

**proofpoint.**

# Analyst and Investor Day

Index ▲ 1.56 ▼ 0.78

**ANALYST DAY 2017**

© 2017 Proofpoint, Inc. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners

# Agenda

1:00–1:05	<b>Welcome</b>	<b>Paul Auvil</b> CFO
1:05–1:35	<b>Strategy Overview</b>	<b>Gary Steele</b> CEO
1:35–2:00	<b>Extending the Email Security Franchise</b>	<b>Bhagwat Swaroop</b> EVP and GM Email Security Products Group
2:00–2:25	<b>Extending the TAP Franchise</b>	<b>David Knight</b> EVP/GM Threat Systems Group
2:25–2:40	<b>Threat Landscape Update</b>	<b>Bryan Burns</b> VP Threat Research
2:40–3:00	<b>Compliance and Digital Risk</b>	<b>Darren Lee</b> SVP/GM Archiving and Governance Products Group
3:00–3:20	<b>Break</b>	

# Agenda

3:20–3:50	<b>Customer Panel (Will Not Be Webcast)</b>	<b>Ryan Kalember</b> SVP Cybersecurity Strategy
3:50–4:10	<b>Driving Growth and Go-To-Market</b>	<b>Tracey Newell</b> EVP Global Field Operations
4:10–4:30	<b>Financial Update</b>	<b>Paul Auvil</b> CFO
4:30–5:00	<b>Q&amp;A</b>	<b>Executive Team and Attendees</b>
5:00–7:00	<b>Cocktail Reception and Appetizers</b>	<b>Executive Team and Attendees</b>

# SAFE HARBOR

This presentation contains “forward-looking” statements that involve risks, uncertainties and assumptions. If the risks or uncertainties ever materialize or the assumptions prove incorrect, our results may differ materially from those expressed or implied by such forward-looking statements. All statements other than statements of historical fact could be deemed forward-looking, including, but not limited to, any projections of financial information; any statements about historical results that may suggest trends for our business and results of operations; any statements of the plans, strategies and objectives of management for future operations; any statements of expectation or belief regarding future events, potential markets or market size, or technology developments; and any statements of assumptions underlying any of the foregoing.

These statements are based on estimates and information available to us at the time of this presentation and are not guarantees of future performance. Actual results could differ materially from our current expectations as a result of many factors, including but not limited to: quarterly fluctuations in our business and results of operations; our ability to address market needs and sell our applications and services successfully; integration of acquisitions; acquisition-related liabilities and charges; the general market conditions; and the effects of competition. These and other risks and uncertainties associated with our business are described in our Quarterly Report on Form 10-Q for the three months ended June 30, 2017, and the other reports we file with the SEC, copies of which are available free of charge at the SEC's website at [www.sec.gov](http://www.sec.gov) or upon request from our investor relations department. All forward-looking statements herein reflect our opinions only as of the date of this presentation and Proofpoint undertakes no obligation, and expressly disclaims any obligation, to update forward-looking statements herein in light of new information or future events.

In addition to U.S. GAAP financials, this presentation includes certain non-GAAP financial measures. These historical and forward-looking non-GAAP measures are in addition to, not a substitute for or superior to, measures of financial performance prepared in accordance with GAAP. The most directly comparable GAAP information and a reconciliation between the non-GAAP figures are provided on slides at the back of this presentation.

Proofpoint is a registered trademark of Proofpoint, Inc. This presentation also contains additional trademarks and service marks of ours and of other companies. We do not intend our use or display of other companies' trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.



**proofpoint.**

# Strategy Overview

Gary Steele, CEO

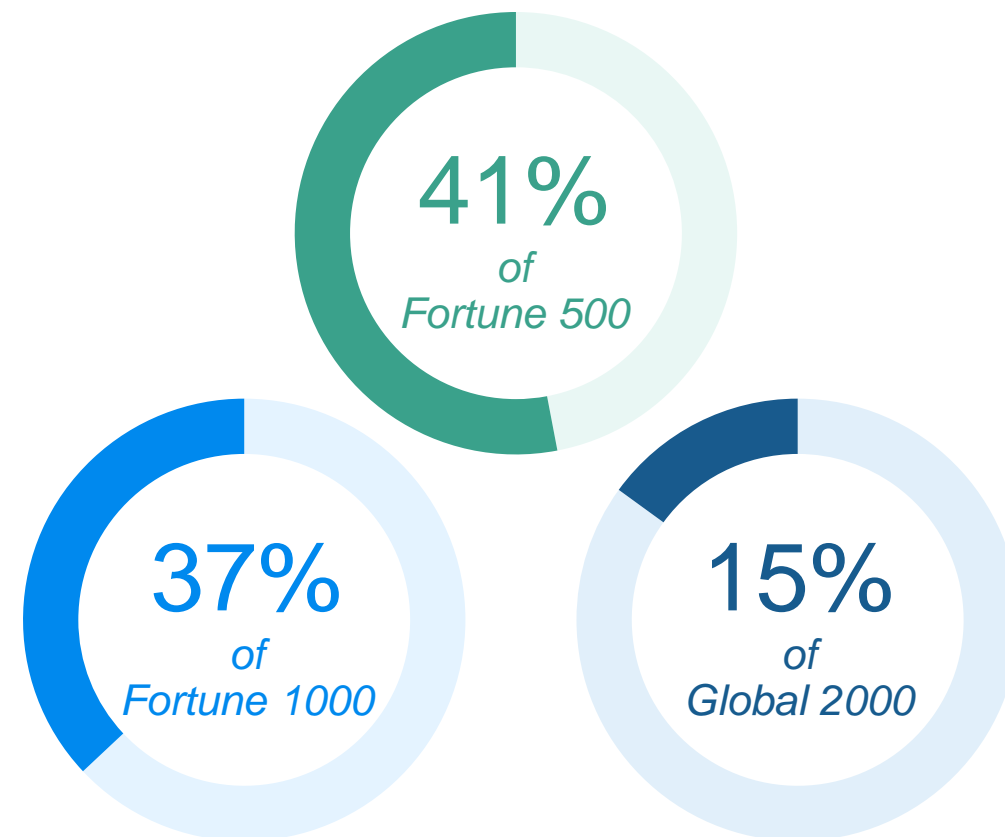
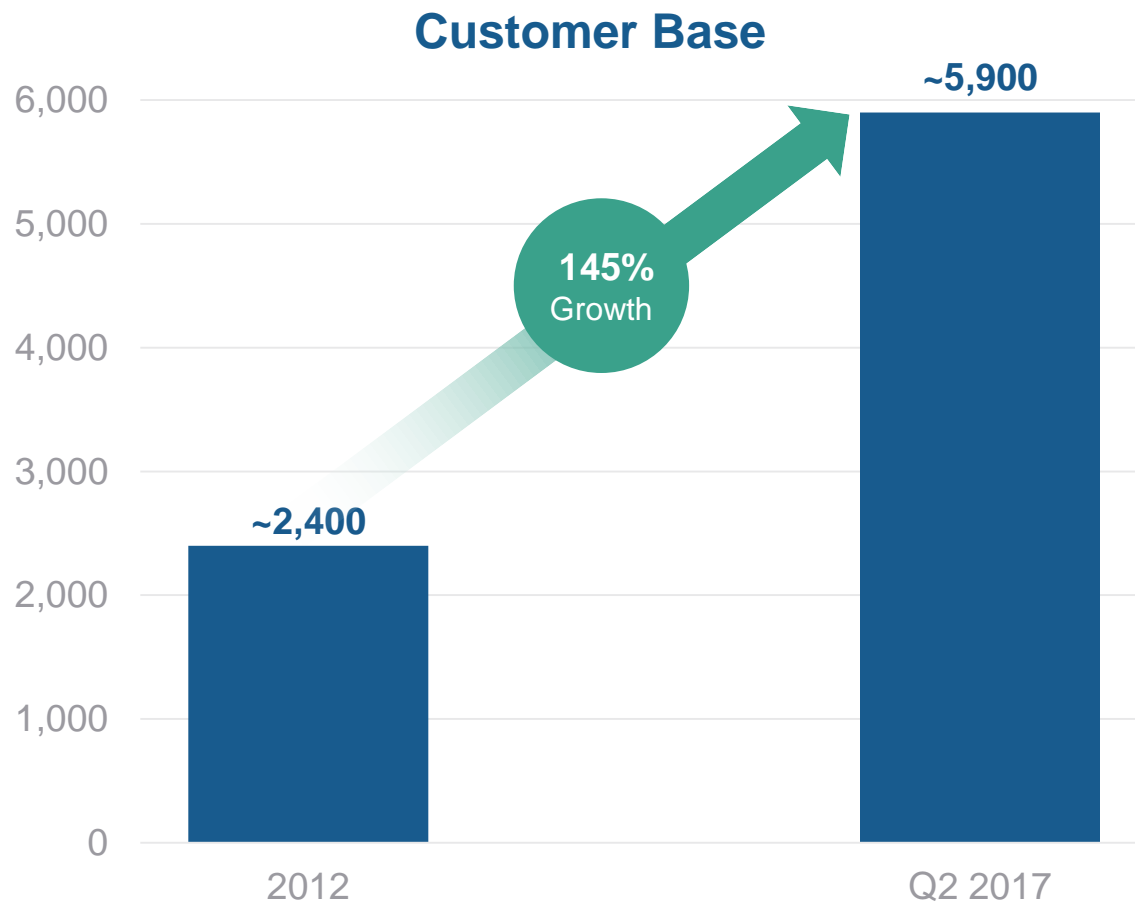


**ANALYST DAY 2017**

# **Next Generation Cybersecurity Company That Protects People, Data, and Brands From Advanced Threats and Compliance Risks**



# Proofpoint in 2017



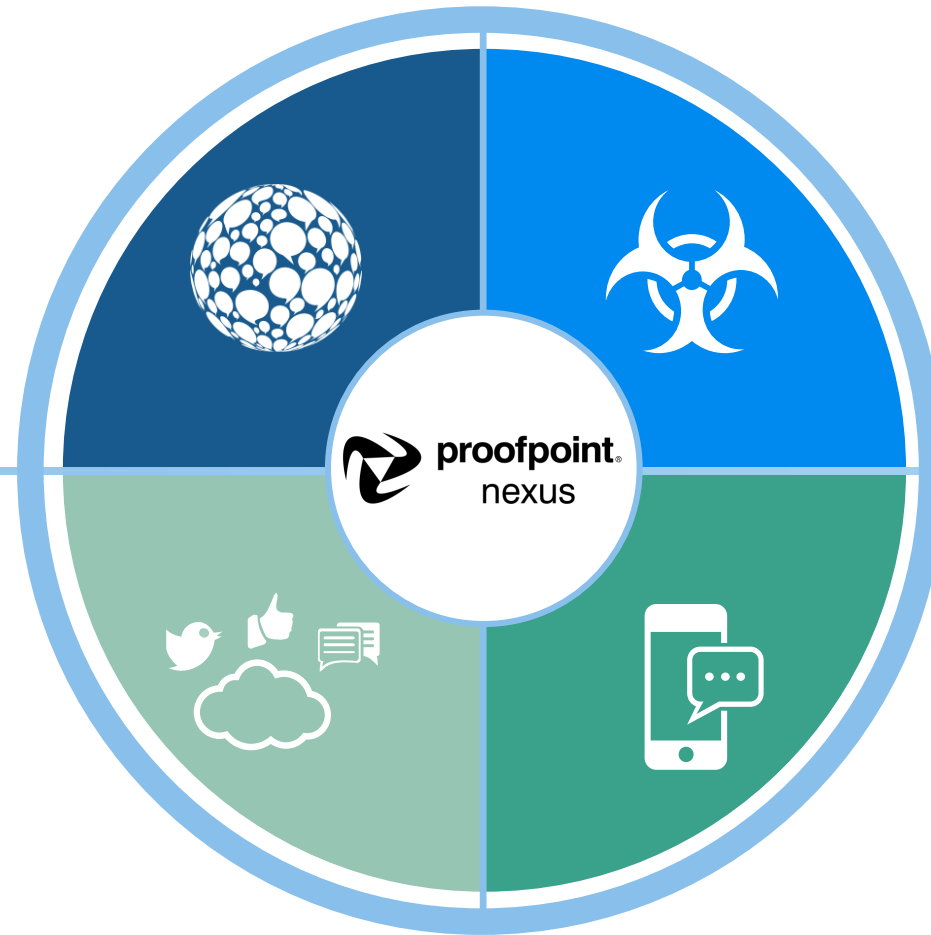
# Unprecedented Visibility

**1B+**  
messages processed  
per day

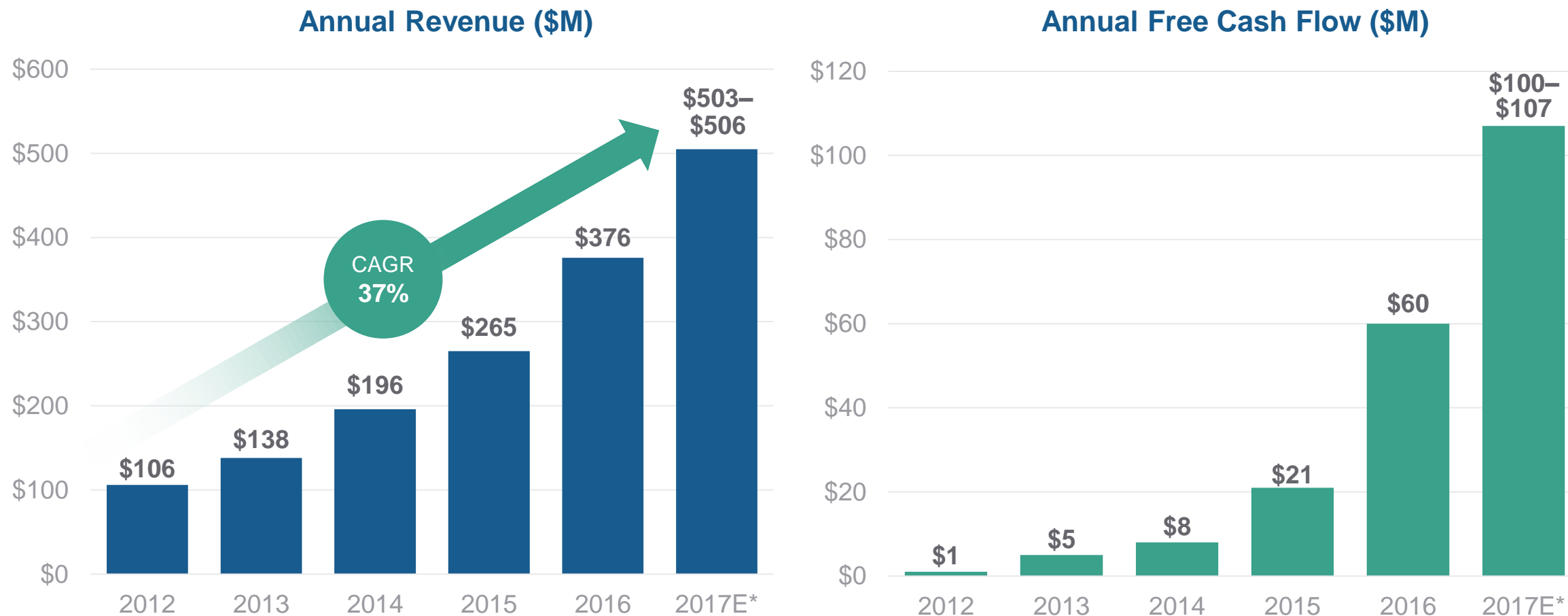
**300,000**  
unique malware  
samples scanned  
per day

**200M+**  
social media  
accounts scanned

**25M+**  
mobile apps  
scanned



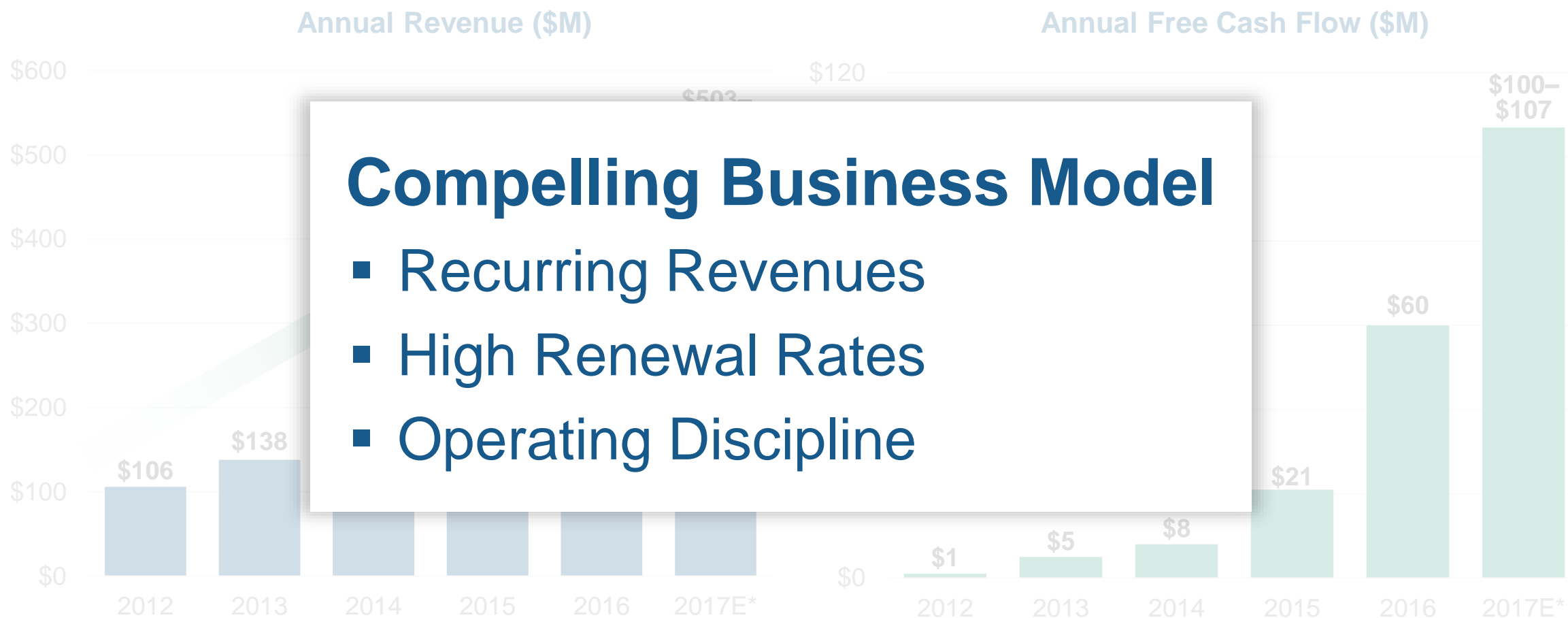
# Strong Track Record of Execution and Growth



\*2017E provided on Form 8K July 27, 2017. 2017E FCF % of revenue assumes midpoint of guidance range. Free Cash Flow defined as net cash provided by operating activities minus capital expenditures.



# Strong Track Record of Execution and Growth



\*2017E provided on Form 8K July 27, 2017. 2017E FCF % of revenue assumes midpoint of guidance range. Free Cash Flow defined as net cash provided by operating activities minus capital expenditures.

