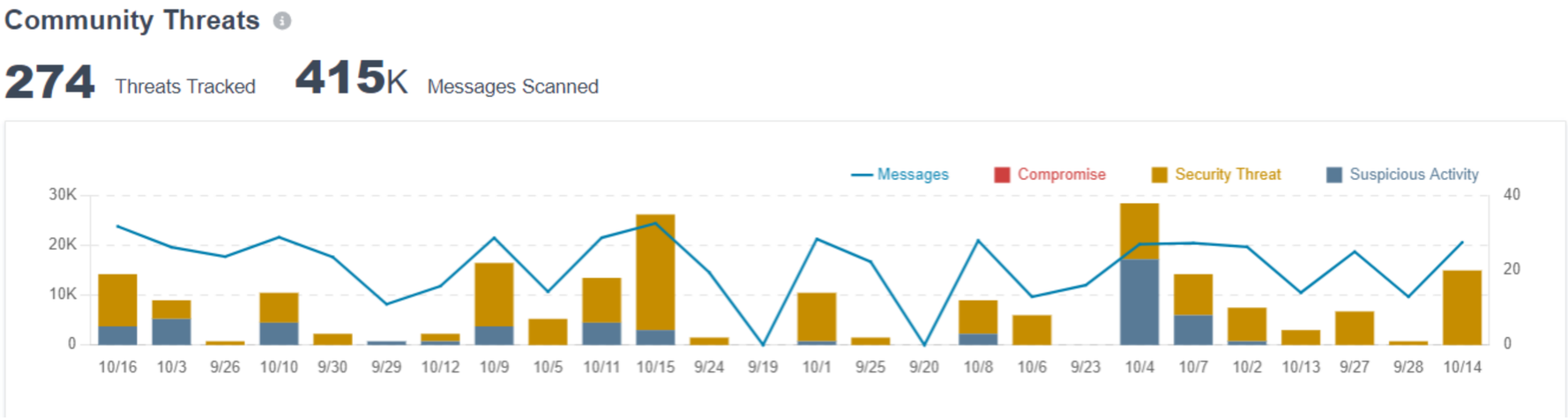
“After signing up, I **didn't receive any info on what to expect** from Sender Domain Monitoring, or more details on the info it would provide. A training video would have been helpful. **Finding Knowledge articles wasn't user friendly** as it was only available via a small "i" icon next to 'Community Threats’.”

“If we had issues show up on some of our domains, I would have gotten more out of the service. “

“I don’t understand what the product does or how to use it to gain insights.”

“It’s hard to see any value in this product over monitoring we get in Everest.”

