ChannelPro

Time is Money:

How Proofpoint Makes Cybersecurity Easy, Efficient and Effective for MSPs

Presented by:

proofpoint®

pax8

Meet the Panelists

Joe Sykora

SVP, Worldwide Channels and Partner Sales

Proofpoint

Ryan Walsh

Chief Operating Officer

Pax8

Paul Jakobsen

Sr. Manager, Essentials Strategic Partners

Proofpoint

Randy Scadden

Sr. Global Sales Engineer

Proofpoint

Why is email security relevant?

The Rise of Ransomware

Ransomware hackers demand $70m after attack on US software firm Kaseya

Between 800 and 1,500 businesses around the world, including supermarkets and dentists' offices, affected by attack


THE WALL STREET JOURNAL.

Home World U.S. Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ

BUSINESS

Beyond Colonial Pipeline, Ransomware Cyberattacks Are a Growing Threat

Schools, hospitals, companies are targeted by 'cyber weapons of mass destruction'

Video: Long Lines at Gas Stations Amid Pipeline Shutdown

Long lines formed at gas stations along the East Coast on Tuesday, as drivers made a run on gasoline amid fears of shortages due to the shutdown of the U.S.'s largest fuel pipeline following a cyberattack. Photo: Robin Rayne/ZUMA

By Robert McMillan, Dustin Volz and Tawnell D. Hobbs

May 11, 2021 12:14 pm ET

PRINT TEXT

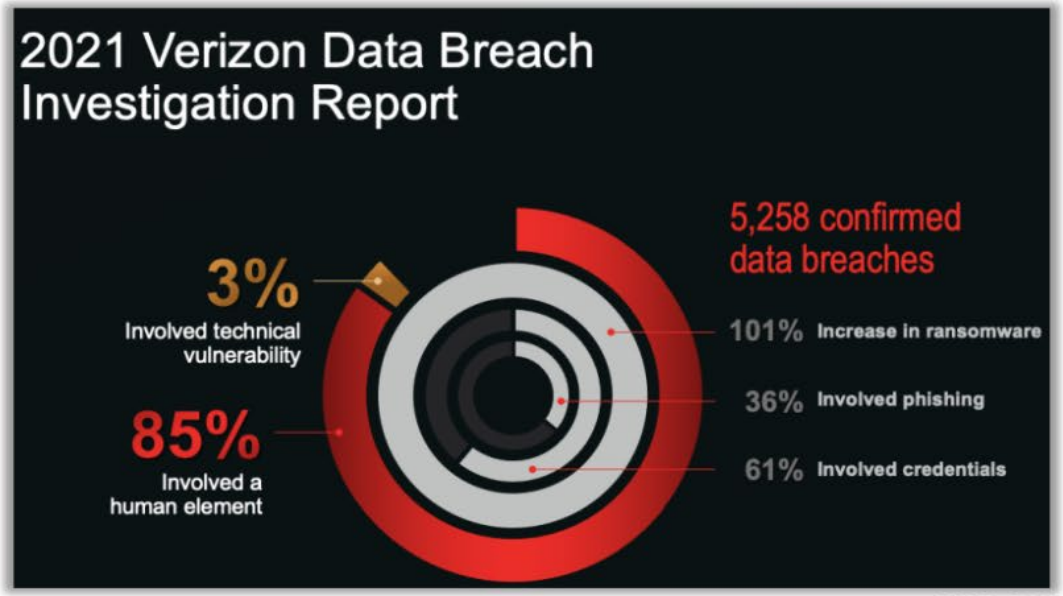
The cyberattack that knocked offline an essential U.S. gasoline pipeline shows how the dangerous, professional-scale hack-for-ransom threat is spreading rapidly, targeting companies, schools, hospitals and other institutions.

UPCOMING EVENTS


The New York Times

F.B.I. Director Compares Danger of Ransomware to 9/11 Terror Threat

The Biden administration is taking steps to counter the growing threat of cyberattacks on U.S. businesses, and encouraging companies to do more to protect themselves.