# What's Changed Since Last Year

Advances in  
Threat Research



Email Fraud  
Defense



TAP SaaS  
Defense



Domain  
Discover



# What's Changed Since Last Year

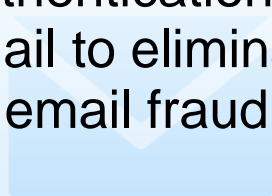
## Advances in Threat Research

Critical role driving overall efficacy



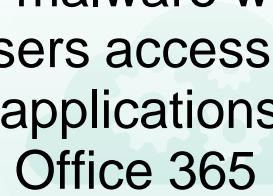
## Email Fraud Defense

Driving the authentication of email to eliminate email fraud



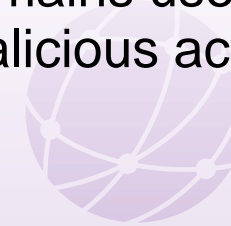
## TAP SaaS Defense

Identify and block malware when users access SaaS applications like Office 365 and G Suite



## Domain Discover

Identify fraudulent domains used for malicious activity



# Attacks Increasingly Target Individuals, Not Infrastructure

Threats use  
social engineering,  
not vulnerabilities



Source: Proofpoint, The Human Factor

Mobile, social,  
SaaS threats ramp  
and evolve

150%

Increase in social media angler phishing

**Customer Service** @Ask\_BankCA  
Mr. Smith, sorry to hear you've been having trouble. To better serve you, please visit our site and login. [banksite.com/CA/customerservice](https://banksite.com/CA/customerservice)

RATs become common in mobile apps



Source: Proofpoint, The Human Factor

Email fraud becomes  
board-level issue

\$5.3B

Direct losses since January 2015,  
up 2,370%

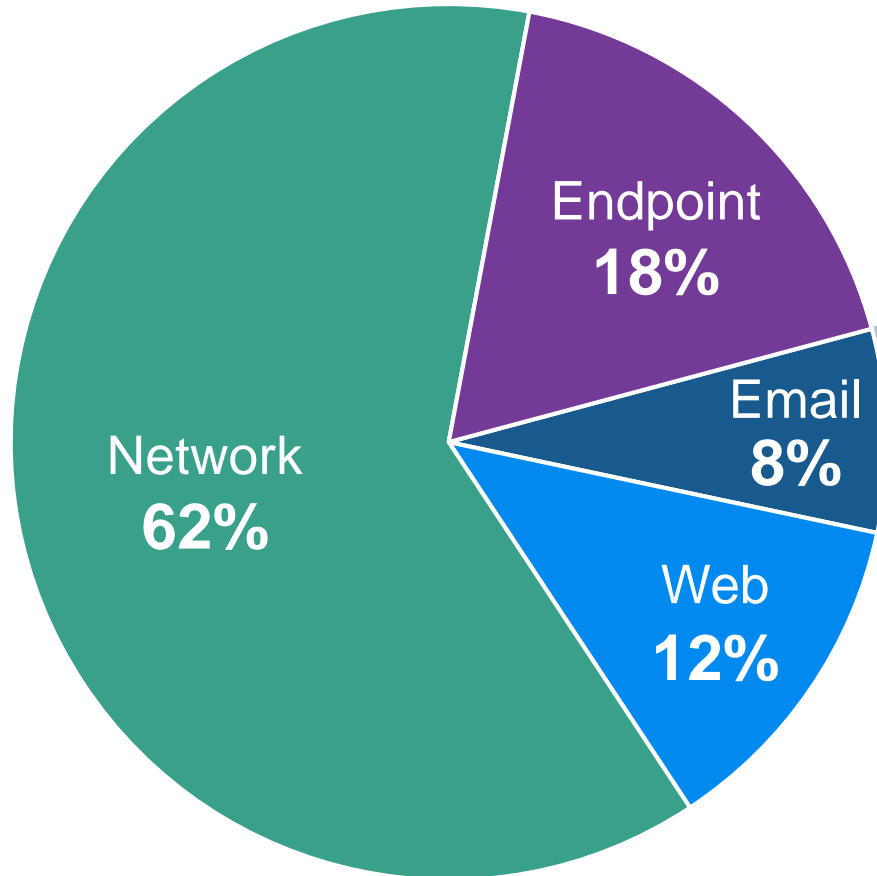
40,203

Organizations victimized  
in the US alone

Source: FBI, ic3.gov

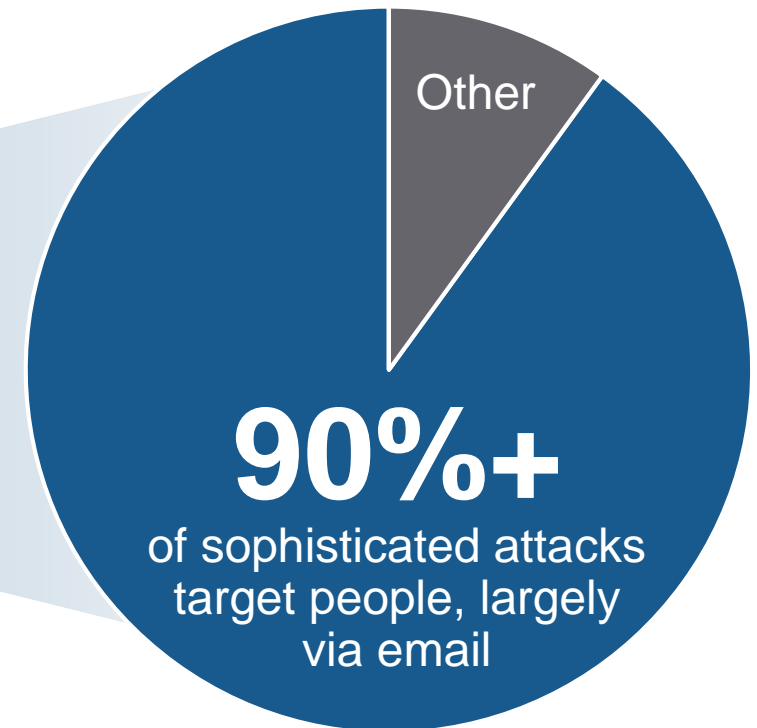
# But Industry Is Not Aligned with the Threats

IT Security Industry



Source: Gartner (2017 forecast)

Attack Vectors



Source: Verizon DBIR, Trend Micro, FEYE, etc.



# Cloud Is Transforming Businesses



# Cloud Is Transforming Businesses



# Proofpoint Platform Protects Individuals

Email

 Office 365

 Exchange

 Suite

Mobile



Social



**proofpoint®**  
nexus

# Proofpoint Platform Protects Individuals

Mobile



Social



SaaS Apps

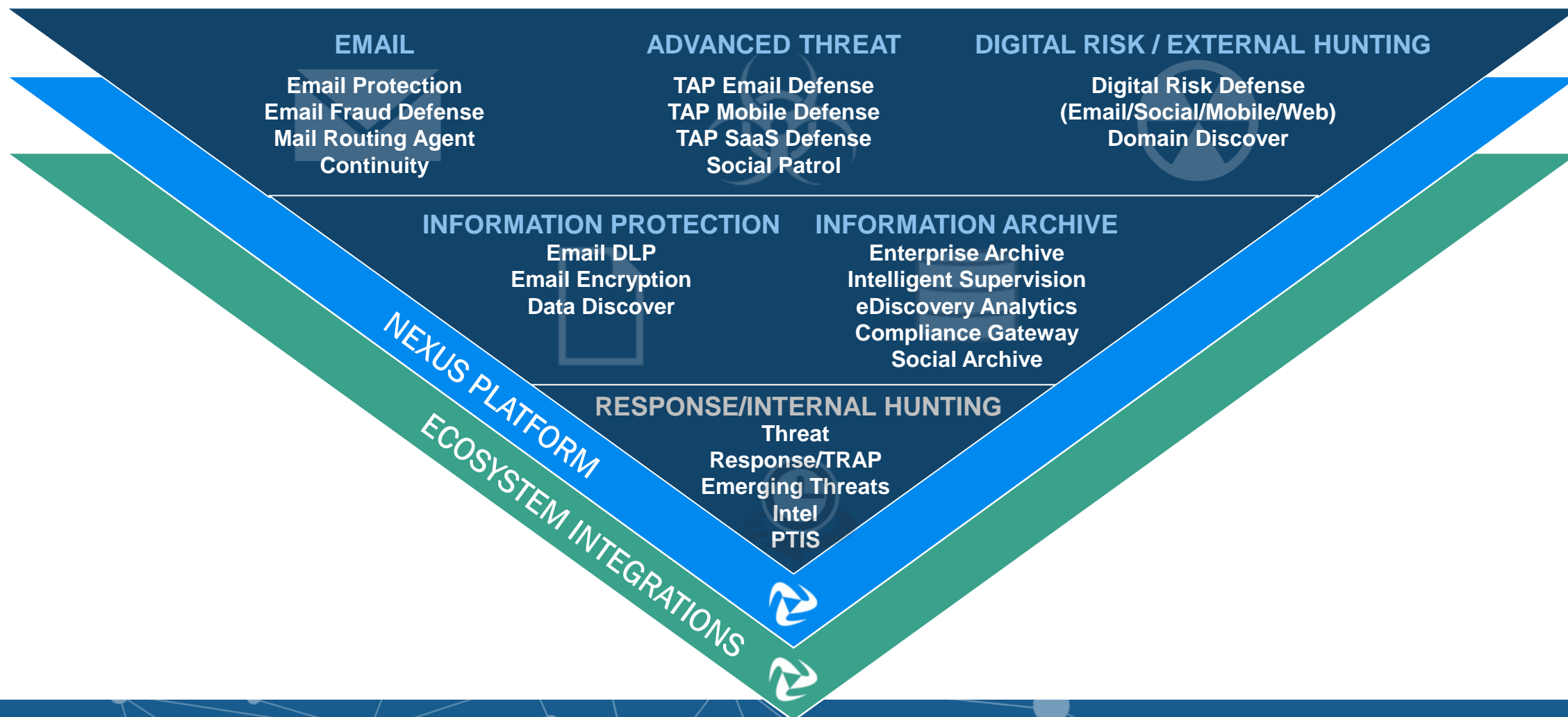


Email



**proofpoint®**  
nexus

# Solutions Across Security, Compliance, Digital Risk



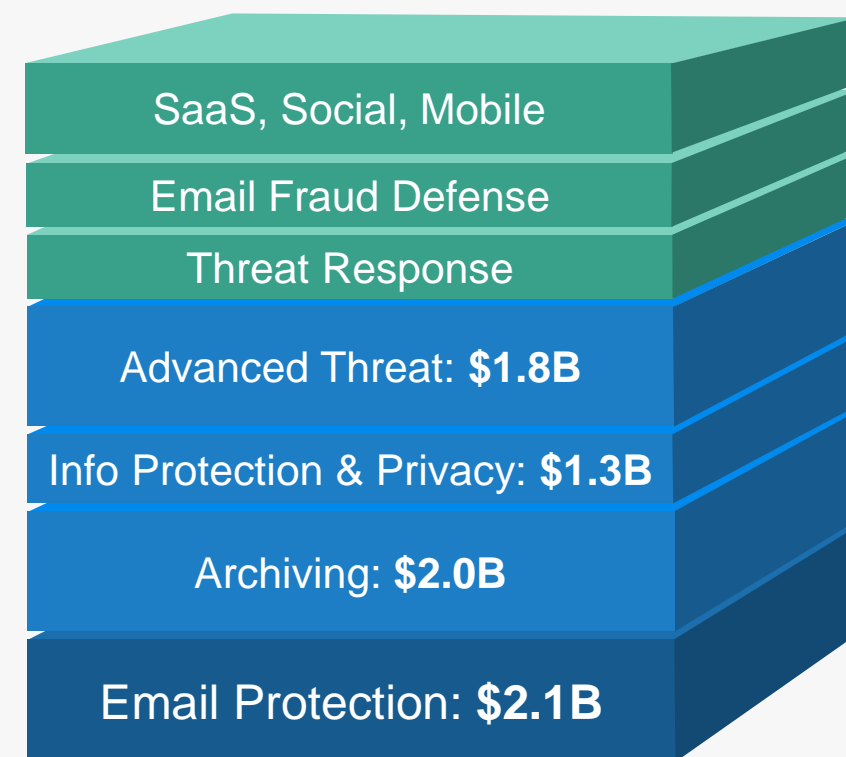
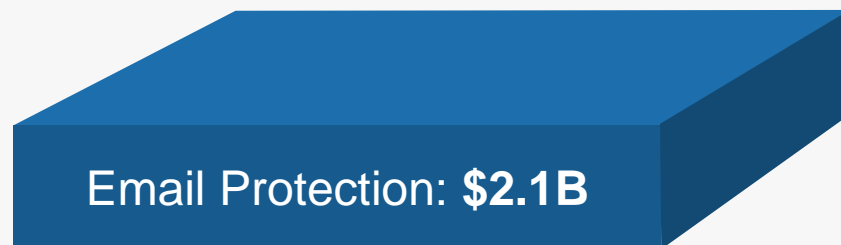


# Product Expansion Fuels Proofpoint's Growth



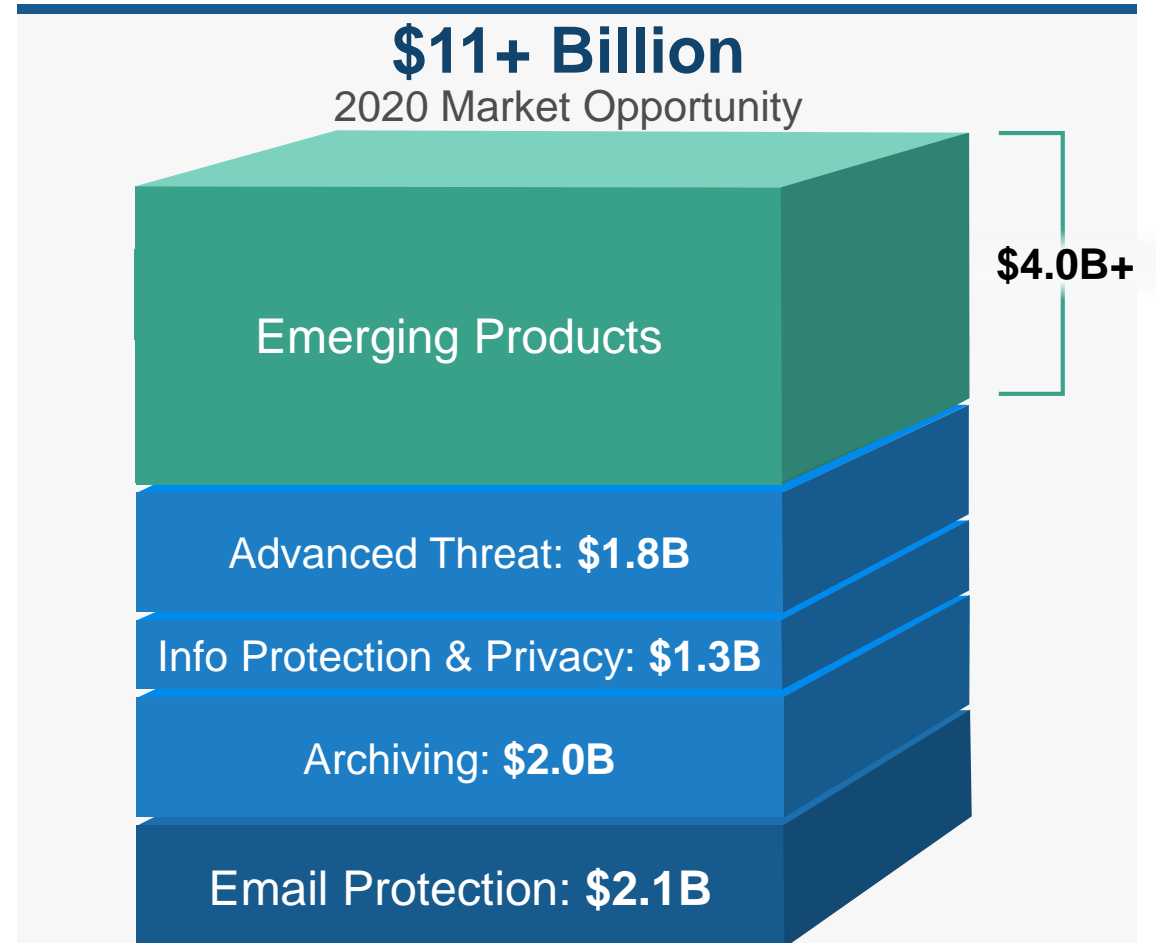
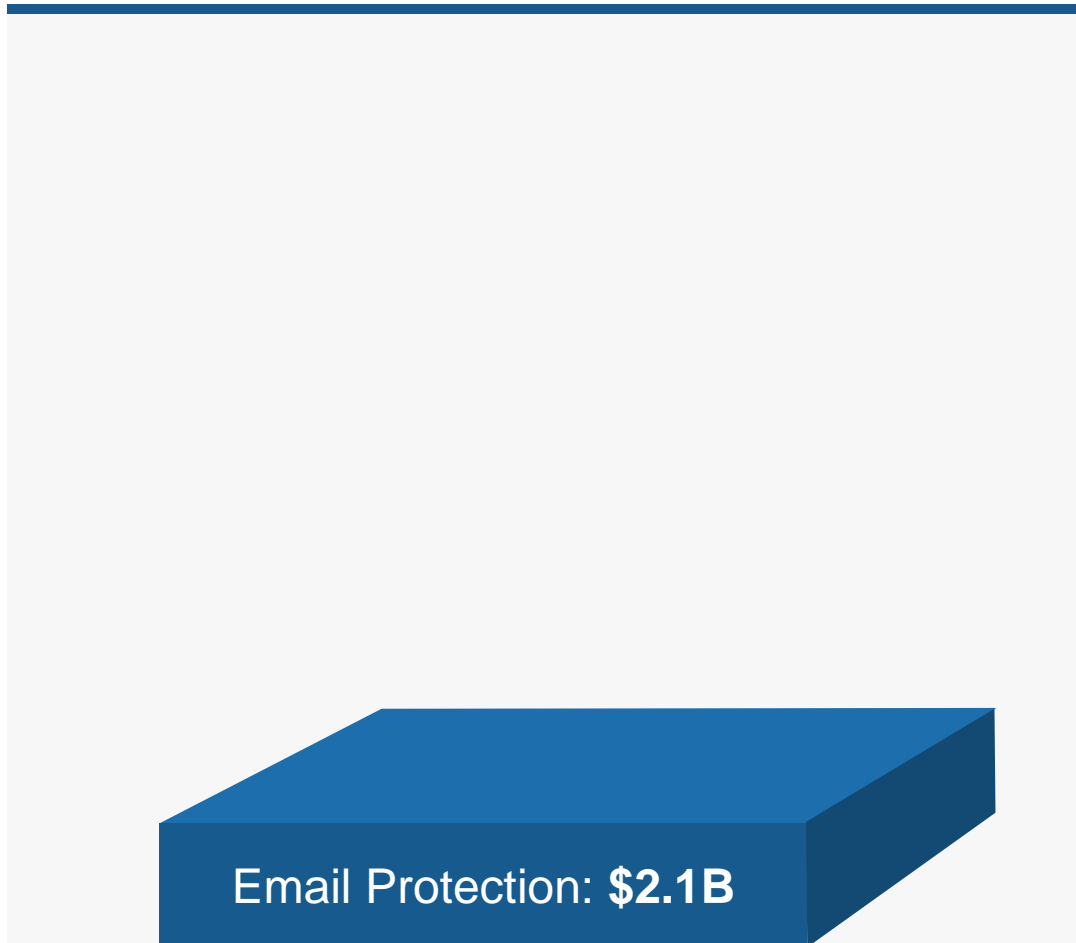
See appendix for sources for market forecasts

# Product Expansion Fuels Proofpoint's Growth



See appendix for sources of market forecasts

# Product Expansion Fuels Proofpoint's Growth



See appendix for sources of market forecasts

# Growth Strategy



# Proofpoint Advantages

- 1** Broad suite of capabilities based on a robust cloud platform
- 2** Innovation and speed deliver industry leading effectiveness
- 3** Highly configurable, but easy to deploy and manage
- 4** Ecosystem built on meaningful technical integration
- 5** Relentless dedication to customer success



**proofpoint™**





**proofpoint.**

# Extending the Email Security Franchise

Bhagwat Swaroop  
EVP/GM, Email Security Group

**ANALYST DAY 2017**

© 2017 Proofpoint, Inc.. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners

# Email Remains the Cornerstone of Business Communication

Employees View Email  
Critical for Productivity



83%

Growing  
5% YoY



225B

emails  
per day

Employees  
Check Email

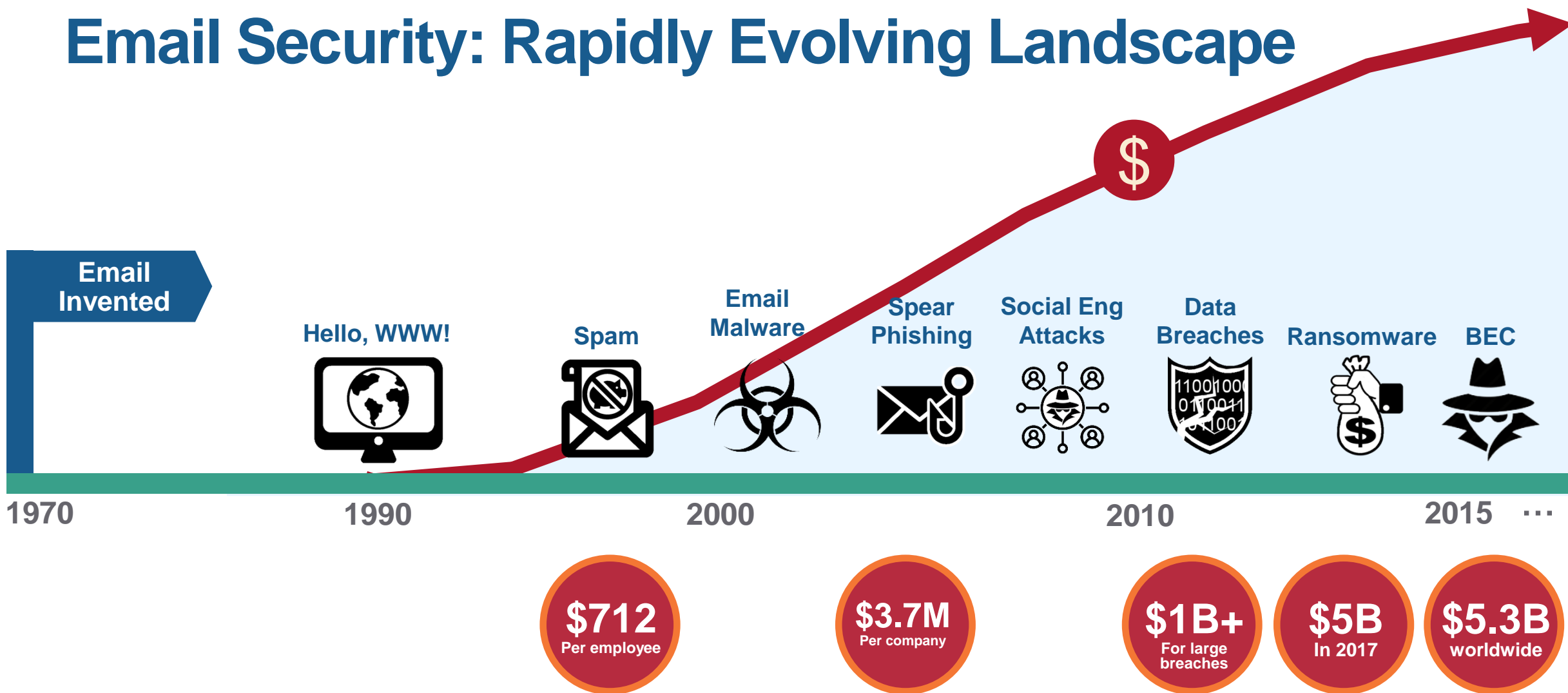


77

times  
per day

Source: Email Statistics Report 2016, The Radicati Group, UC Irvine research, Wiki

# Email Security: Rapidly Evolving Landscape



Source: CSOnline.com, Cybersecurity ventures, Nucleus Research, FBI

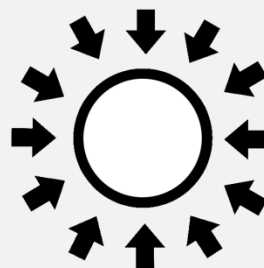
# Major Shifts at Play: Creating Tailwinds