# Quantitative Feedback



validity

# What's Next

# Extending the beta!

# Improve Customer Experience & Value

01

Curating a more effective onboarding experience

02

Incorporating contextual insights into the dashboard AND real-time alerts

03

Expanding message feeds to increase coverage

04

Implementing additional checks to detect more threats

validity

# Open Beta

# Reasons to Enroll

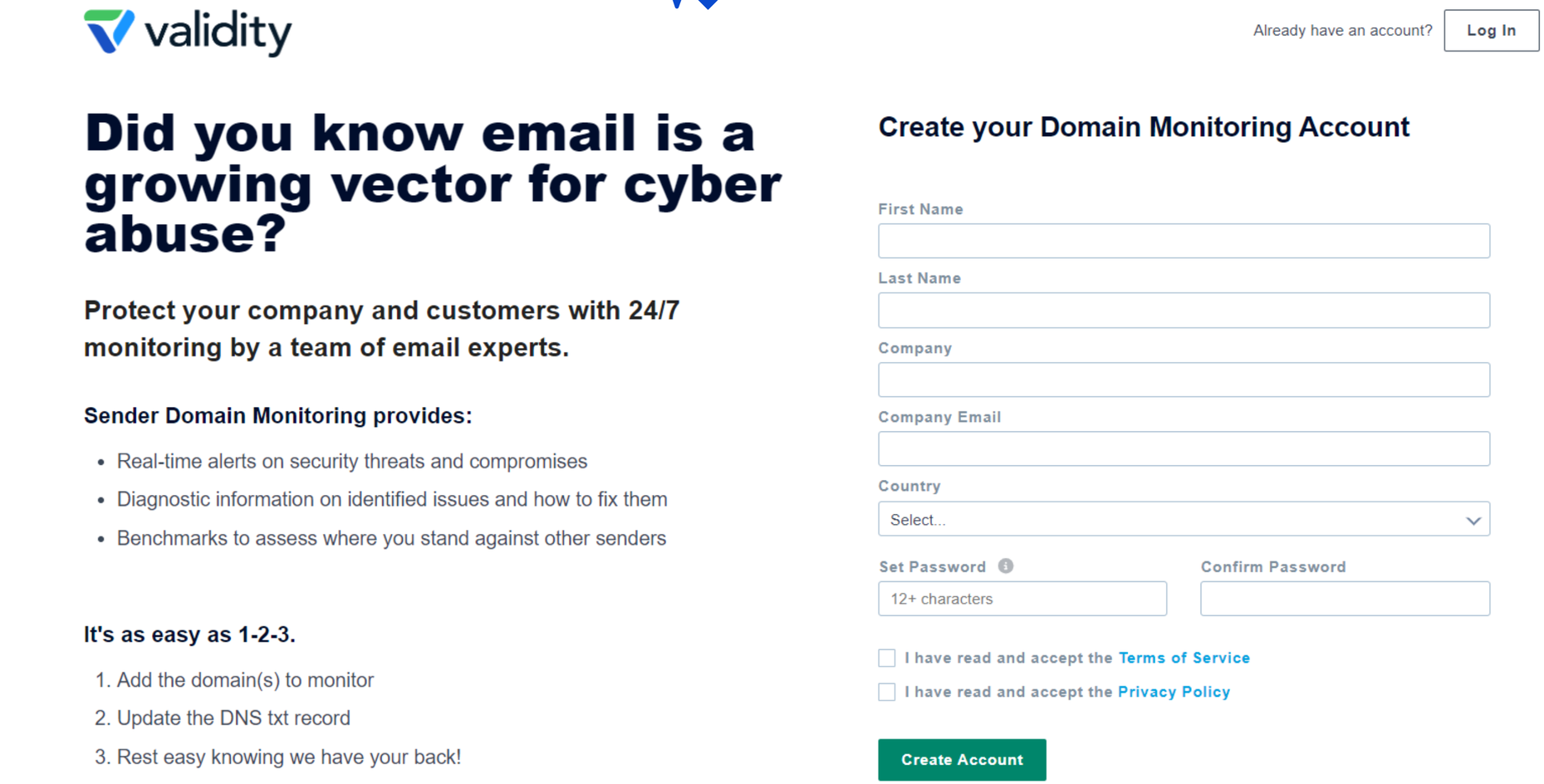
1. **Early Access:** Be the first to experience new features and get the benefits before anyone else.
2. **Enhanced Security:** Enjoy peace of mind knowing that your sending domains and IPs are protected from potential threats with 24/7 monitoring by our team of expert analysts. Timely, accurate, and actionable notifications are delivered in near real time via email, Slack, or Teams ensuring you can detect and respond to any suspicious activity as it happens.
3. **Direct Influence:** Your feedback directly shapes the development of the tool, making sure it fits your purposes and requirements.

# Requirements

- Ability to update DNS record on the domain(s) you wish to monitor.
- Willingness to provide detailed feedback.

# How

my.validity.com/monitoring/sign-up



# Timing

## October

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 |
| 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 27 | 28 | 29 | 30 | 31 | | |

## November

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |

## December

| S | M | T | W | T | F | S |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | 9 | 10 | 11 | 12 | 13 | 14 |
| 15 | 16 | 17 | 18 | 19 | 20 | 21 |
| 22 | 23 | 24 | 25 | 26 | 27 | 28 |
| 29 | 30 | 31 | | | | |

validity

# Resources

# Sender Domain Monitoring Resources

**Help Center Articles**

- What is Sender Domain Monitoring?
- Managing Domains
- Notifications

**FAQs**

- Talking Points (In Sales Enablement SharePoint)

**COMING SOON!**

- Product page
- Infographic
- ”First Look” introduction content from the SANS Institute, a cybersecurity thought leader.
- Persona documentation
- 3 Pillars documentation

validity

# Q&A