The accidental impact of cloud

proofpoint.

Your clients never signed up for this

The accidental impact of cloud

proofpoint.

Email is **#1 threat vector**

90+%

attacks are email-based

Attack campaigns resulted in a **successful compromise**

In finance

20%

In healthcare

40%

Office 365

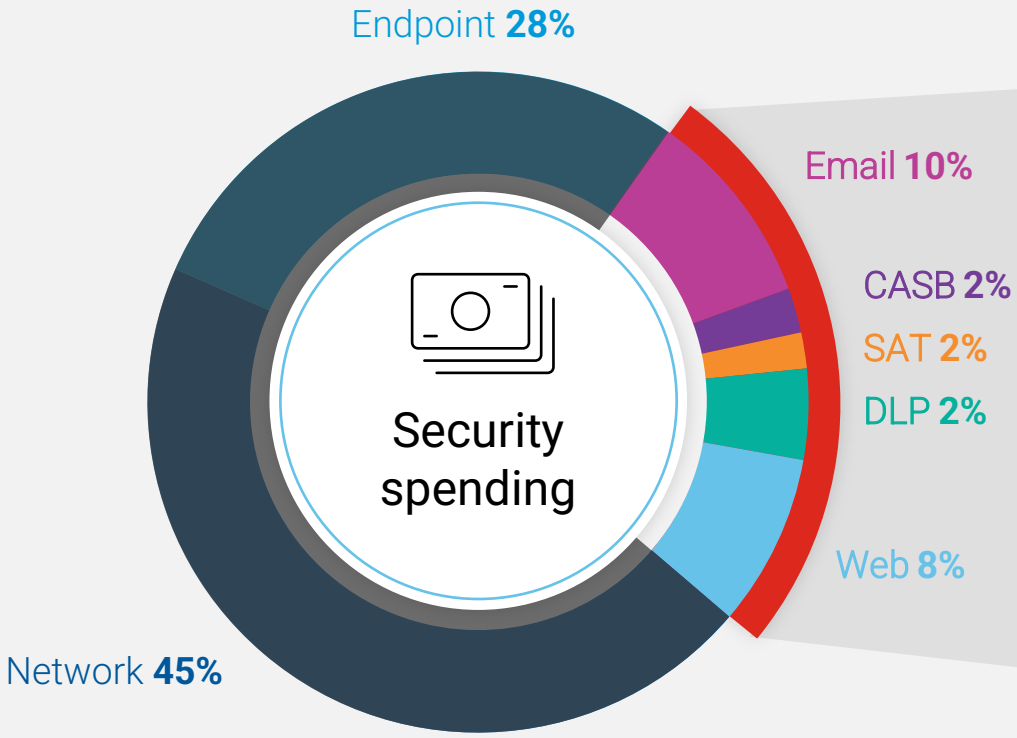
59M+

malicious messages targeted at Proofpoint customers sent or hosted by Microsoft Office 365 in 2020

proofpoint.