## Email is #1 Threat Vector



90%+ advanced threats  
propagated via email

## Dynamic Threat Landscape



Malware and  
non-malware attacks

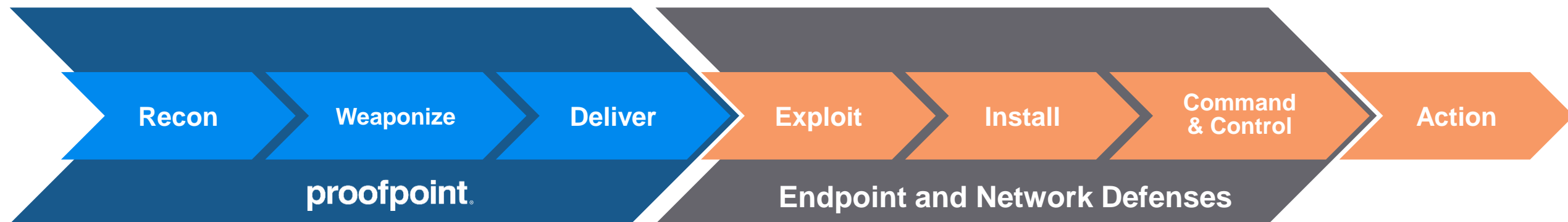
## Move to Cloud



Strong growth  
of Office 365, G Suite

Source: Verizon DBIR

# Email: Most Effective Place to Block Attacks in Kill Chain



## Effective Security

Move left in Attack Chain and prevent attacks before damage

## Less Effective

Attacker already has foothold, damage done

# Email Security Leadership

## Industry Leadership



**Top Banks, Healthcare, Retail**



## Strong Customer Growth



**~5,900 Customers**

**~2,600 TAP Customers**



**35% International Growth**

## Proven Effectiveness



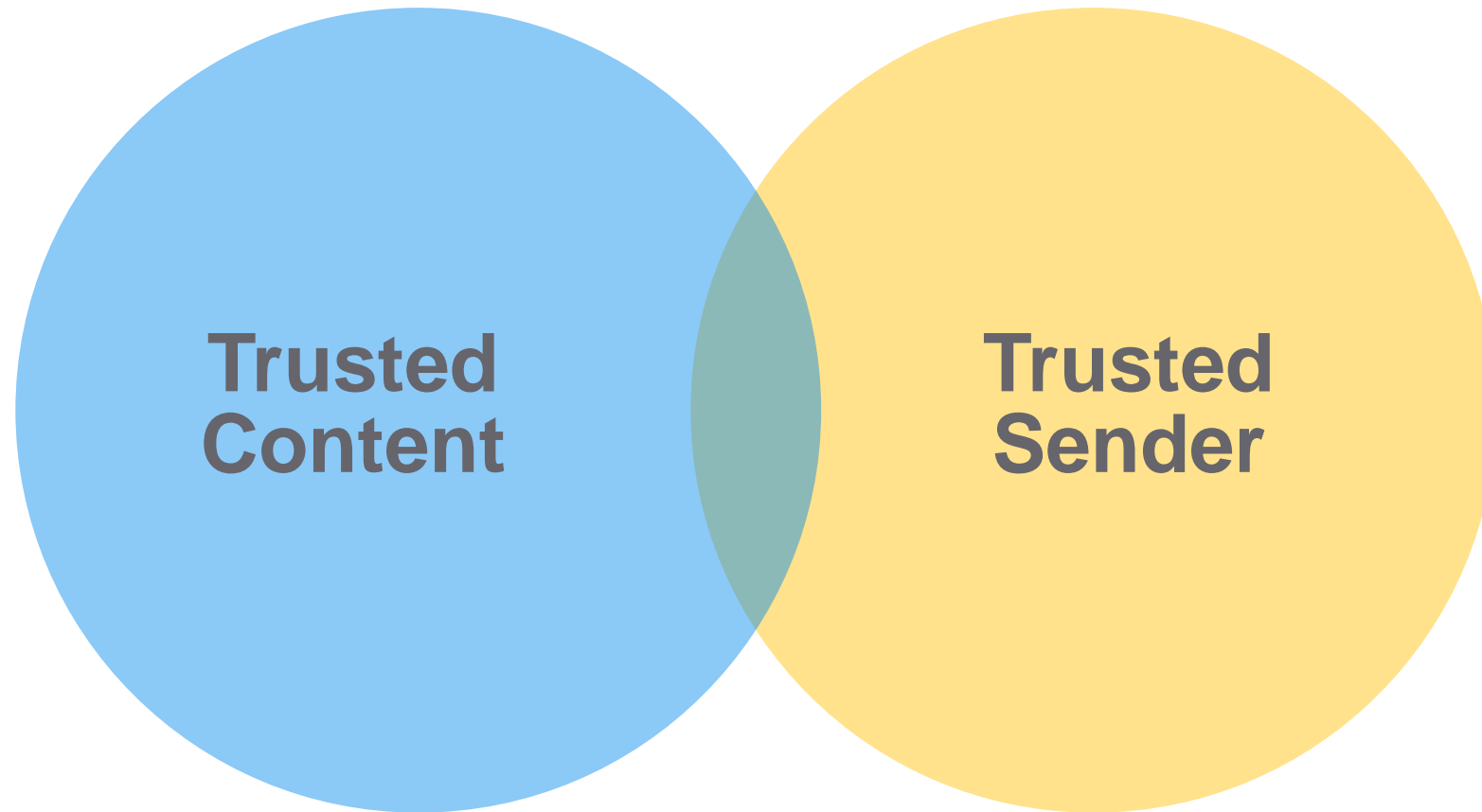
**100M Ransomware Emails in a Day**



**2000 Major Attacks Campaigns**

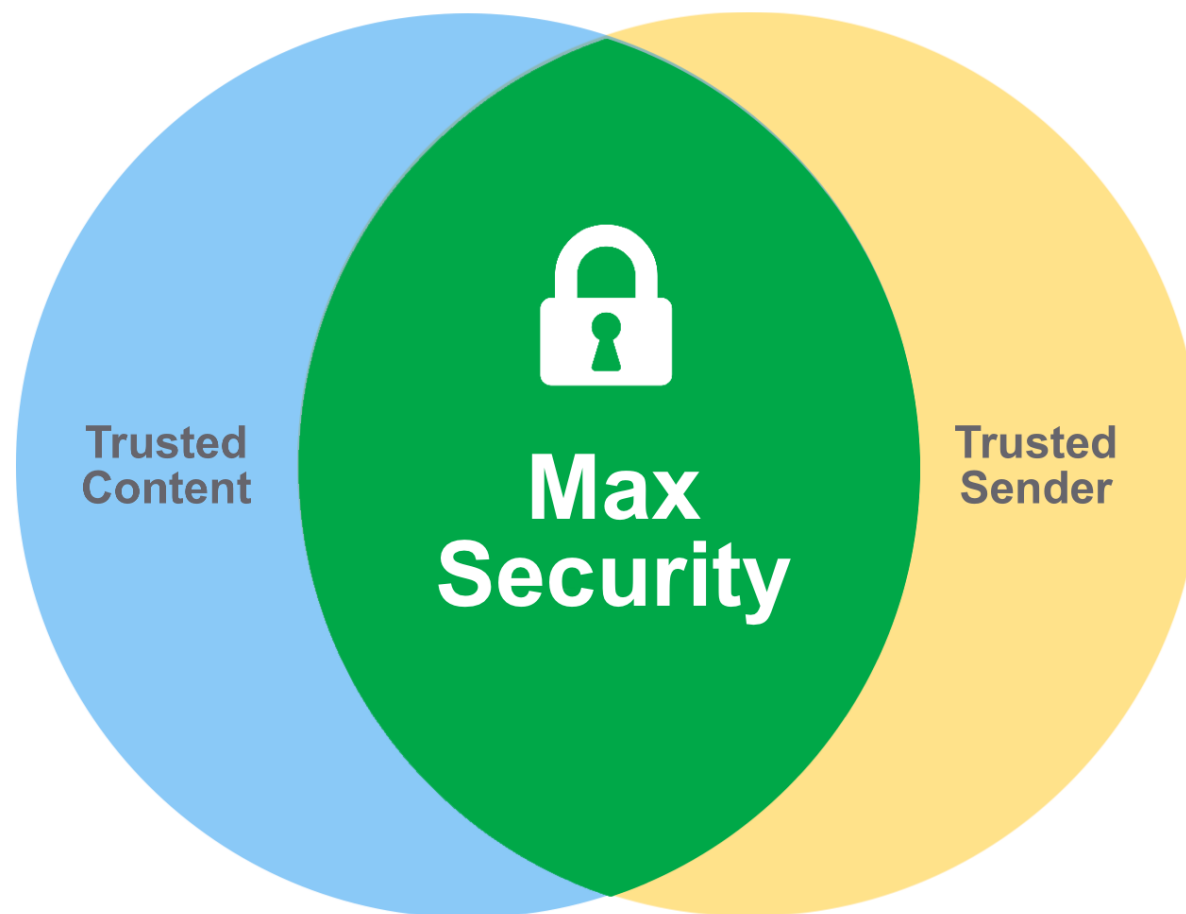
Source: Proofpoint Threat Research 2017

# Maximum Security





# Maximum Security



# Extending the Email Franchise

**proofpoint.** Advanced Email Security

Email arrives



Email Security

# Extending the Email Franchise

**proofpoint.** Advanced Email Security

Email arrives



SPAM



Virus



Malware



DDOS



Phishing

# Extending the Email Franchise

**proofpoint.** Advanced Email Security

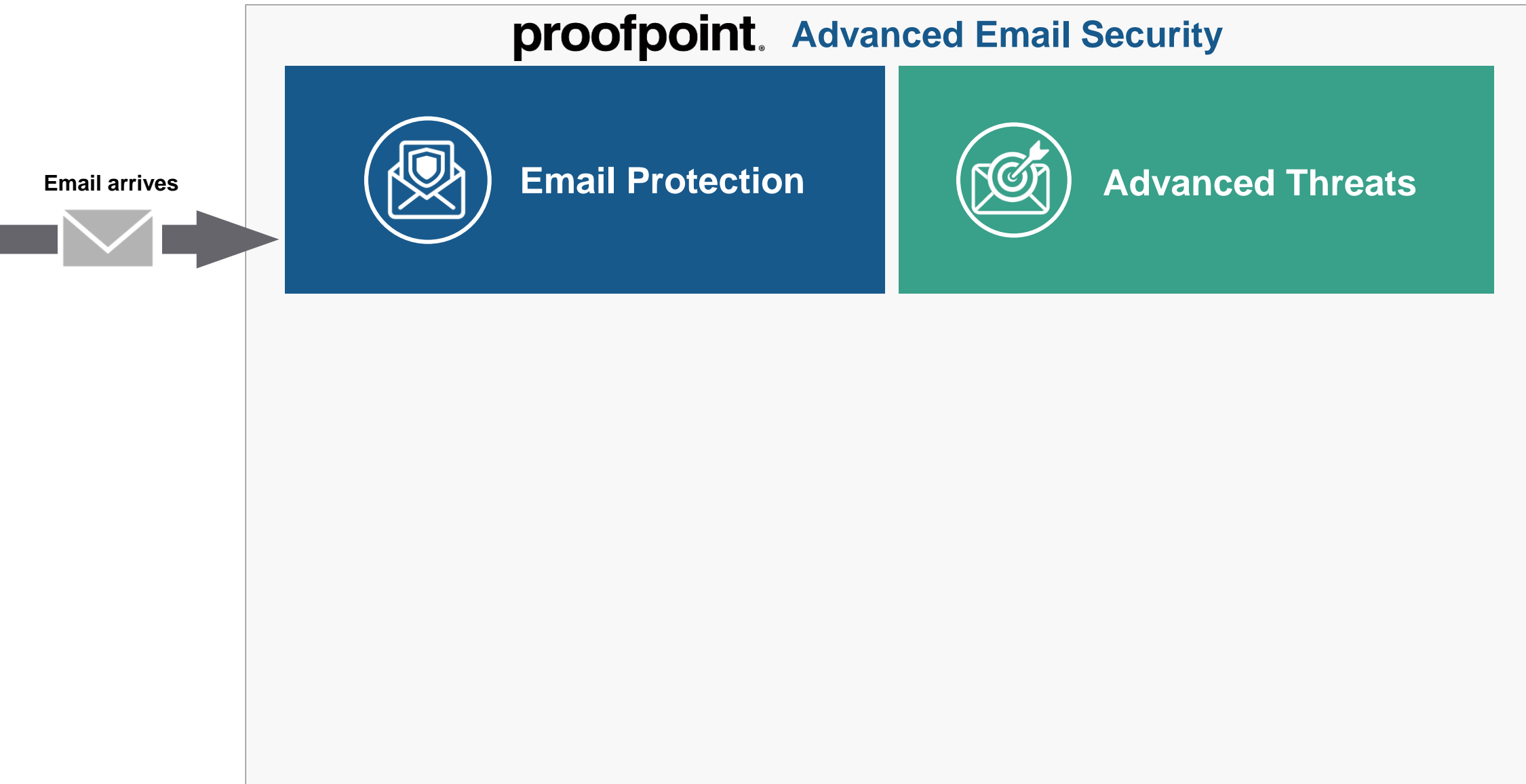


Email Protection

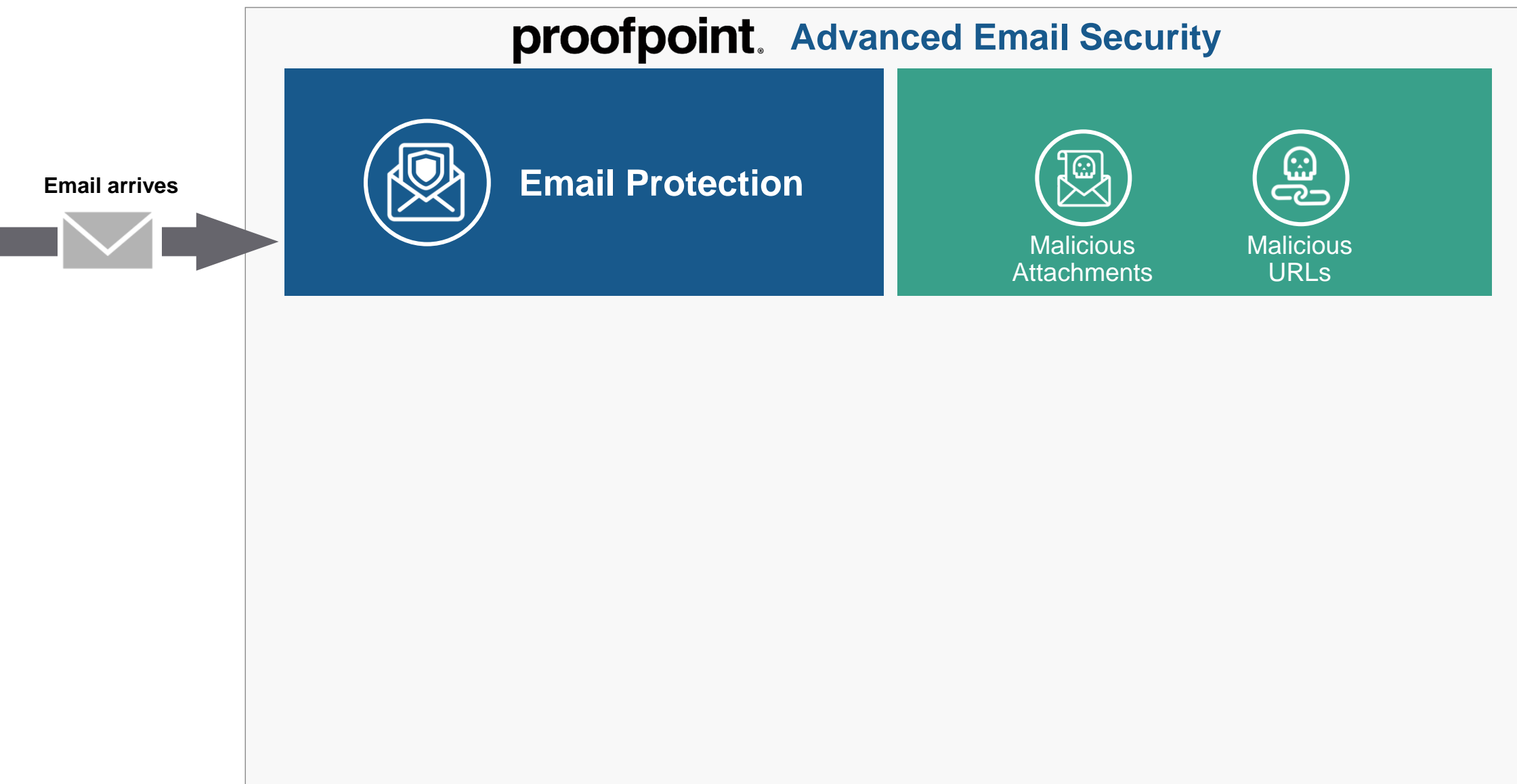
Email arrives



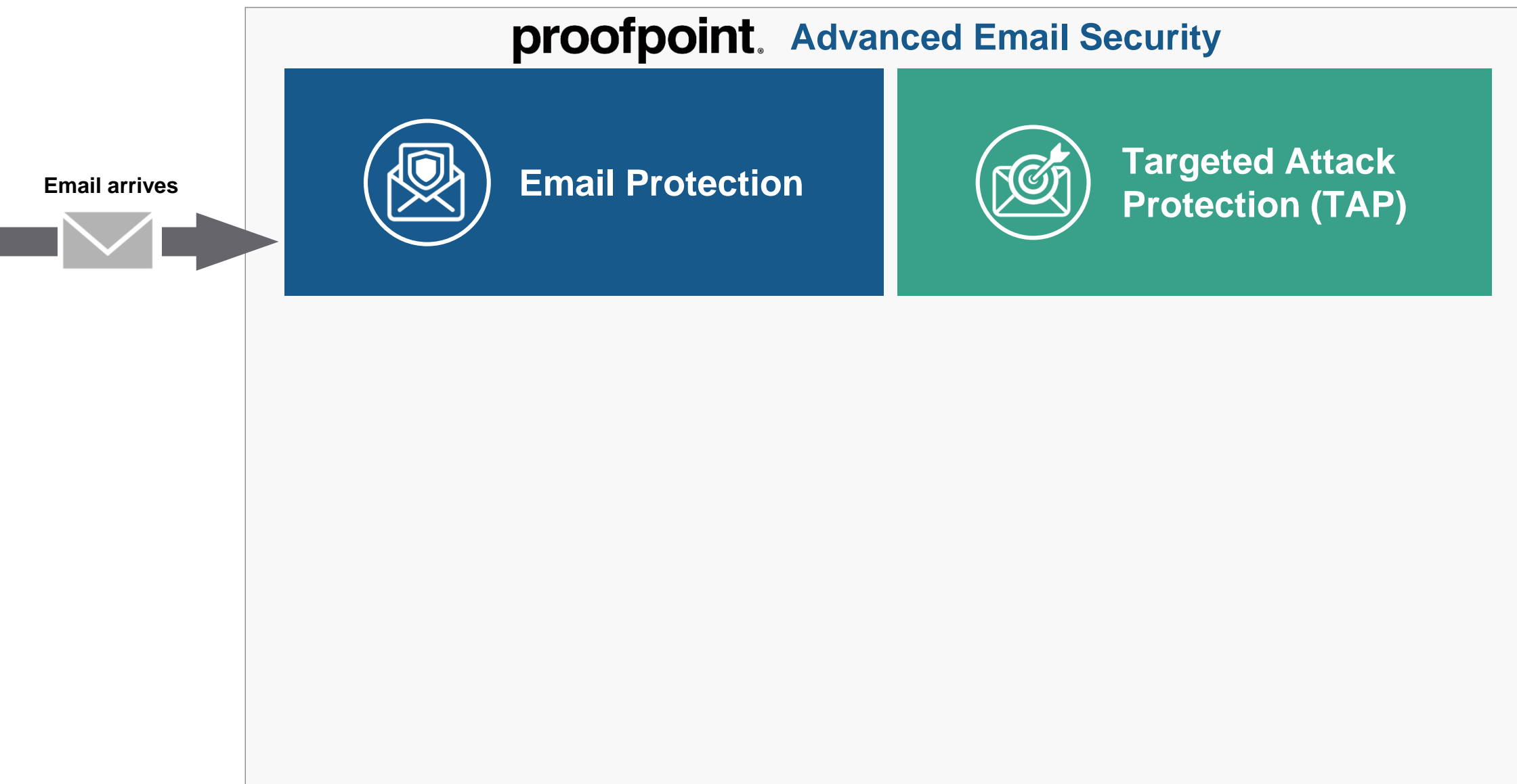
# Extending the Email Franchise



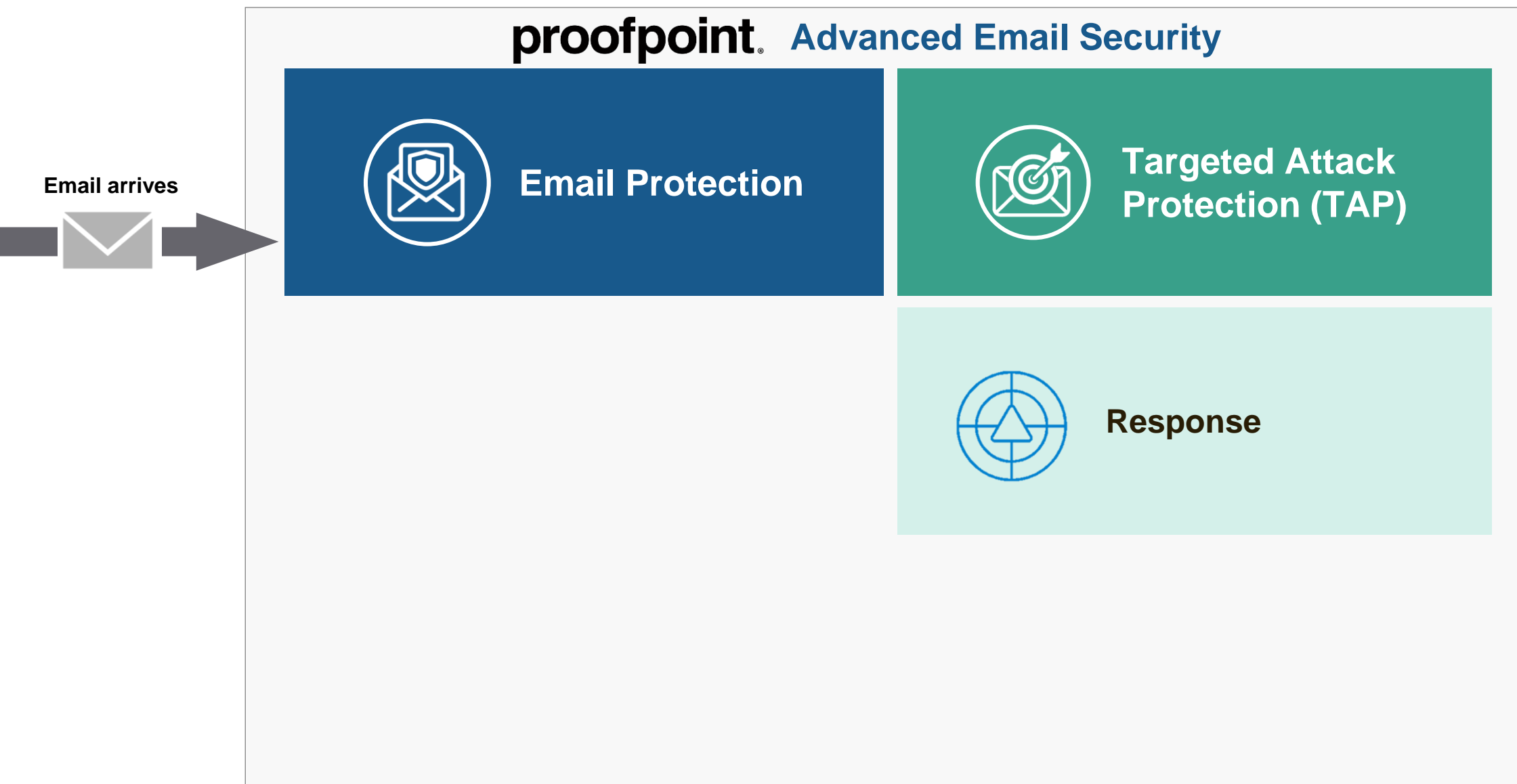
# Extending the Email Franchise



# Extending the Email Franchise

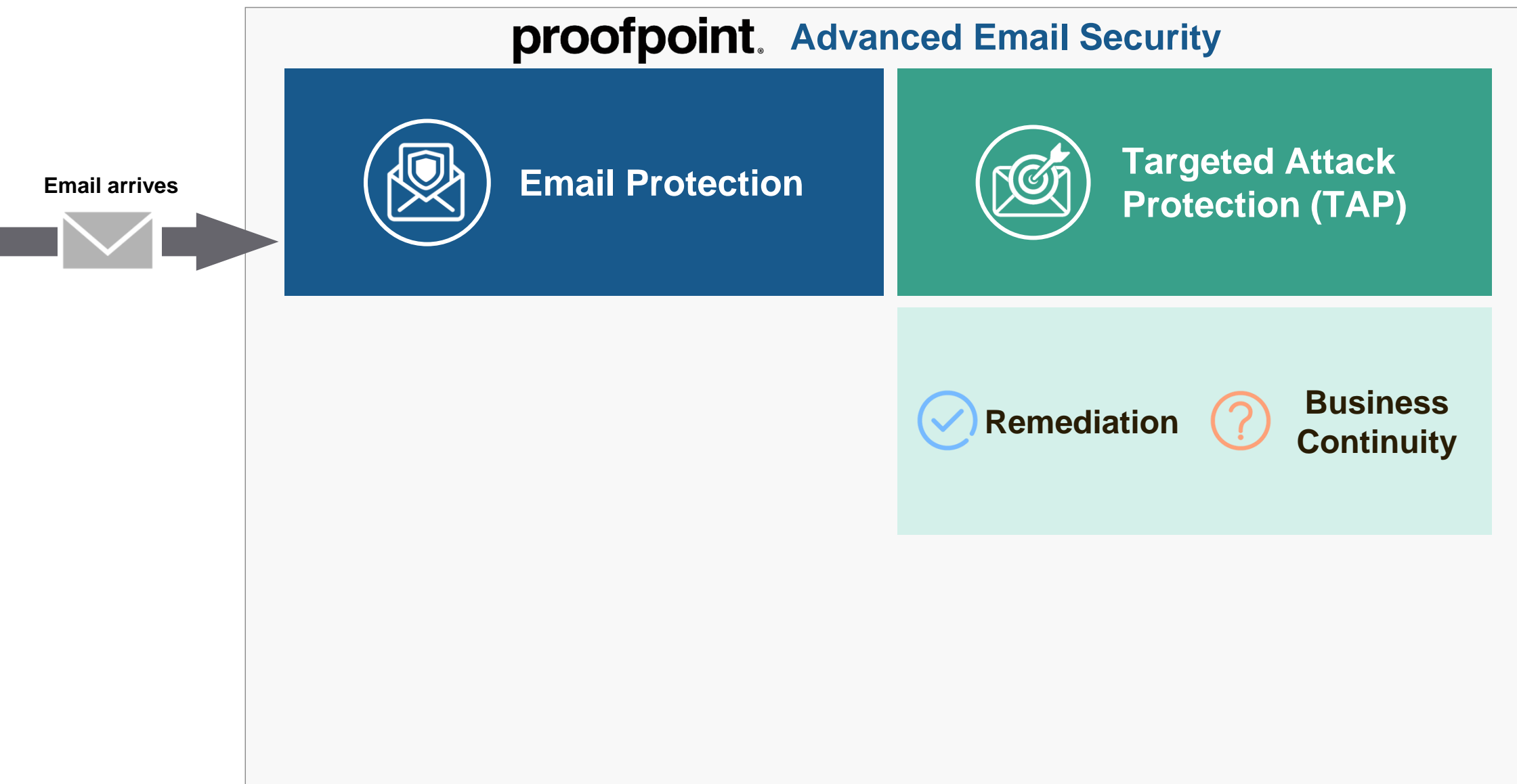


# Extending the Email Franchise

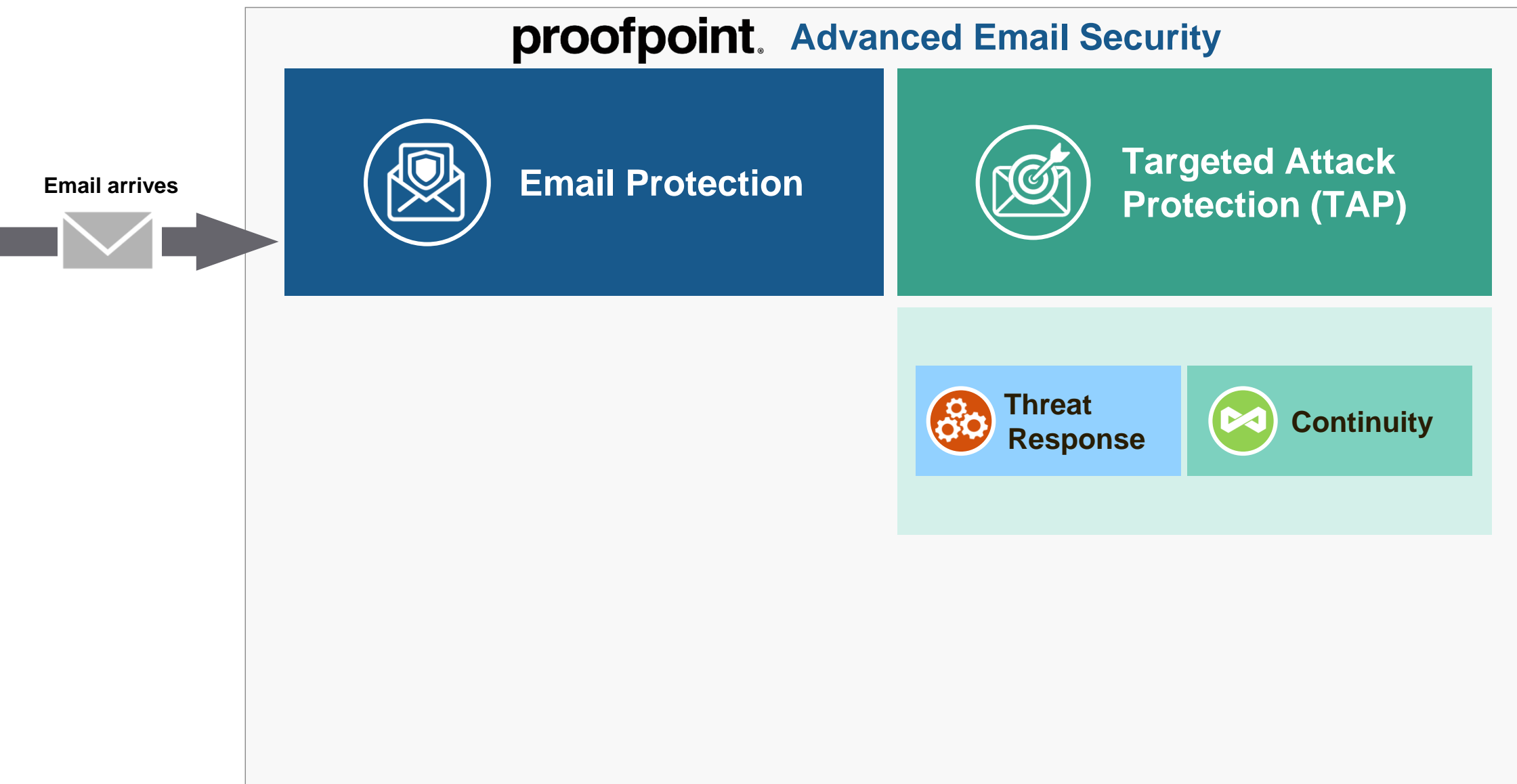




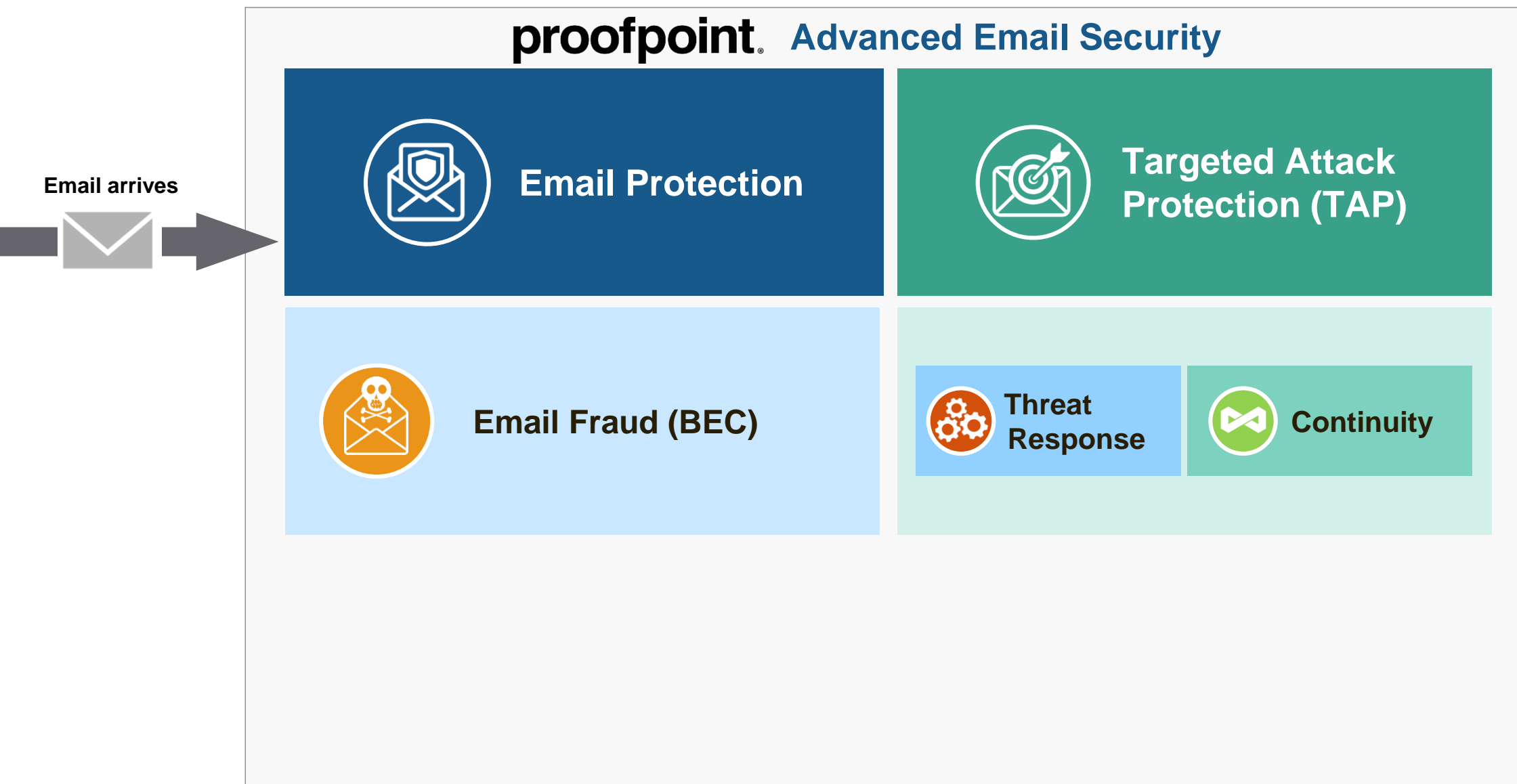
# Extending the Email Franchise



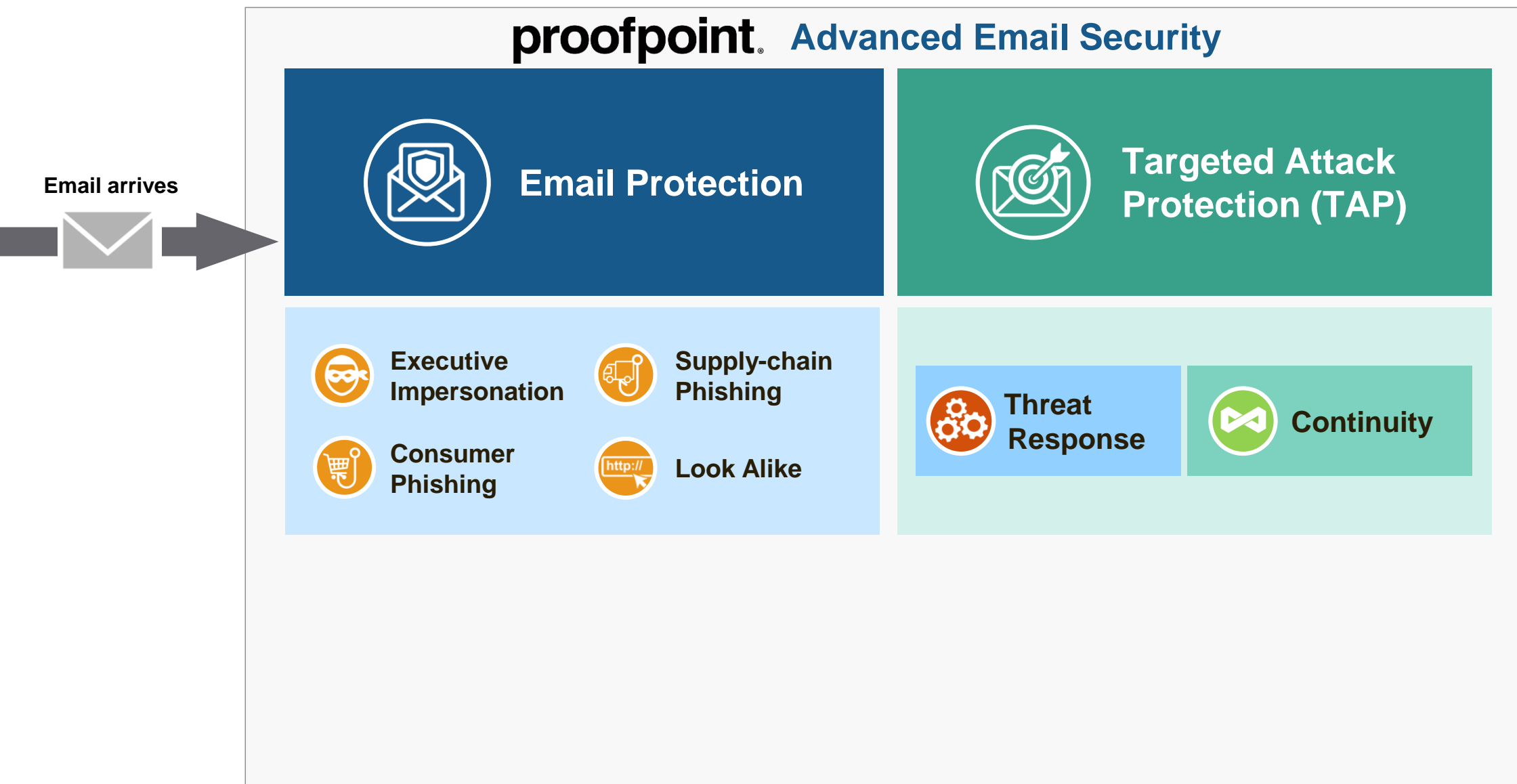
# Extending the Email Franchise



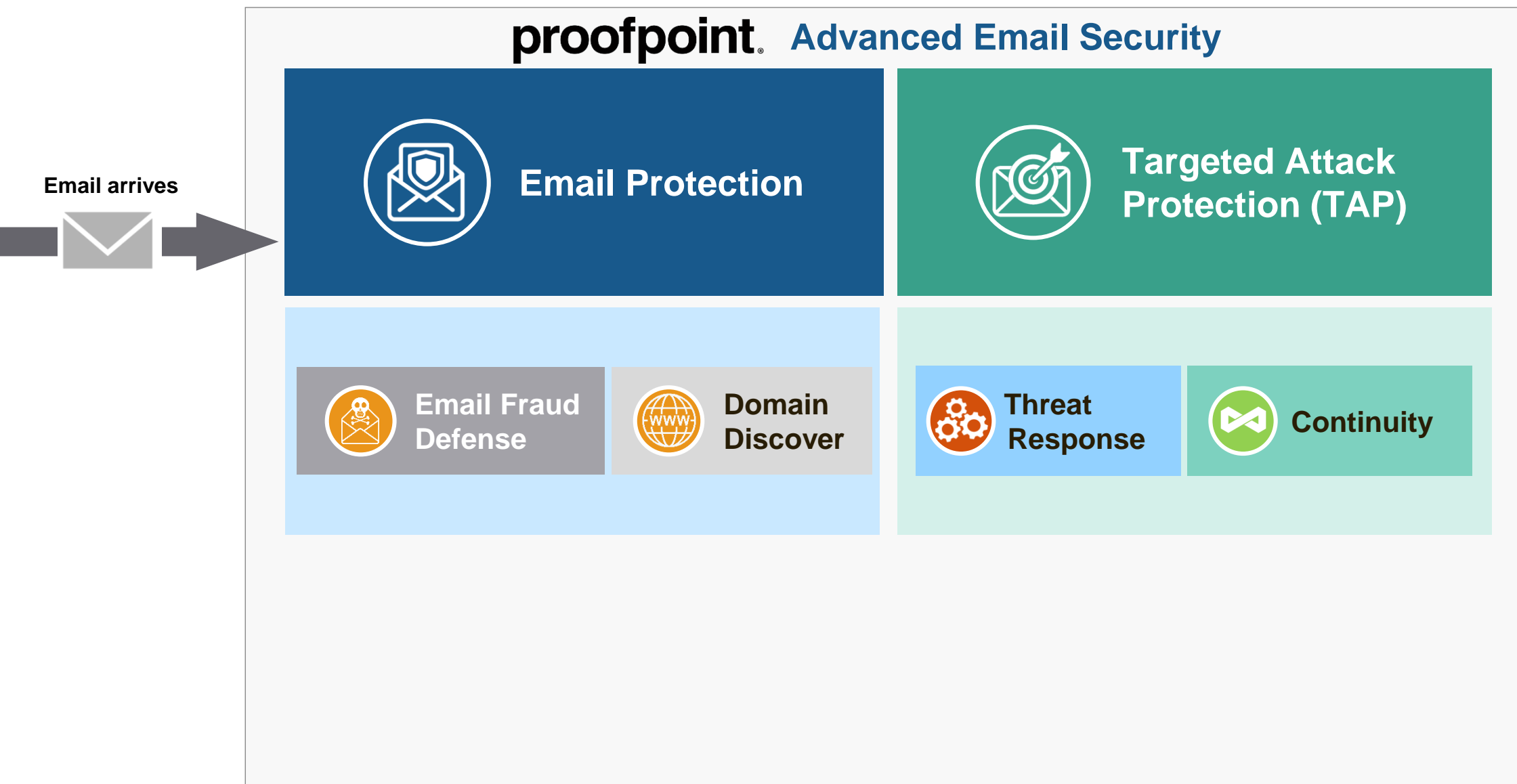
# Extending the Email Franchise



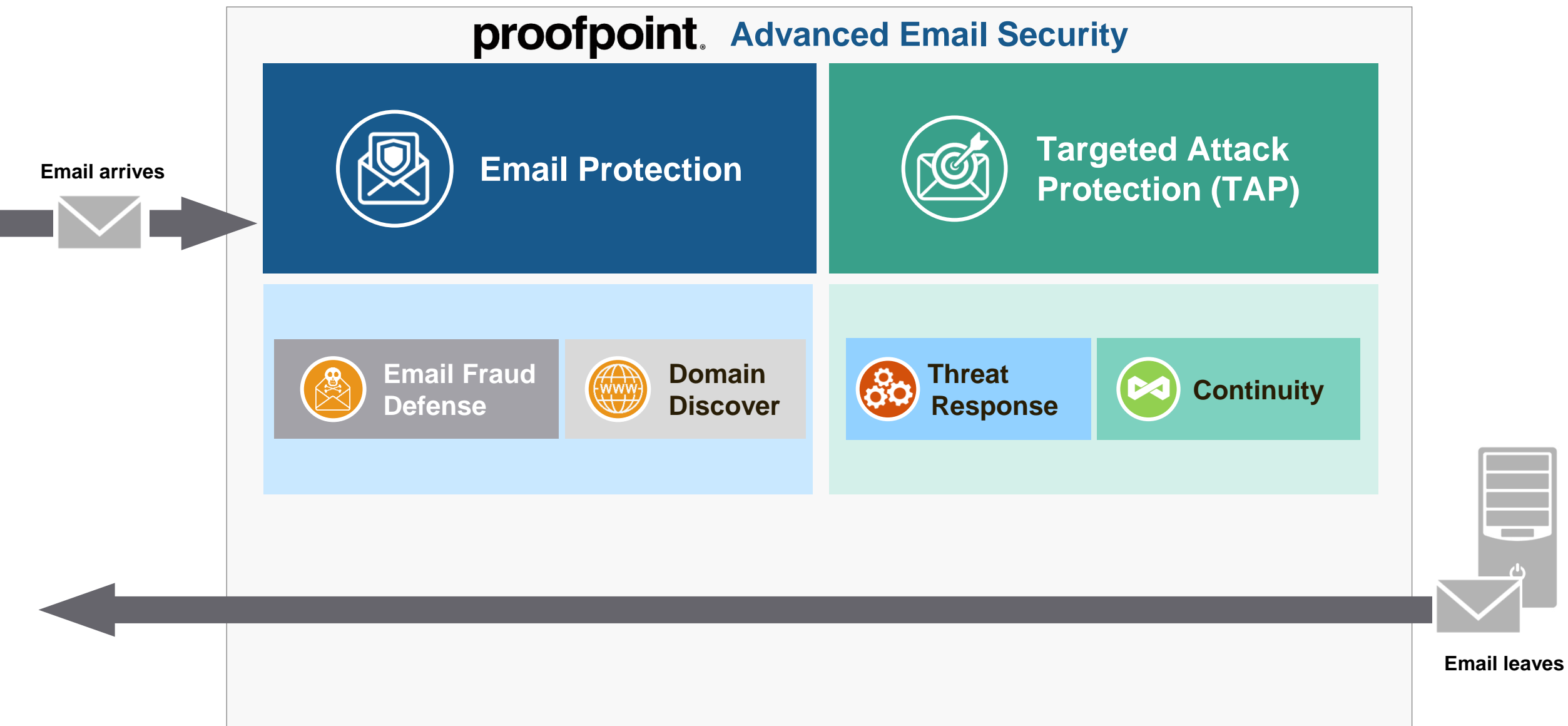
# Extending the Email Franchise



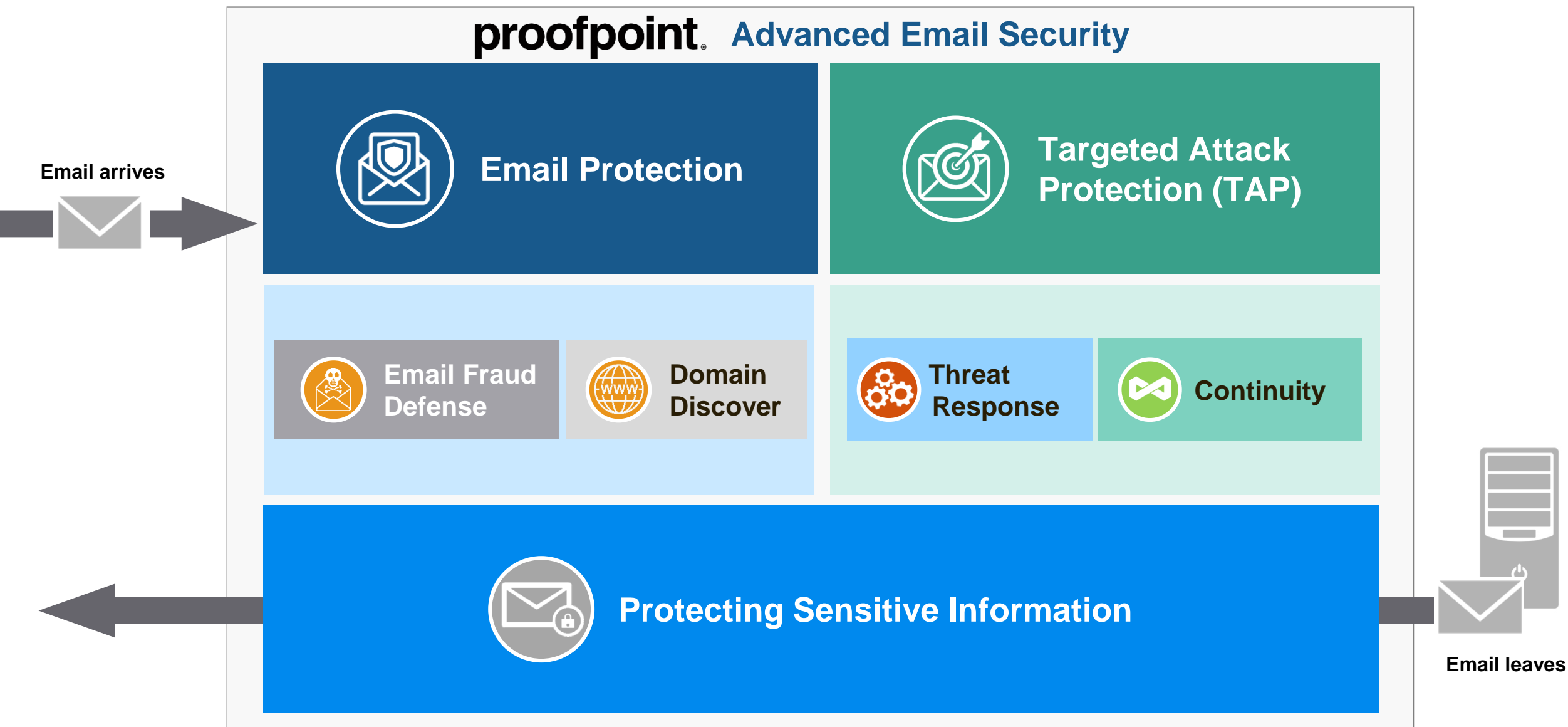
# Extending the Email Franchise



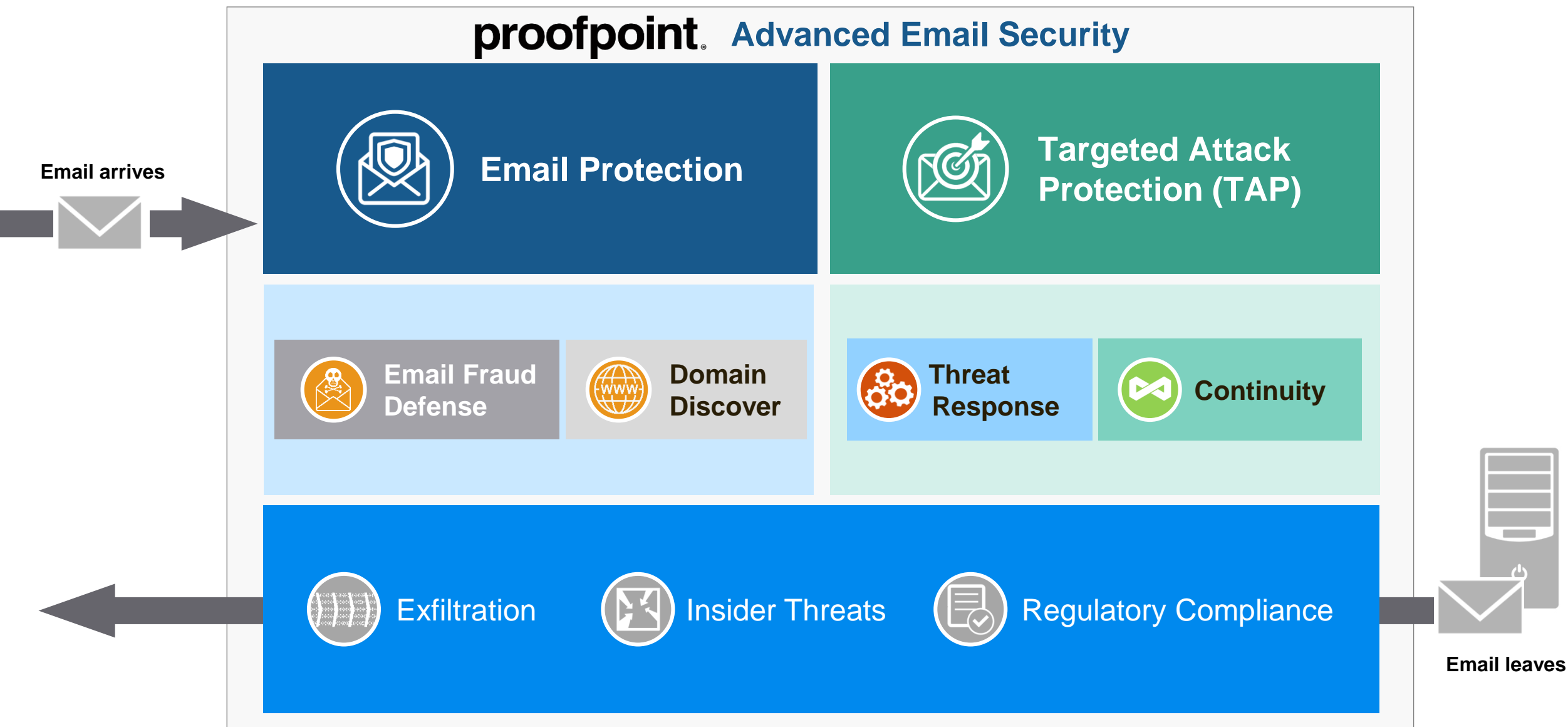
# Extending the Email Franchise



# Extending the Email Franchise

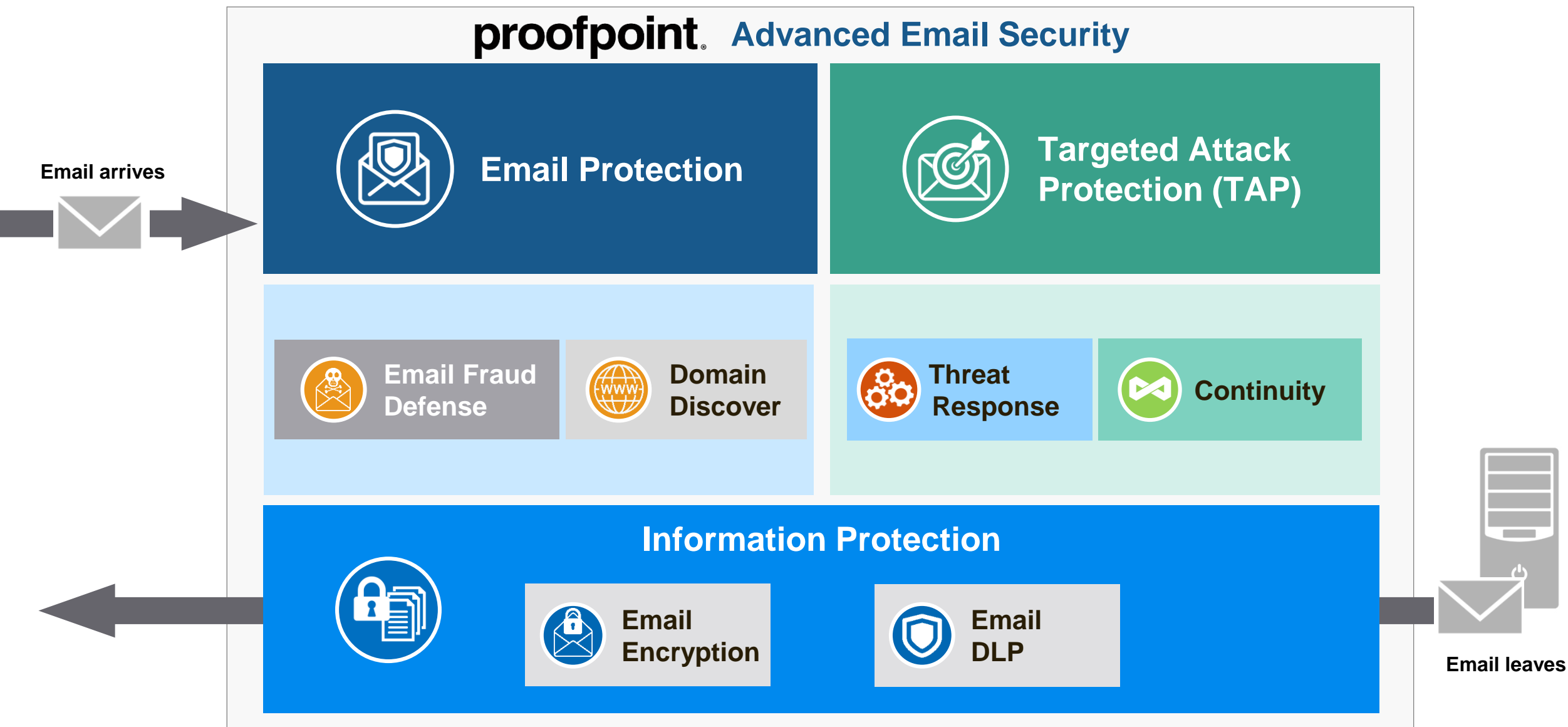


# Extending the Email Franchise





# Extending the Email Franchise



# Email Protection: Continued Leadership and Innovation



**Best in Class  
Effectiveness**



**Rich, Actionable  
Intelligence**



**User Experience  
and Flexibility**

**Visibility to Global Threat  
Campaigns at F1000  
Companies**



**Advanced Machine Learning  
with Content, Context,  
Behavior Analysis**



**Granular Filtering, Custom  
Configuration and Control**



**Rich Reporting, Visualization  
and Ecosystem Integration**





# Dramatic Increase in Advanced Threats

## New Ransomware Increased



**4.3X**

Q1 2016 vs. Q1 2017

## Malicious URLs



**90%**

Credential  
Phishing Attacks

## Malicious Messages



**250%**

Q1 2017 vs. Q2 2017

Source: 2017 Human Factor Report, Proofpoint Threat Research

# Targeted Attack Protection: Pulling Ahead With Industry Leading Solution



**Powerful Advanced Threat  
Protection**

**Swift Response  
Against New Vectors**

**Superior Threat Insights  
and Visibility**

**Discern Broad Campaigns  
and Targeted Attacks**



**Identify Targeted, Impacted  
and At-Risk Users**



**Inspect All Attachments,  
URLs at Delivery and at Click**



**Detailed Forensics Insights  
and Reporting**





# Rapid Remediation with Threat Response

**Rapid  
Detection**

**Automated  
Remediation**

**Clear  
Reporting**

Automate Collection  
and Prioritization via  
TAP Integration



Confirm Infections  
via Forensics  
Across Organization



Easy, Insightful  
Drill-down on  
Threat, Origin, Targets



Benefit from  
Built-in and  
Custom Views



# Continuity: Email Always Available



**Always-on**

**Anywhere, Any Device**

**Seamless User Experience**

**Full Access to  
Emails, Contacts, Calendar**



**Automatic Cutover,  
Restoration and Syncing**



**Hassle-free  
Cloud-based Solution**



**Extensive  
Multi-Platform Coverage**



# Email Fraud is a Big and Fast Growing Problem



## Cost of Email Fraud



**\$5.3B**

40,203 companies

## Consumer Phishing Campaigns



**150%**

YoY Increase

## Domain Spoofing Attacks



**2/3**

of all imposter emails

Source: SANA Institute, FBI, APWG, Proofpoint Threat Research

# Everyone is Targeted



## All Organizations – Large and Small

Finance boss at Te Wananga o Aotearoa falls for 'whaling' scam

**Belgian Bank Loses €70 Million to Classic CEO Fraud Social Engineering Trick**

**Cybercriminals Steal \$54 Million from Aircraft Parts Maker**

**07 Tech Firm Ubiquiti Suffers \$46M Cyberheist**

AUG 15



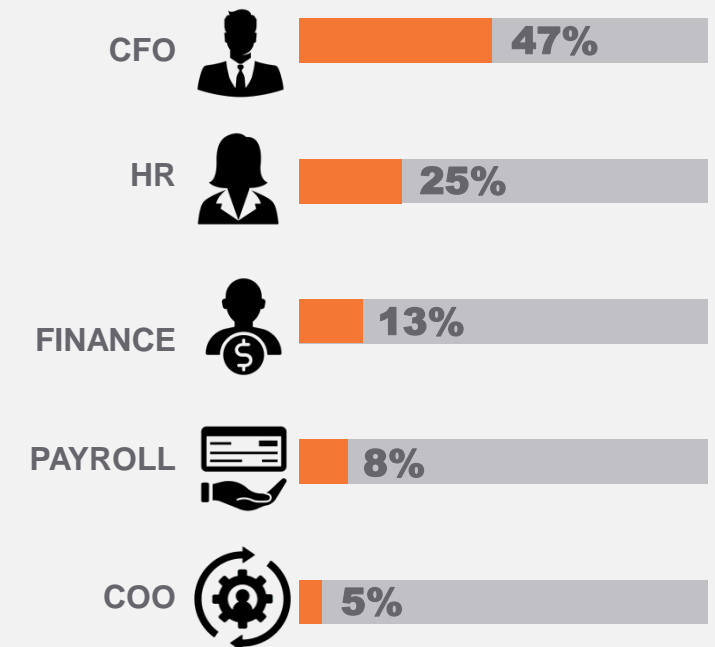
Networking firm **Ubiquiti Networks Inc.** disclosed this week that cyber thieves received \$46.7 million using an increasingly common scam in which crooks...