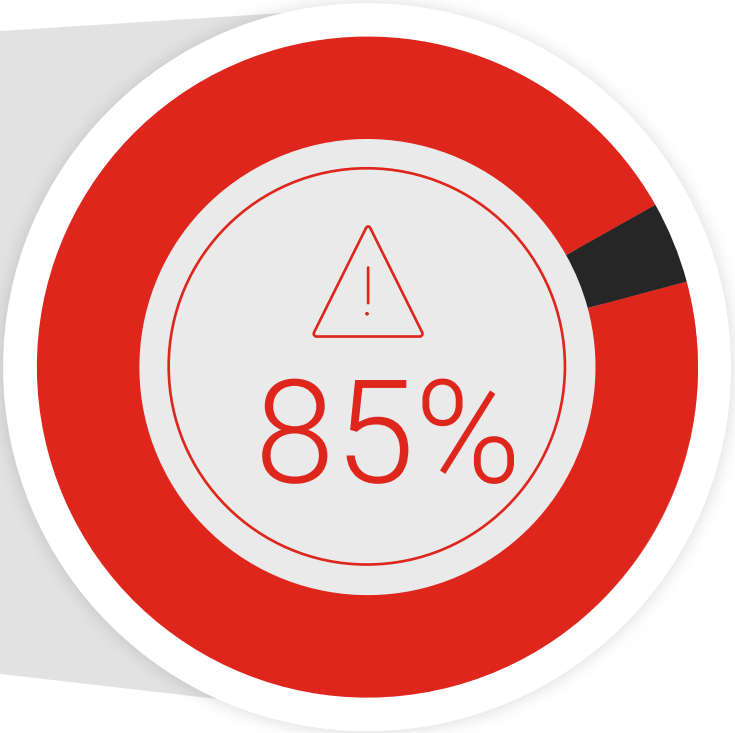
Attackers focused on people, but most defenders didn't

proofpoint.



Source: Gartner Information Security, Worldwide 2019–2025, 4Q 2020 update (2021 forecast)

BREACHES



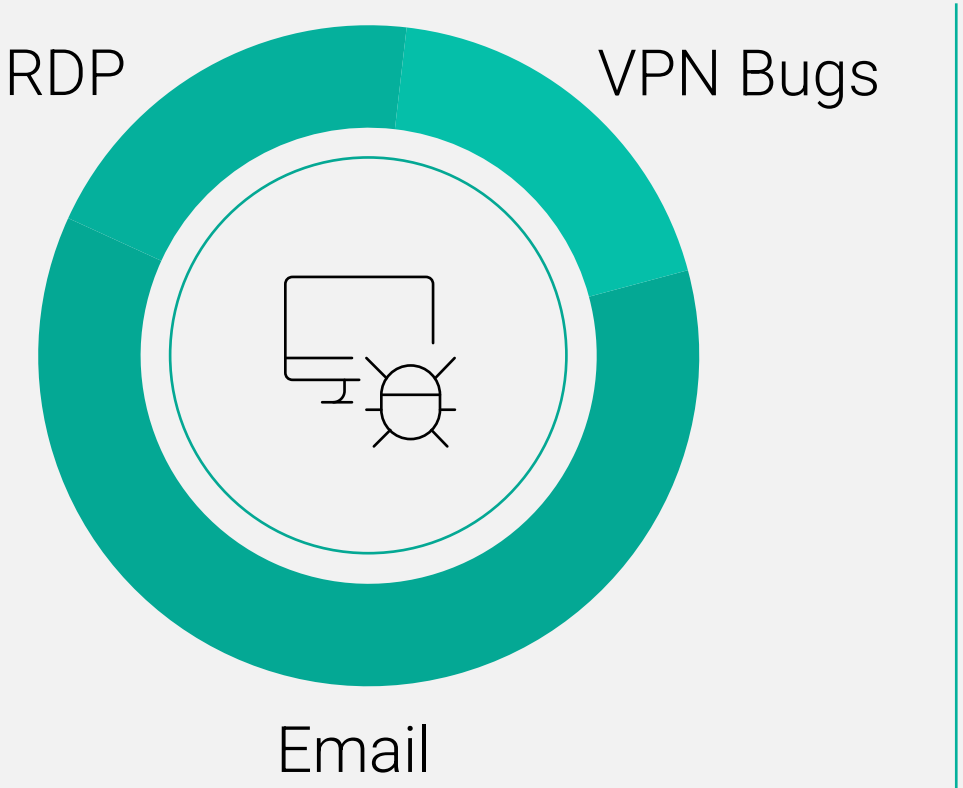
of breaches start with attacks targeting people, human error, or insiders

Source: 2021 Verizon DBIR

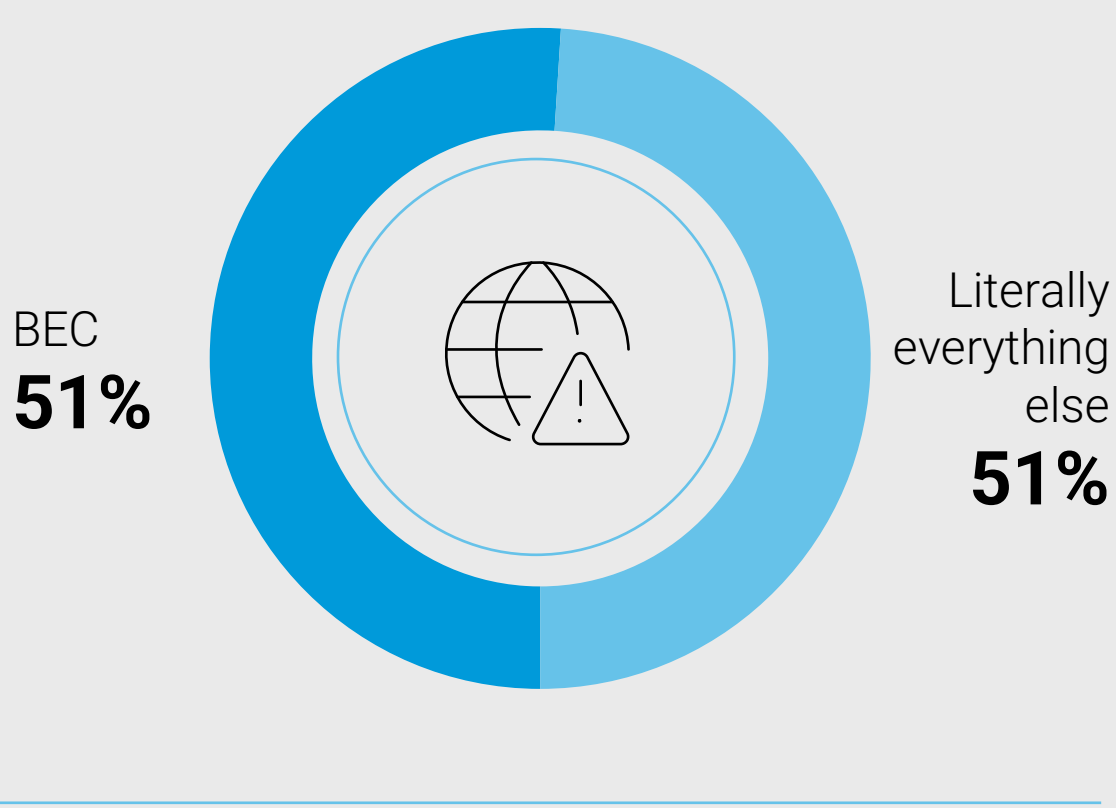
The scale of threat & loss is unprecedented

proofpoint.

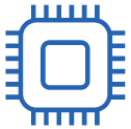
Ransomware initial access



Cybercrime Losses



Losses can be significant, especially SMBs

Threats now use social engineering, not vulnerabilities[1]	Shift to cloud creates new threat vectors, data exposure[2]	Email fraud is on the rise[3]	SMB threat landscape: 30-day average[4]
 Rely on user to run malicious code  Malicious links are credential phishing	Gartner®  "Email is the most important Office 365 service"  Hybrid integration is important, but also a large source of technical problems	**$26.6B+** Direct losses worldwide (June 2016-July 2019) **166,349** Incidents worldwide	 **129** Email Attacks  **57** Phishing Attacks  **73** Malicious Attachments