## All Industries

### Average BEC Attacks Per Company Targeted

VERTICAL	2017-Q2
Manufacturing	44
Telecommunications	39
Technology	38
Energy/Utilities	31
Business Services	29
Automotive	26
Financial Services	23
Retail	22
Transportation	20
Healthcare	19
Entertainment/Media	17

## All Functions



Source: Proofpoint Threat Research



# Comprehensive Solution for Email Fraud



## Email Protection



**Configuration**  
Gateway  
Rules



**Detection**  
Impostor  
Classifier

## Email Fraud Defense



**Authentication**  
Complete  
DMARC Solution

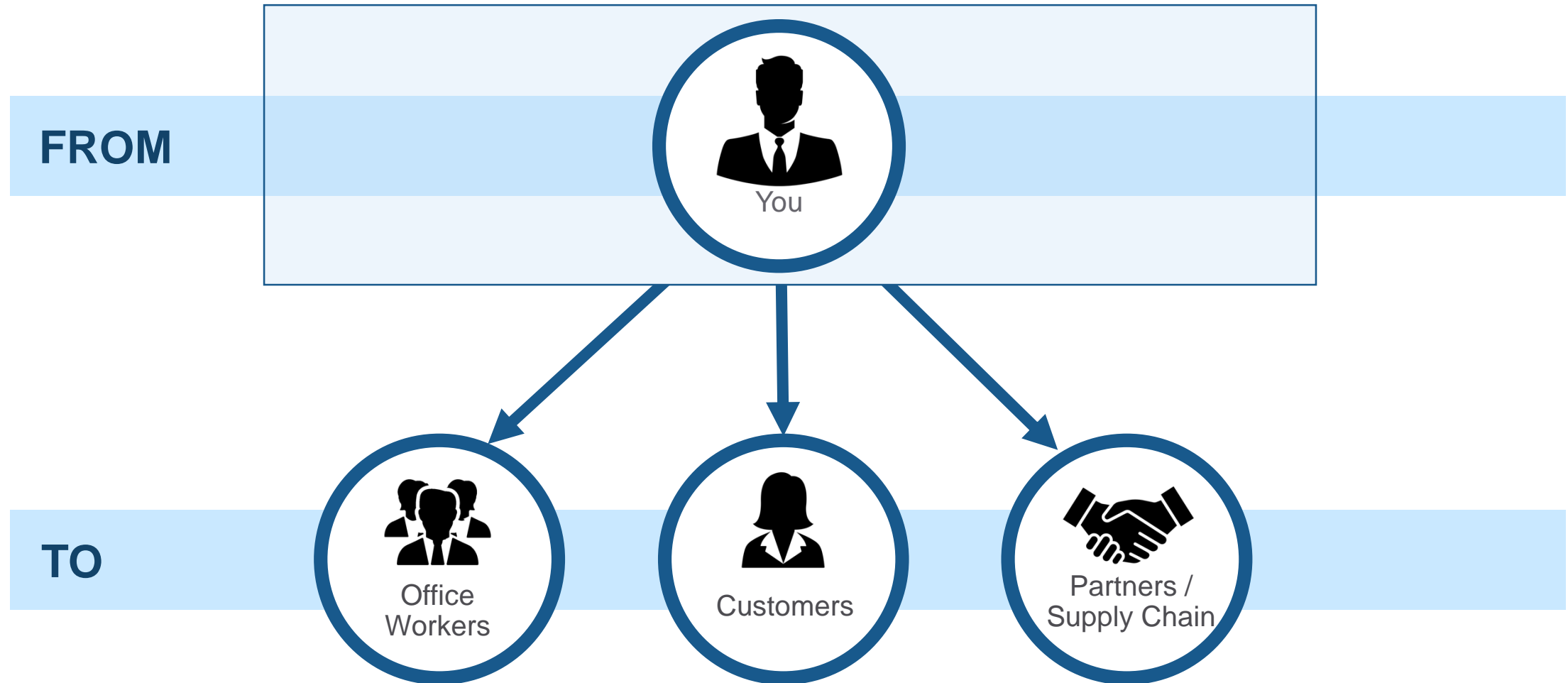
## Domain Discover



**Look Alike**  
Domain  
Protection

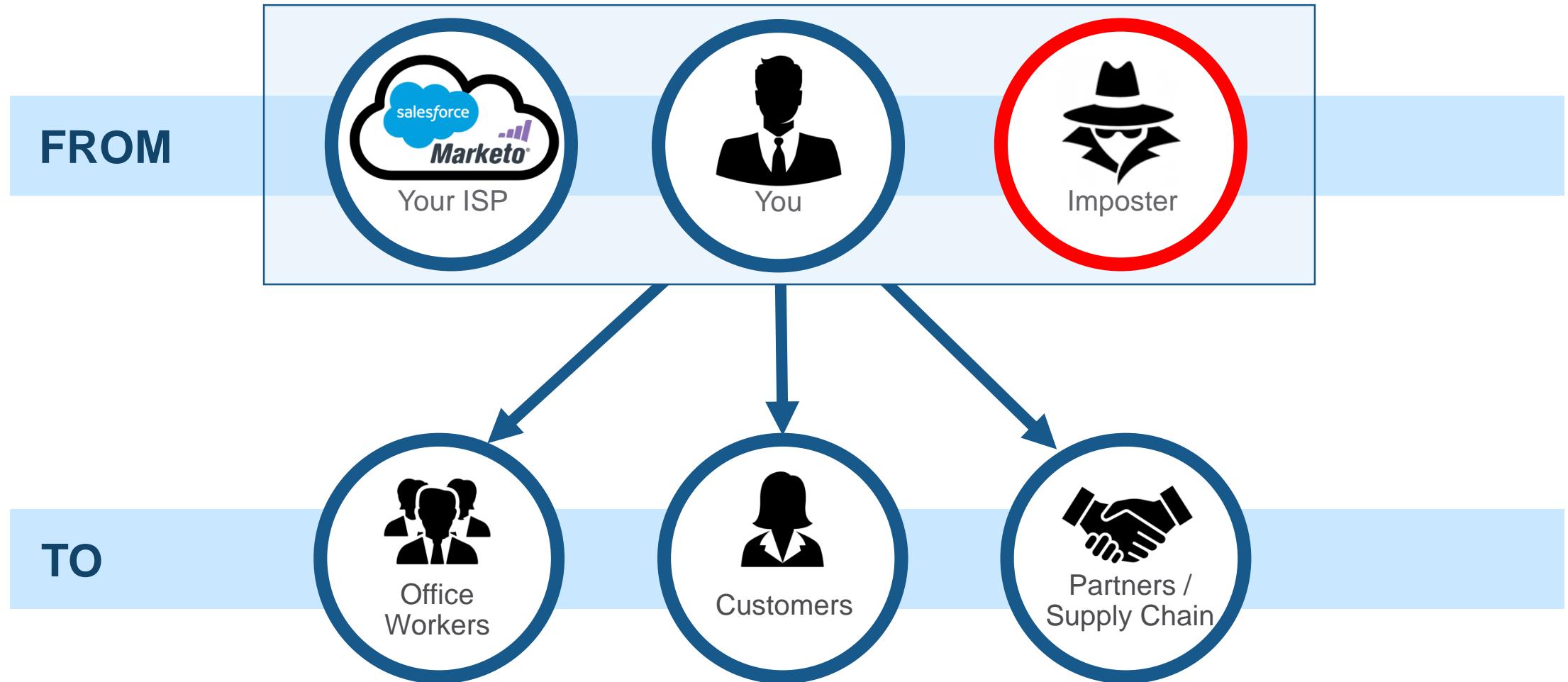


# Need to Have 360° Visibility

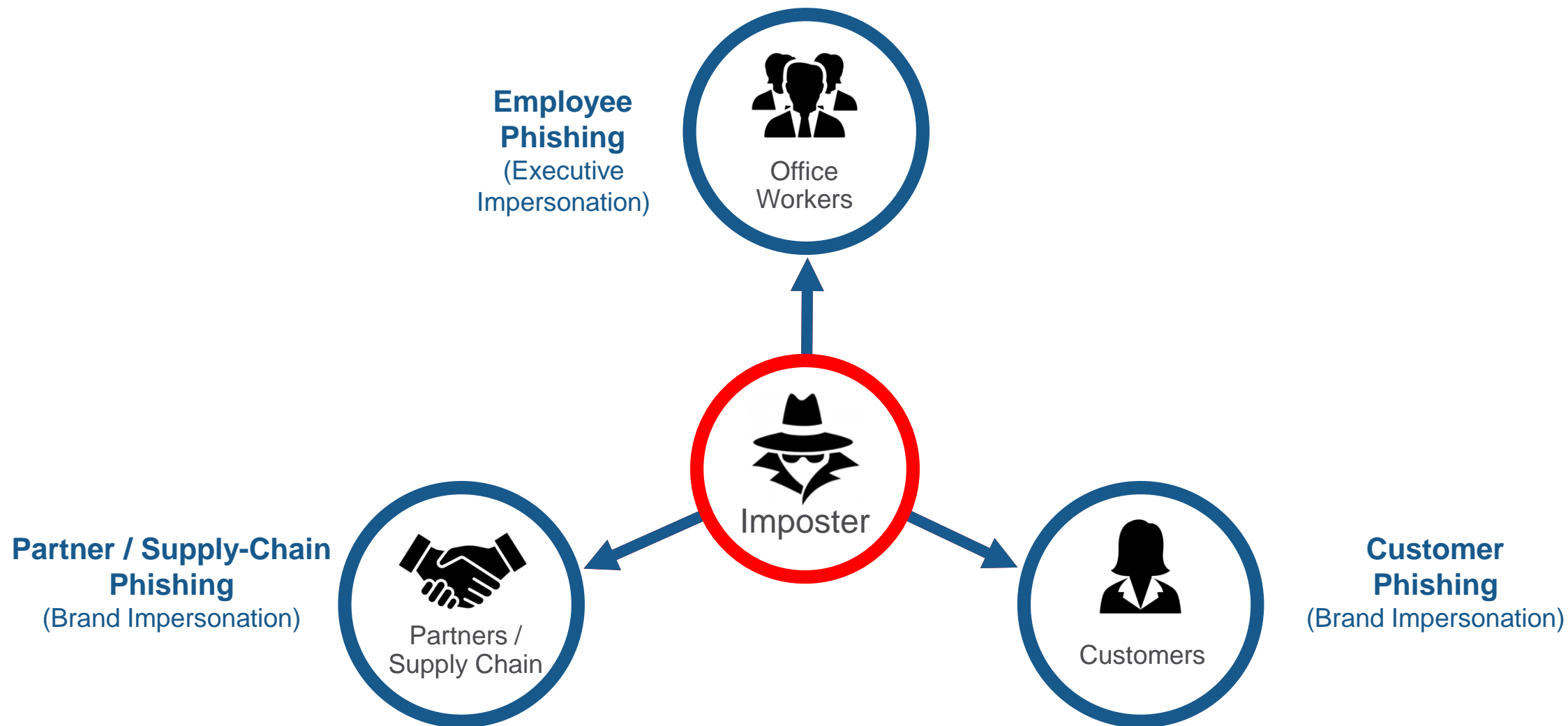




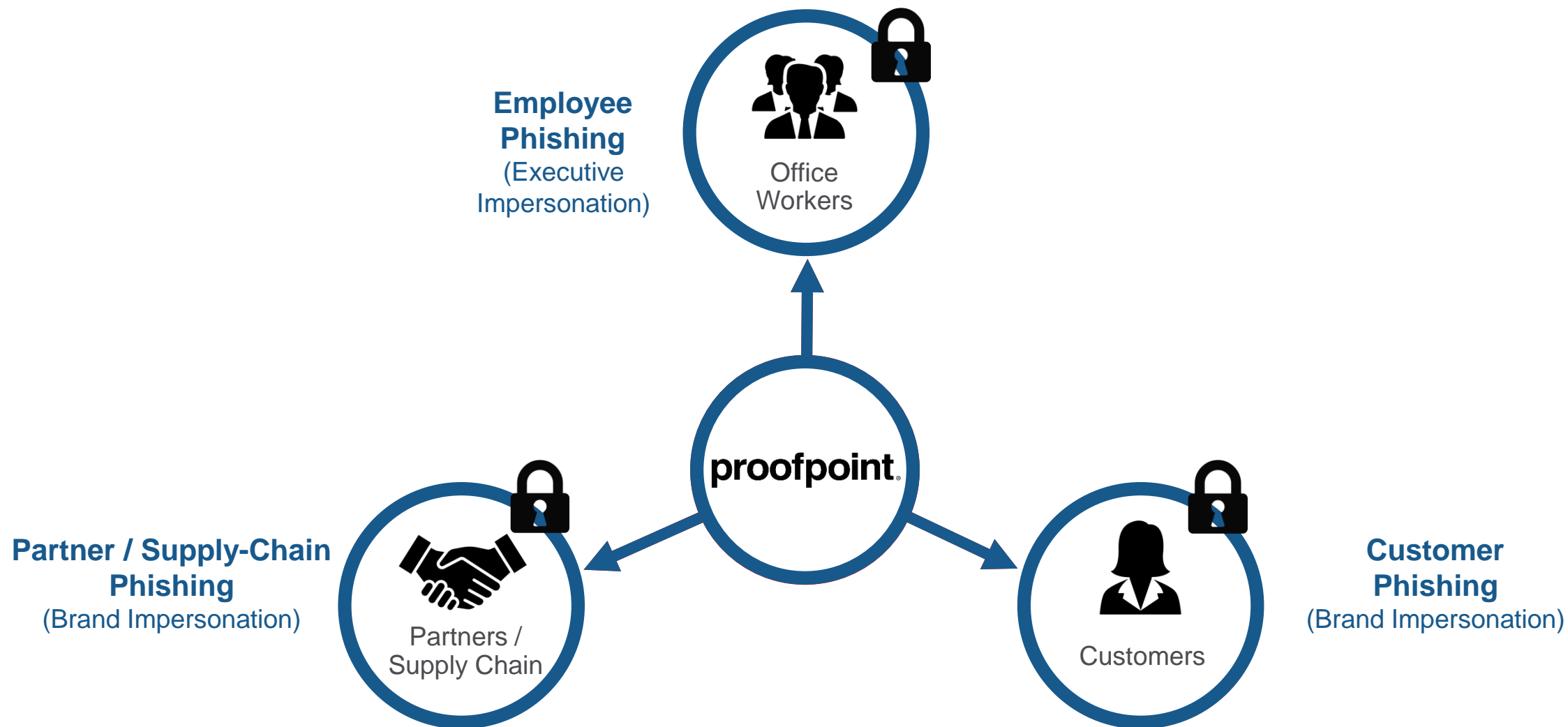
# Need to Have 360° Visibility



# EFD Provides Full Email Ecosystem Protection



# EFD Provides Full Email Ecosystem Protection



# Email Fraud Defense: Rapid Growth Propelled by Best in Class Solution

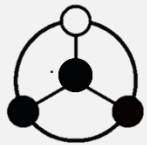


**Intelligent Authentication**

**Full Ecosystem Protection**

**Robust Management**

**Gain 360° Visibility**



**Minimize Implementation  
Risks with Rich Sender  
Intelligence**



**Smart Policy Enforcement via  
Email Gateway Integration**



**Stay Ahead in a  
Dynamic Environment  
with Managed Services**



Source: SC Awards 2017, Best Fraud Prevention Solution



# Protecting Information Matters

## Massive Increase in W2 Scams

**3,400%**

Q1 2016  
vs. 2017

## Huge Costs to Organizations

**\$3.6M**

Avg. cost  
of data breach

## Strict Regulatory Environment

Up to  
**4%**

of Global Rev in  
GDPR Fines

Source: Ponemon Cost of Data Breach Study 2017, Proofpoint Threat Research

# Email DLP: Accelerating Momentum with an Integrated Solution



**Rapid Results**

**No Blind Spots**

**Smart Management**

Accurately Detect Exfiltration  
of Full Files or Data Fragments



Deploy Quickly with a  
Cloud-native Solution



Rich Pre-built Rules  
and Dictionaries



Achieve Compliance for  
HIPAA, GDPR etc.