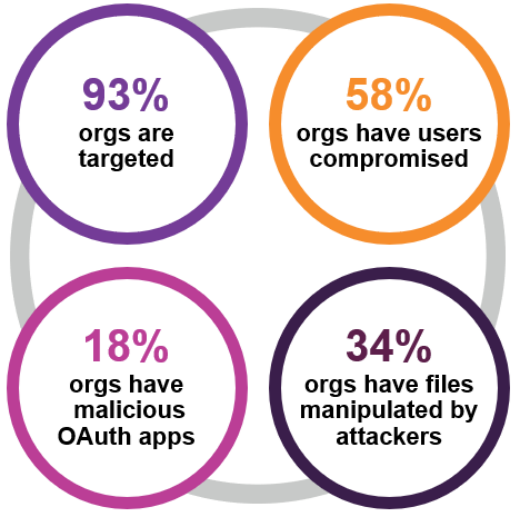
proofpoint.

Why has Proofpoint been so successful in the email security space?

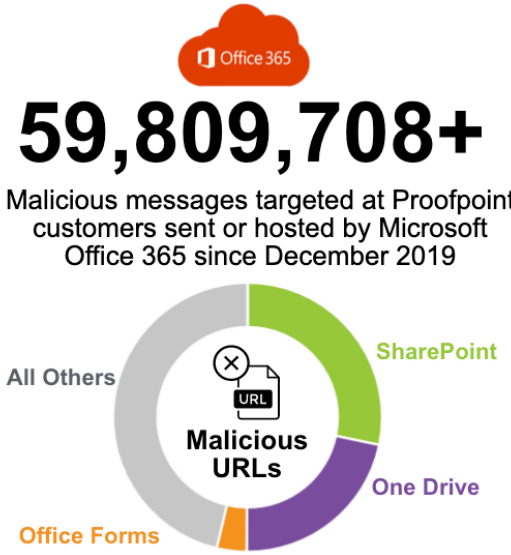
Why isn’t Microsoft O365 enough?

Microsoft continues to be a top target for bad actors

1 Attackers have the Microsoft Blueprint



2 Legitimate filesharing abuse on O365



3 "Not Good Enough"

1,000+ Accounts moved to Microsoft only to move to another secure email gateway (SEG) within a **7.2** months on average

4 Proofpoint 10 days behind Microsoft

Threat Type	Blocked
Bulk Email	1,141,409
Low Risk Spam	85,985
Malicious Spam	35,801
Phish	2,017
Malware	2,300

proofpoint.

Analysts: “Third party security tools should secure O365”

Gartner

Market Guide for Email Security

Published 8 September 2020 - ID G00722358 - 39 min read

By Analysts Mark Harris, Peter Firstbrook, Ravisha Chugh

Initiatives: Infrastructure Security

Dramatic increases in the volume and success of phishing attacks and migration to cloud email require a reevaluation of email security controls and processes. Security and risk management leaders must ensure that their existing solution remains appropriate for the changing landscape.

Overview

Key Findings

- The adoption of cloud office systems from Microsoft and Google continues to grow, forcing security and risk management leaders to evaluate the native capabilities offered by products.
- Impersonation and account takeover attacks are increasing and causing direct financial loss, as users place too much trust in the identities associated with incoming email and are inherently vulnerable to deception and social engineering.
- There is no single technology solution to business email compromise (BEC) attacks. Solutions need to be a combination of technology and user education.
- Compliance and regulation requirements and concerns are putting greater emphasis on email data security.
- Vendors are evolving to support new detect and response capabilities by integrating directly with the email system via API rather than replace the MTA role. This enables faster deployment and multiple complementary solutions to improve detection accuracy.

Gartner

If you have stronger security requirements, consider M365 E3, along with select third-party tools — particularly an email security gateway and a CASB.

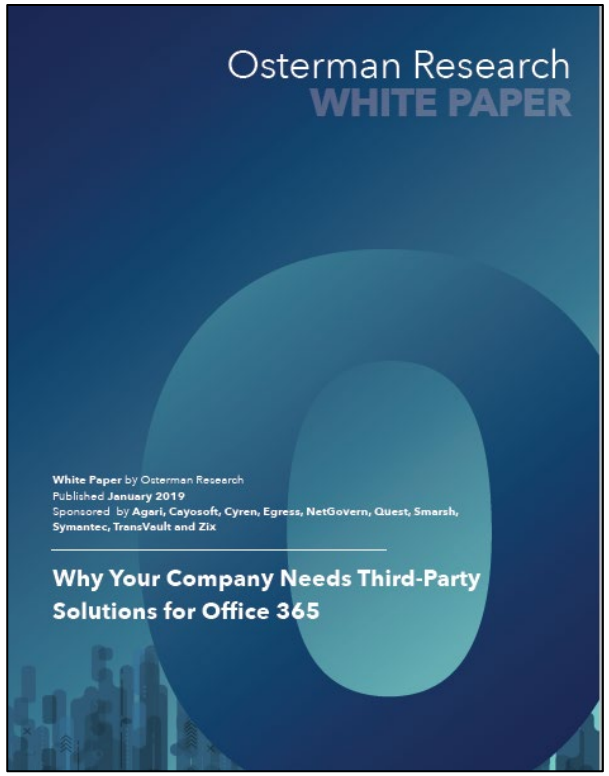
Exchange ATP has no ability to recognize so-called business email compromise.

Microsoft has an opportunity and an incentive to solve the phishing issues, but based on historical results, it must become more agile and respond more rapidly to changing attacker tactics. As Microsoft's SEG market share increases, smart attackers will specifically target Microsoft's defenses.

Gartner, Fighting Phishing 2021

Microsoft continue investment in Office 365 security improvements, and research shows that more than one in four companies route their email traffic directly, effectively using the built-in capabilities as the first line of defense. At the same time Gartner clients report dissatisfaction with natively available capabilities and are, therefore, choosing to supplement with third-party products.

Gartner, Market Guide for Email Security 2020



Osterman Research

Market research and insight on security, archiving and other technologies

proofpoint.

What are some common challenges MSPs face trying to protect their customers?

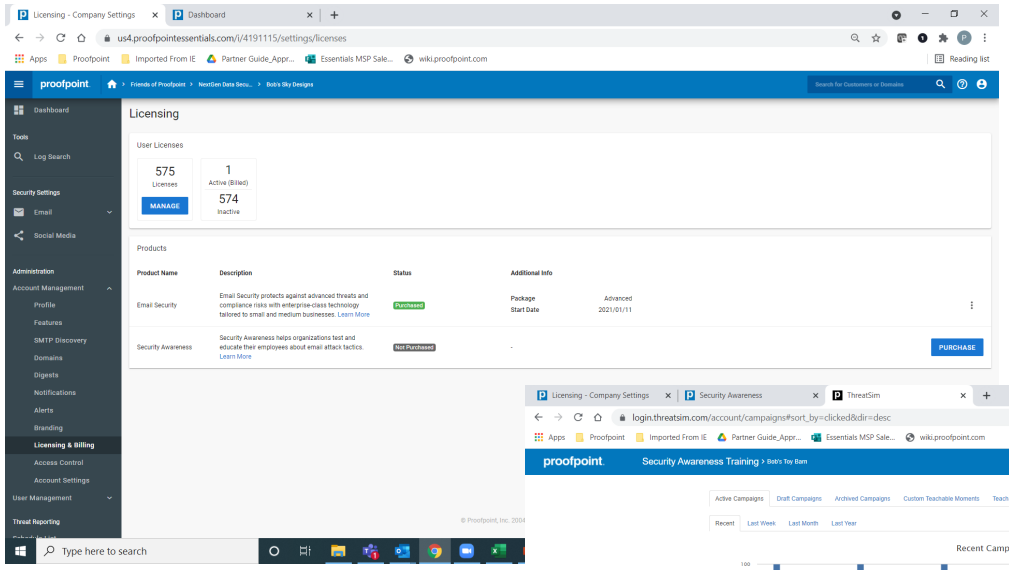
How does the Proofpoint Essentials Platform enable MSPs to be more efficient and manage more customers?