# Email Encryption: Take Back Control of Data

End-to-end Protection

Granular Message Control

Enhanced User Experience

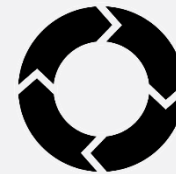
No Prying Eyes Protect with  
Strong Encryption



No Weak Links with  
Policy-based Automation



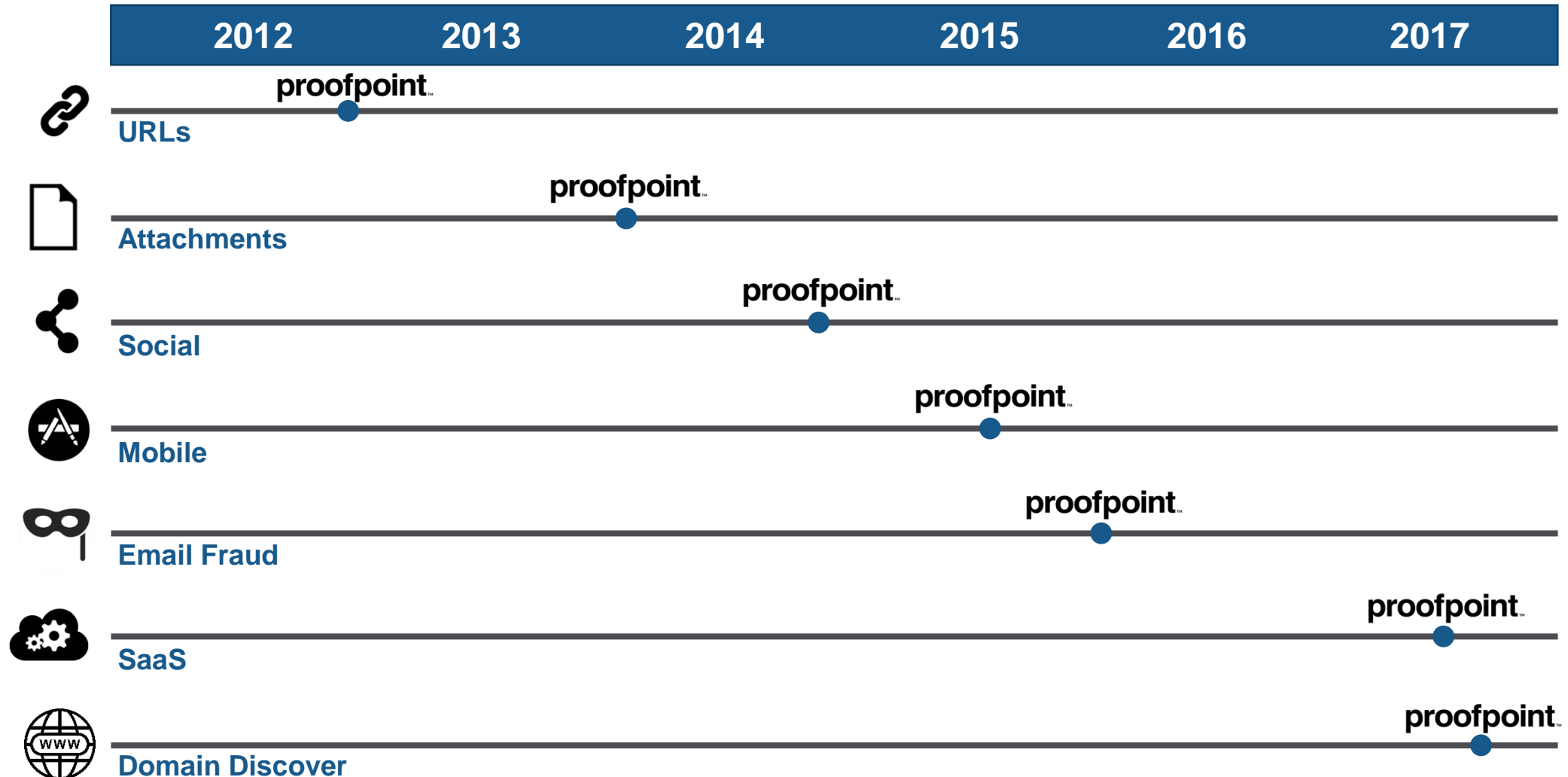
Full Life Cycle Solution Expire  
Emails, Keys via Policies



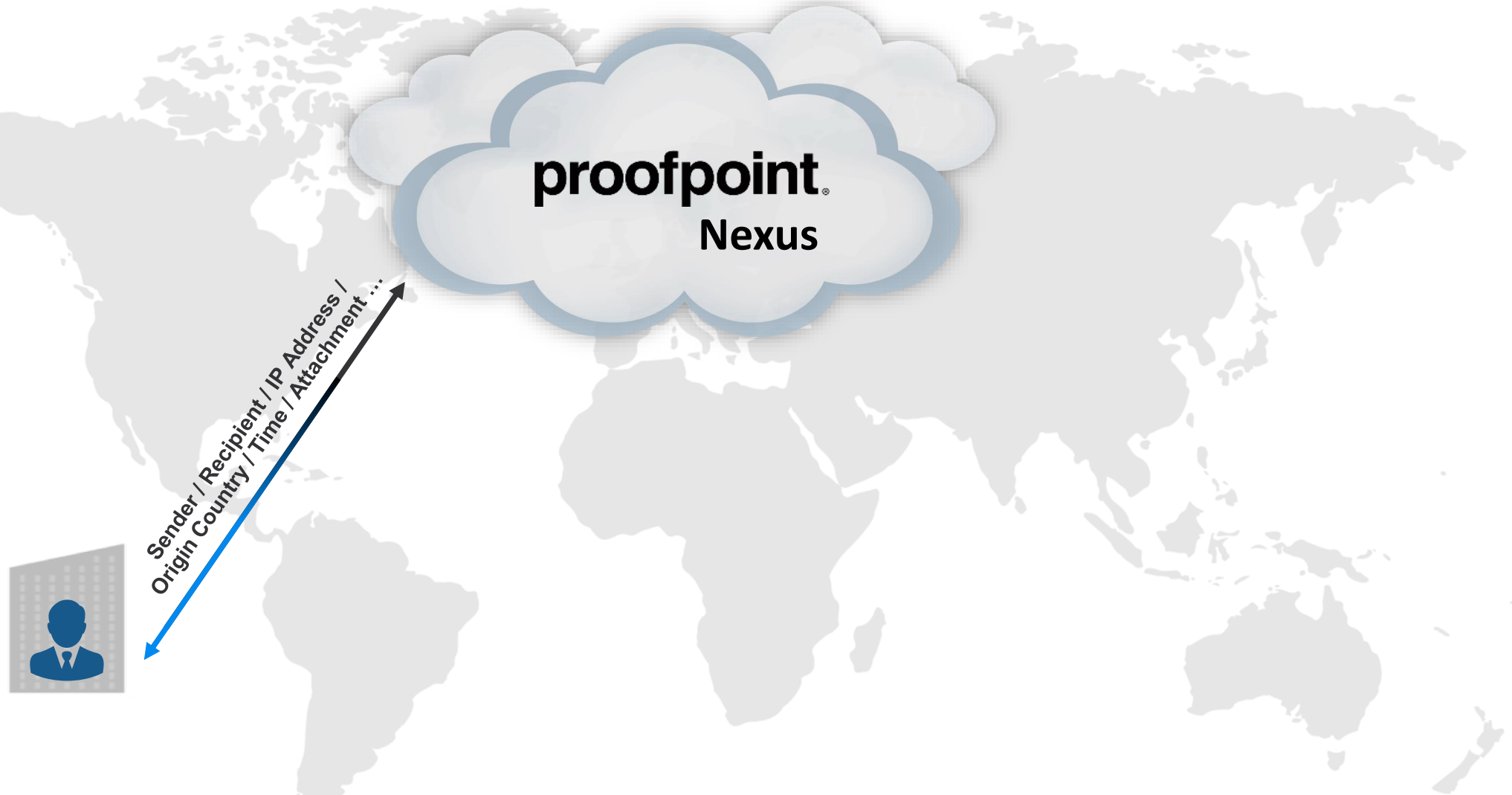
Simplified Key Management  
Service by Proofpoint



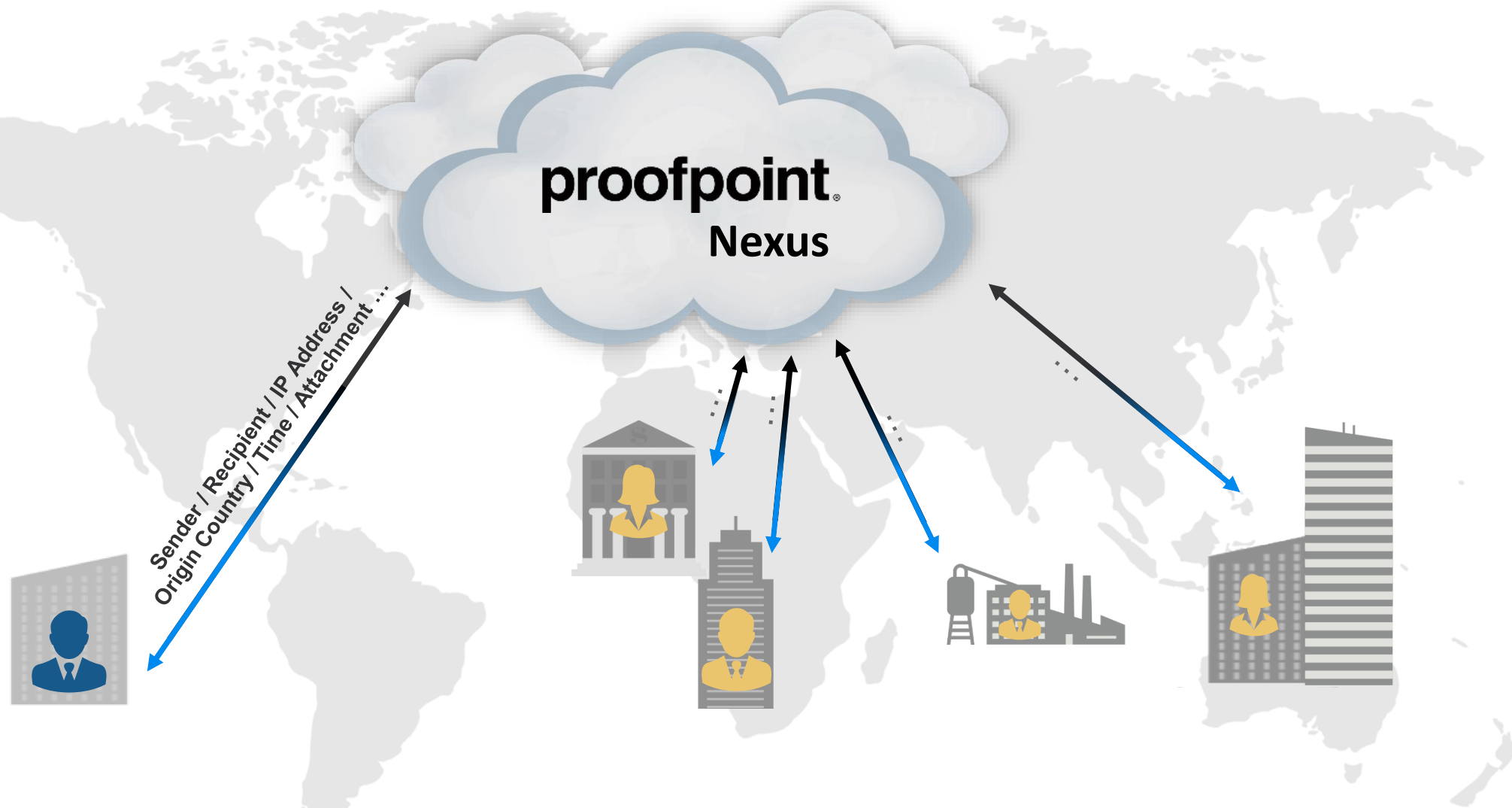
# Leading with Innovation



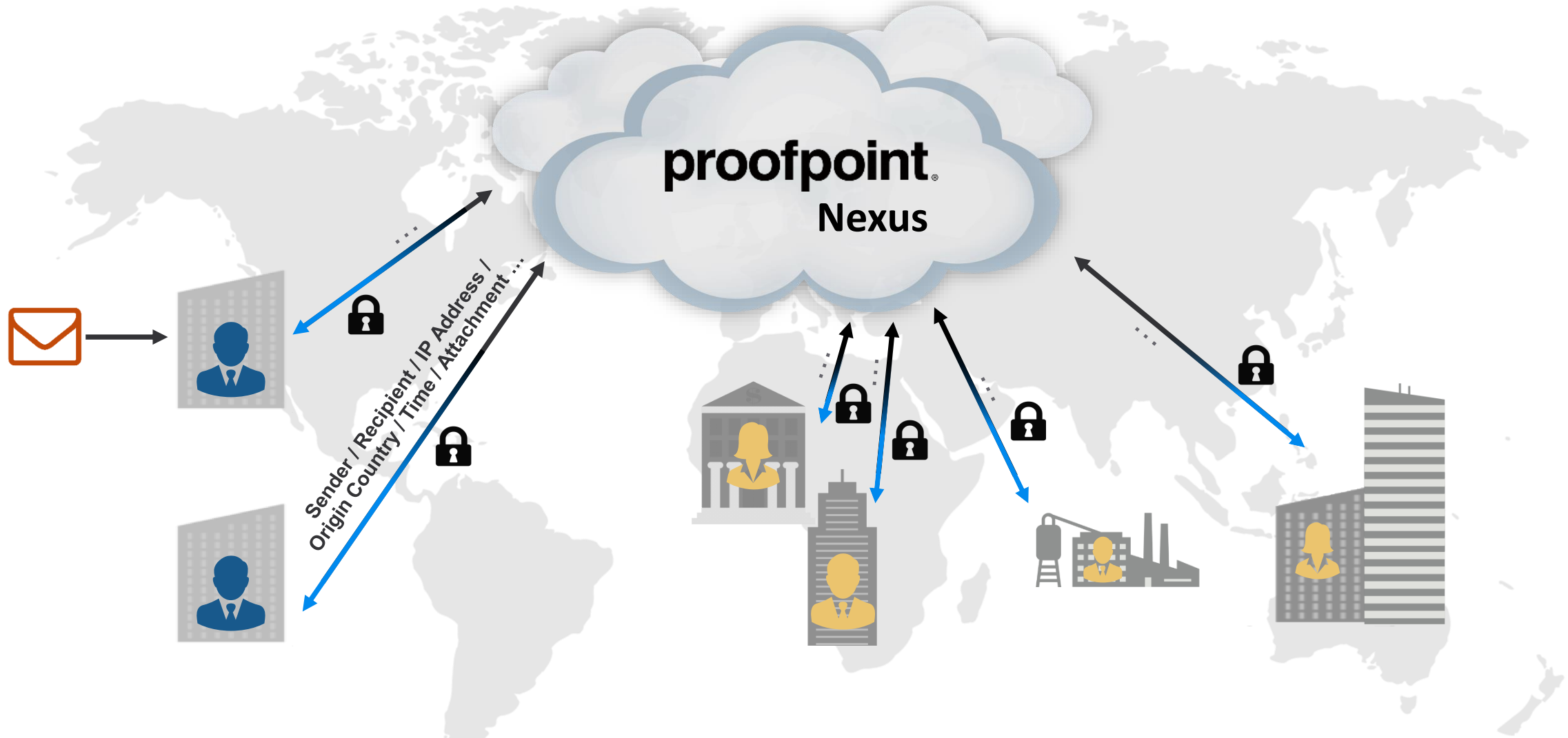
# Network Effect Benefits All Our Customers



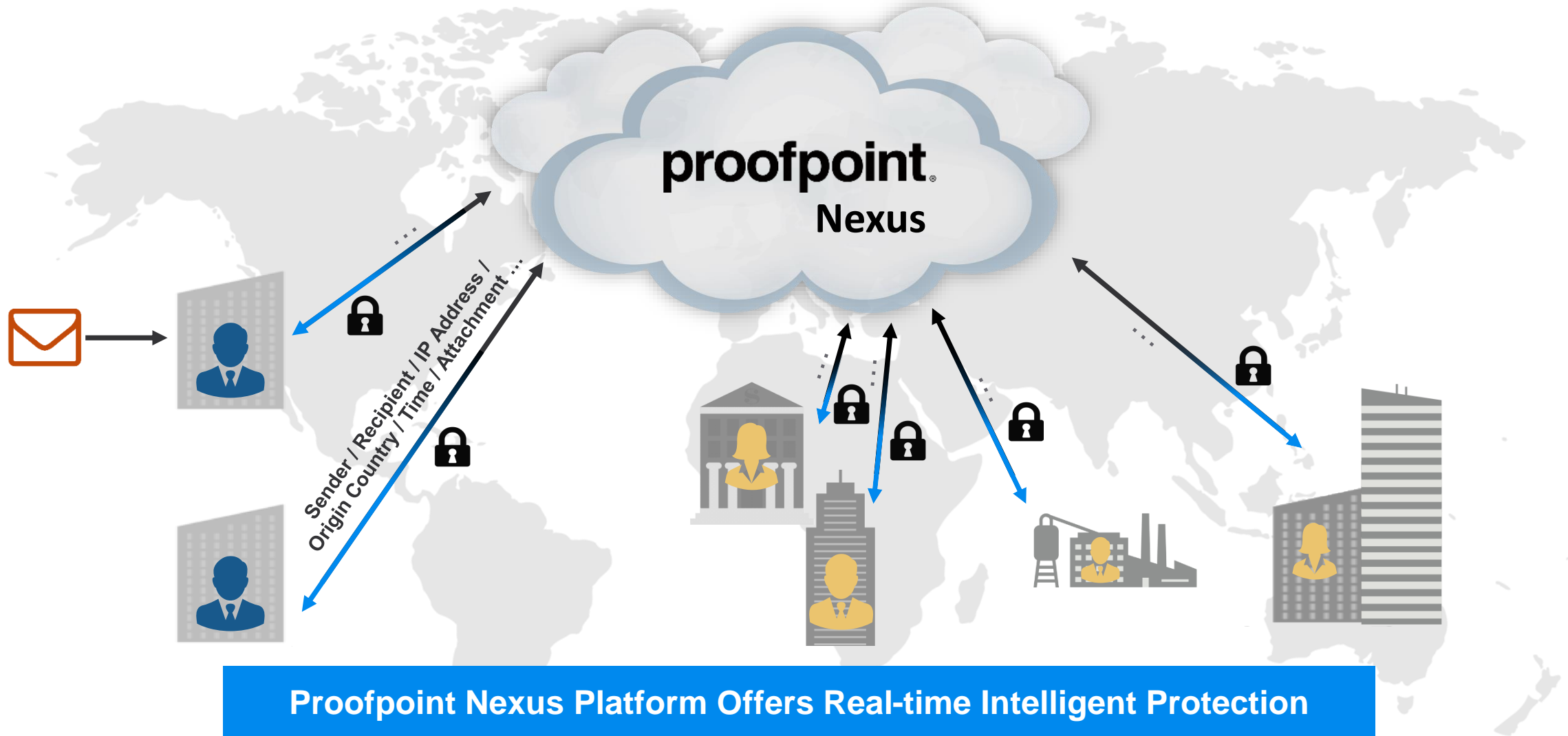
# Network Effect Benefits All Our Customers



# Network Effect Benefits All Our Customers



# Network Effect Benefits All Our Customers



**proofpoint**<sup>TM</sup>





**proofpoint.**

# Extending the TAP Franchise

David Knight

EVP/GM, Threat Systems Group



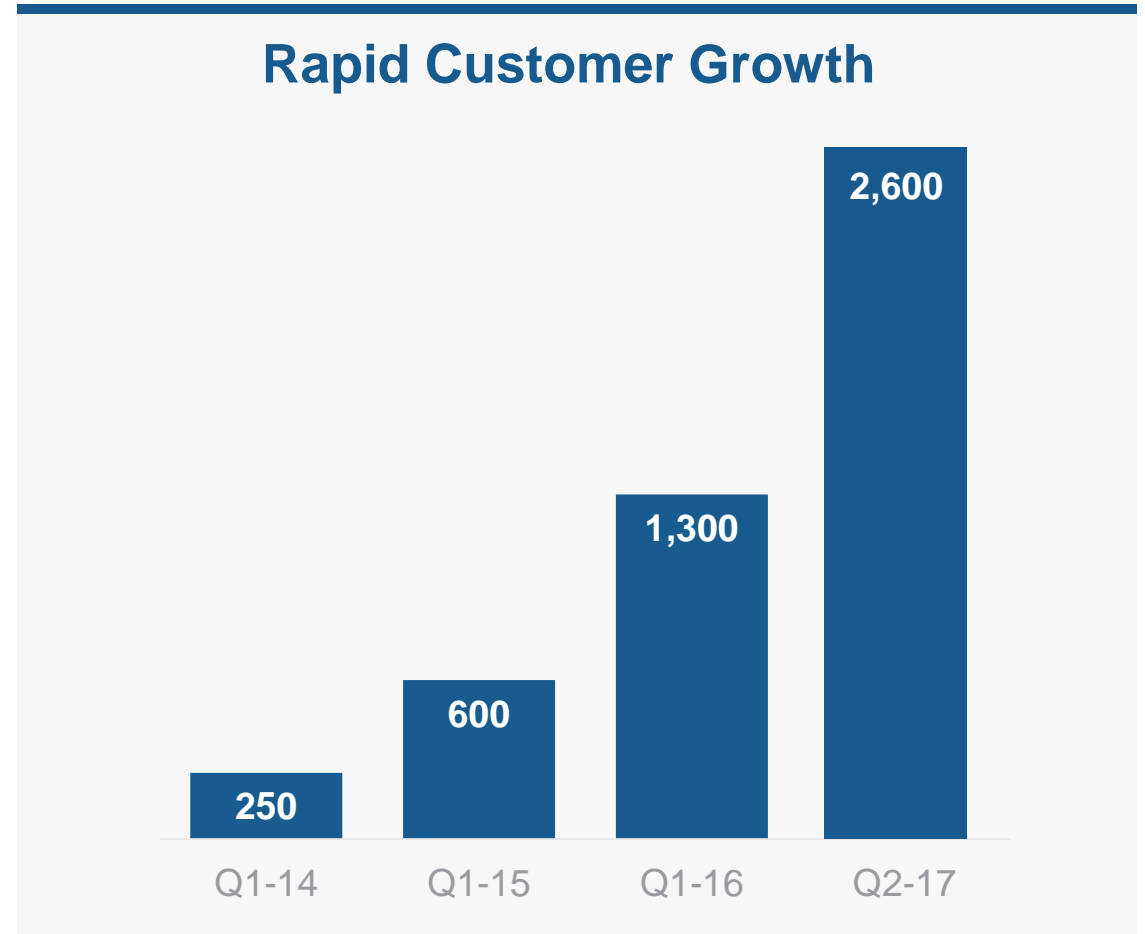
**ANALYST DAY 2017**

© 2017 Proofpoint, Inc.. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners