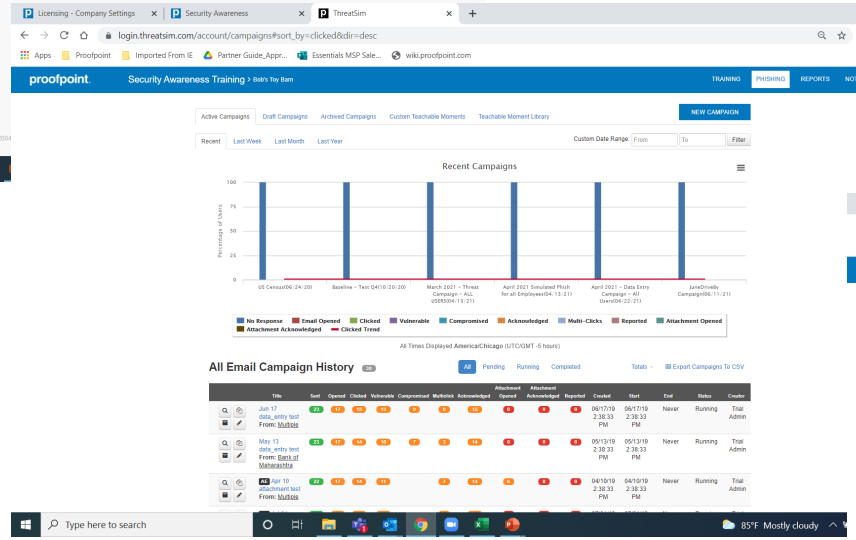
How does the Proofpoint platform provide a more holistic approach to security and enable MSP's to easily scale and increase revenue?

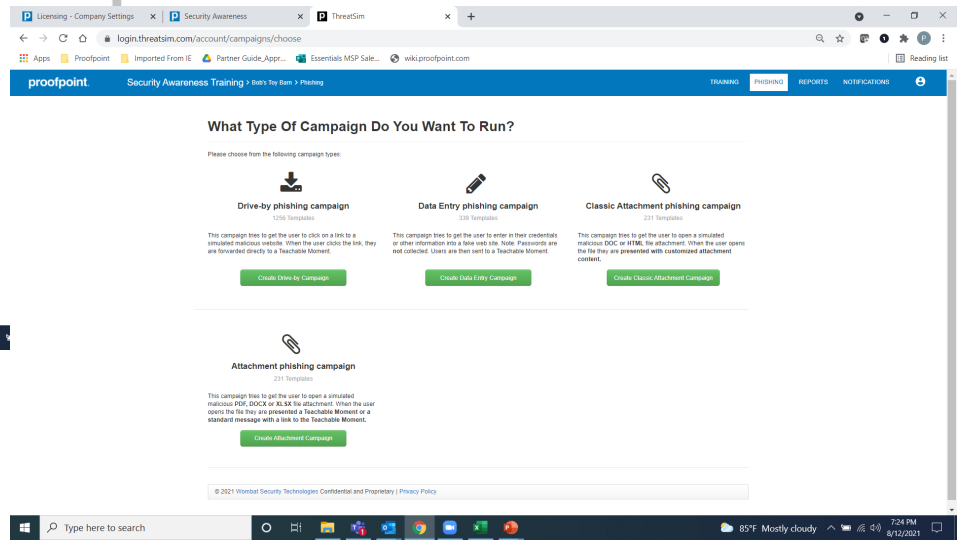
When was a Pax8 partner faced with the challenge of having to migrate a large customer base from another solution over to Proofpoint?

What have you seen from the partner community as a reaction to the Kaseya attack?

Security Awareness from Proofpoint







ChannelPro

Thank You!

proofpoint®

pax8