# TAP Continues to Drive Growth

- 2,600 customers
- Leading brands in key verticals including: financial services, healthcare, retail, high-tech, aerospace and defense, telecommunications and energy
- Growing international footprint
- Traction with the most sophisticated security teams in the world and mid-market companies with small teams



# TAP—Why We Win

## Unique Visibility

See more enterprise attacks than anyone and we're extending this lead

See it first—99%+ never make it downstream

## Unmatched Effectiveness

Powerful detection ensemble

Malware and credential theft detection

## Rich Threat Intelligence

Targets and methods

Campaign, malware and actor attribution

Targeting and peer comparisons

Analyst curated intelligence feed

## Cloud-Speed Innovation

Continuous development of new capabilities

Rapid adoption of new technologies

Immediate deployment across all customers

# A Few Recent TAP Innovations

Dedicated threat intelligence  
extraction environment



Malware family  
attribution and reporting



Global and vertical  
industry benchmarking



Second-generation real-time,  
machine learning-based  
predictive URL sandboxing

Notable and targeted  
threat identification

Detection enhancements  
too numerous to discuss

# Extending the TAP Franchise

**E-mail Fraud  
Threats**



**SaaS  
Threats**



**Proactive Targeted  
Attack Protection**



**Threat Response  
Automation &  
Orchestration**



# Email Fraud Continues to Grow



**10,000s**

Imposter attacks  
identified during  
Q2 of 2017

**1,500**

Customers  
targeted

**Wide Variety  
of Targets**

Lower in the  
organization  
“Up” not just down  
Across the supply chain

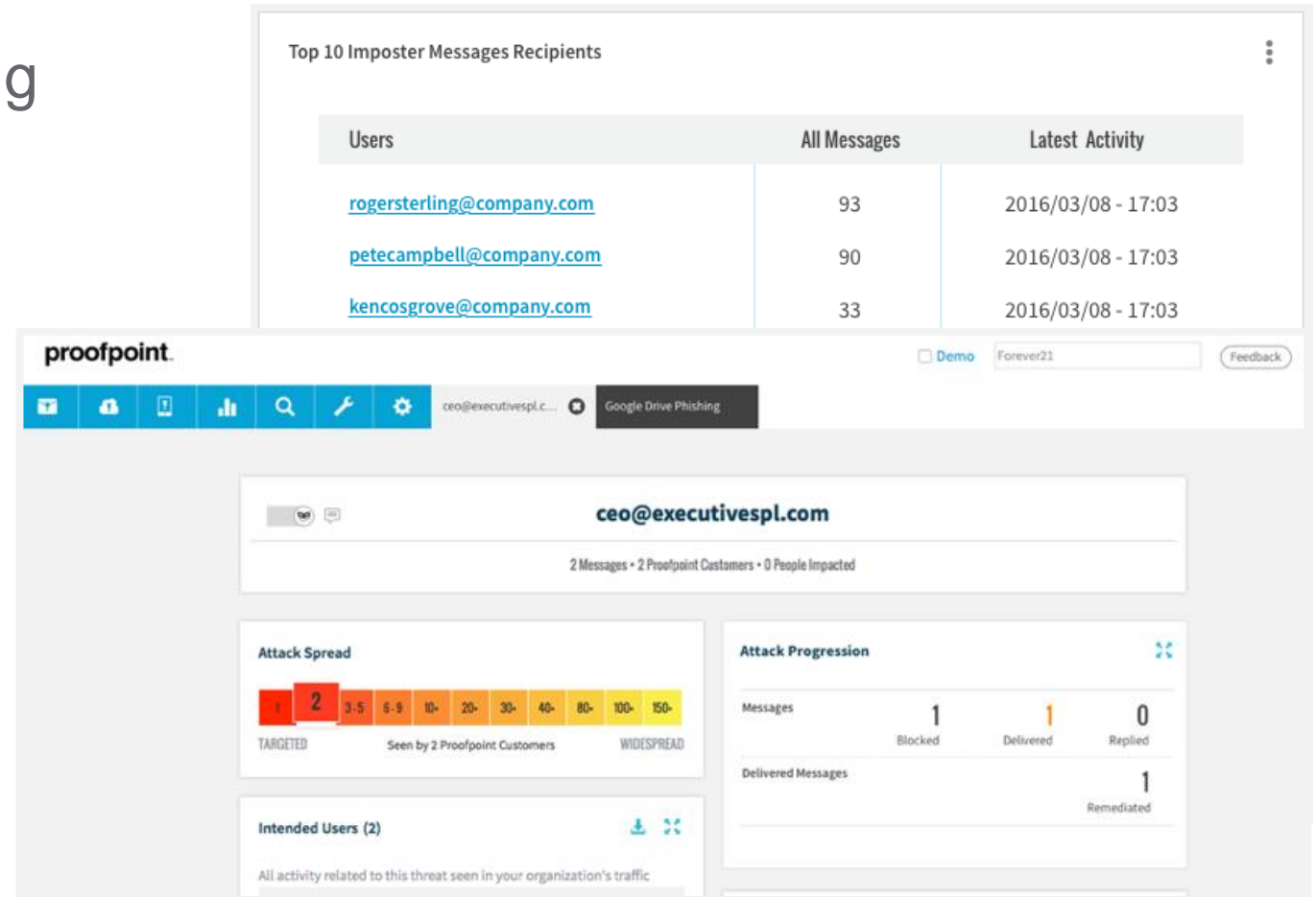
**Look-alike  
Domains**

Many permutations  
detected daily

# TAP Integration: Email Fraud Threats



- Unique visibility into who is being targeted by imposter threats
- Highlighting of targeted execs and malicious domains
- Robust reporting and alerting



# SaaS Adoption Continues to Accelerate

- Average of 15 sanctioned SaaS applications
  - Security is a leading concern
- Creating new threat vectors
  - Malicious attachments shared via SaaS collaboration platforms
  - Malicious resumes via HRMS apps
  - Malicious links in help-desk tickets





# TAP SaaS Defense

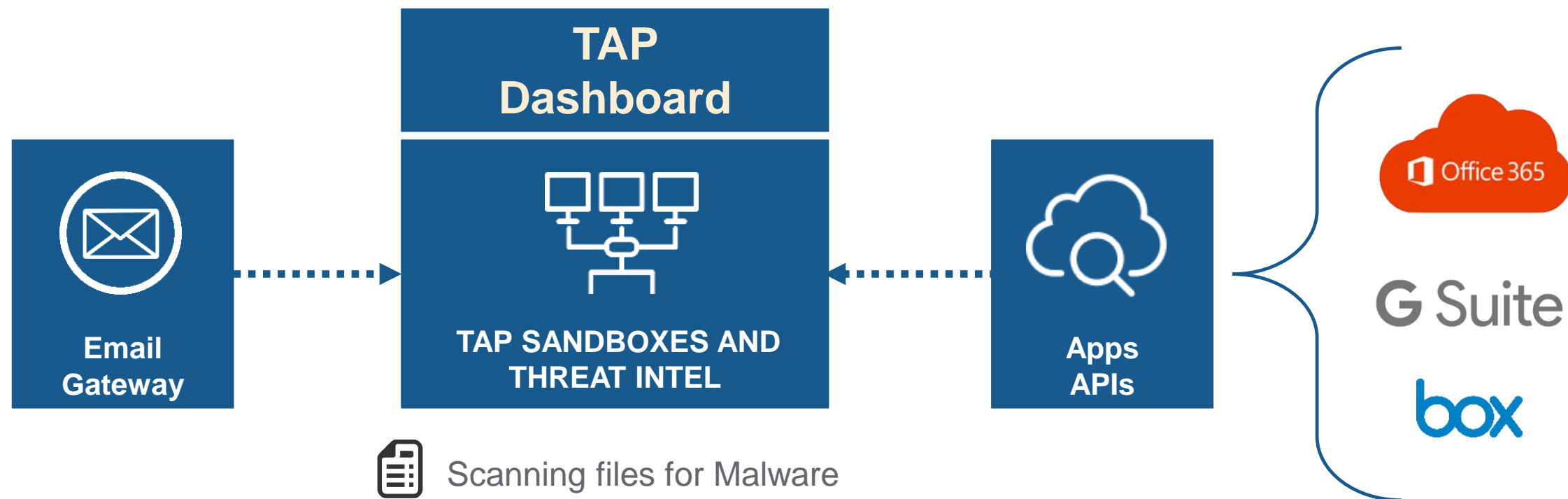
The same proven capabilities from the TAP Email Defense, now available for SaaS Applications

File Defense for O365 OneDrive, O365 SharePoint, G-Suite Drive, Box

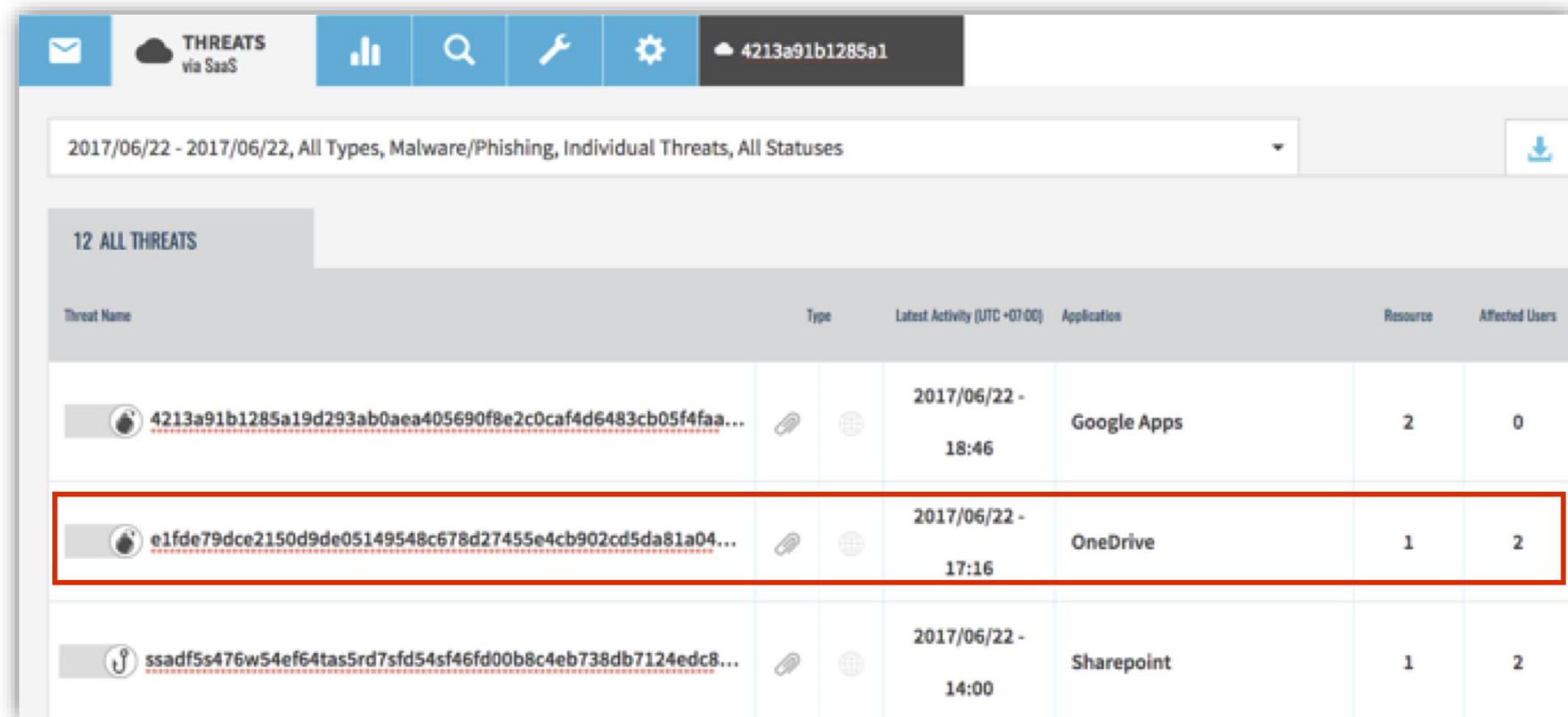
- Leverages TAP dynamic malware analysis
- Protects externally shared attachments
- Integrated to the TAP Dashboard
- Feeds the Nexus Threat Graph
- Provides powerful data access context for all threats









# TAP SaaS Defense: High Level Architecture



# Integrated Threat Visibility & Intelligence



Threat Name	Type	Latest Activity (UTC +01:00)	Application	Resource	Affected Users
 4213a91b1285a19d293ab0aea405690f8e2c0caf4d6483cb05f4faa...		2017/06/22 - 18:46	Google Apps	2	0
 e1fde79dce2150d9de05149548c678d27455e4cb902cd5da81a04...		2017/06/22 - 17:16	OneDrive	1	2
 ssadf5s476w54ef64tas5rd7sfd54sf46fd00b8c4eb738db7124edc8...		2017/06/22 - 14:00	Sharepoint	1	2

# Integrated Threat Visibility & Intelligence

5402cab4f601b...

**5402cab4f601b8b755fb9512dd00036f12ee14c173925ea350a4d4470aa0d383**

2 Resources • 1 Application • 2 People Affected

### File Info

Type	pdf
File Names	Maor_CV_new.pdf
SHA256	5402cab4f601b8b755fb9512dd00036f12ee14c173925ea350a4d4470aa0d383
MD5	eaec52bcf986d395376ababf306c82
Size	205312B

### Resources (2)

This threat is detected in your SaaS applications

Name	Application	Operations	Affected Users	First Activity (UTC +00:00)	Latest Activity (UTC +00:00)
Helen_Smith_Resume_2017.pdf	OneDrive	Add to Folder	ygrindlinger@proofpoint.com	2017/08/28 - 04:15	2017/08/28 - 04:15
Maor_CV_new.pdf	OneDrive	Add to Folder Download File/Folder	tmagid@proofpoint.com	2017/08/28 - 04:15	2017/08/28 - 04:15

### Forensics

Reports Report #1: 2017/08/30 - 04:58 (UTC +00:00) || Windows ... ▼

# Integrated Threat Visibility & Intelligence

The screenshot displays the Proofpoint interface with a top navigation bar containing icons for email, cloud, analytics, search, tools, and settings. The main content area is titled "Resource Details" and shows information for a file named "Maor\_CV\_new.pdf".

**Resource Details**

Application	Microsoft OneDrive	Threats	5402cab4f601b8b755fb9512dd0003...	Affected Users	ygrindlinger@proofpoint.com
Type	PDF	Operations	Add to Folder Download File/Folder		
Location	https://www.hostname.com/document/82				
Owner	hr@proofpoint.com				
Created	2017/08/30 - 06:04 (UTC +00:00)				

**Activity** 2017/08/28 04:15 - 2017/08/28 04:15 (UTC +00:00)

**Download File/Folder** 2017/08/30 - 05:55 Affected Users: 1

Action	Download File/Folder	Source IP	71.2.19.86
Affected Users	ygrindlinger@proofpoint.com	User Agent	Google Chrome

**Add to Folder** 2017/08/30 - 05:55

Filename	Maor_CV_new.pdf	Source IP	66.21.56.112
SHA256	5402cab4f601b8b755fb9512dd00036f12ee14c173925ea350a4d4470aa0d383	User Agent	Mozilla Firefox
Affected Users	None	Originating Agent	maor@badguy.zz

# Rise in Threats Using Look-Alike Domains

- Look-alike domain use growing
  - 1,000s attacks seen during Q2 2017
  - 3x increase over the prior quarter
- Used in highly targeted attacks
  - Email fraud
  - Targeted credential phishing
  - Targeted malware distribution
- Many are quite difficult to spot
- Lots of interesting variations...

## Example Techniques

legitimatecorp.com <-> legltlmatecorp.com  
legitimatecorp.com <-> legitirnatecorp.com  
legitimatecorp.com <-> legiitmatecorp.com  
legitimatecorp.com <-> legitiimate-corp.com  
legitimatecorp.com <-> legitimatecorp-us.com  
legitimatecorp.com <-> legitimatecorp.co  
legitimatecorp.com <-> legitimätecorp.com

# Rise in Threats Using Look-Alike Domains

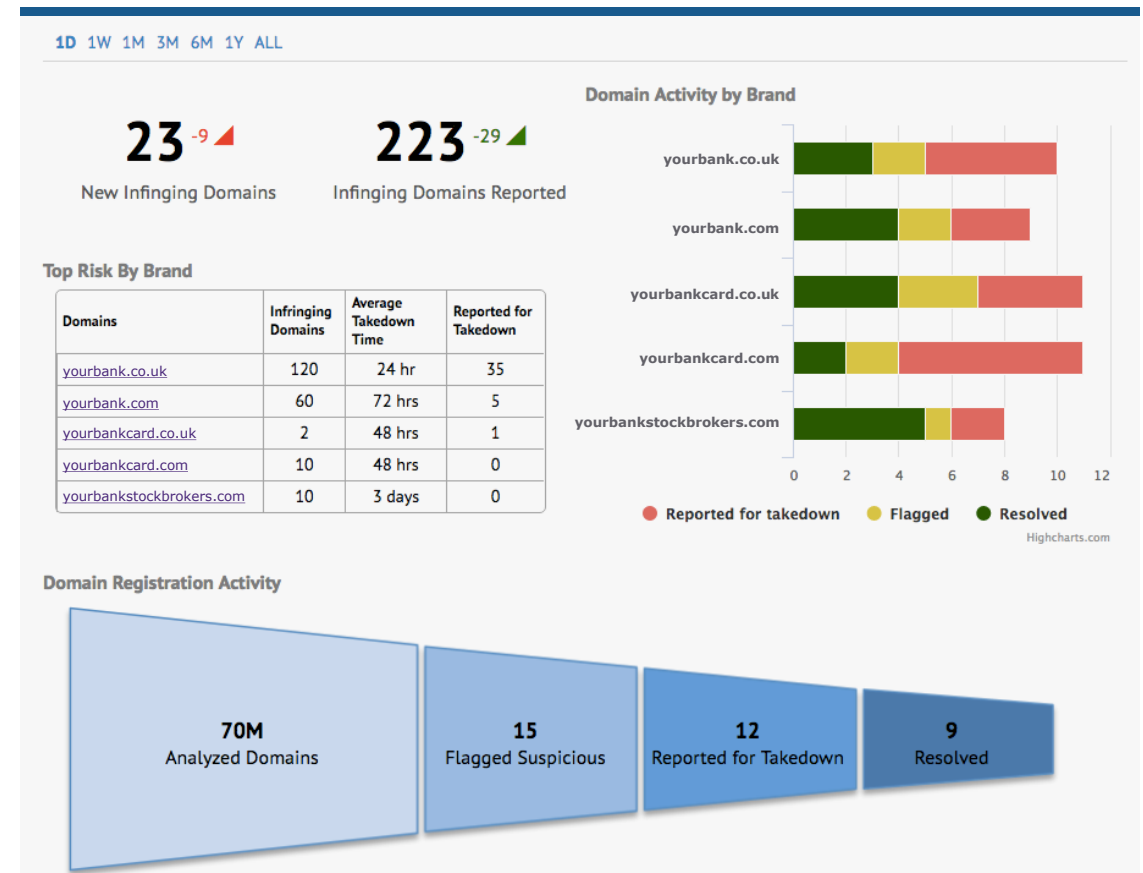
- Look-alike domain use growing
  - 1,000s attacks seen during Q2 2017
  - 3x increase over the prior quarter
- Used in highly targeted attacks
  - Email fraud
  - Targeted credential phishing
  - Targeted malware distribution
- Many are quite difficult to spot
- Lots of interesting variations...

## Example Techniques

legitimatecorp.com <-> legi**l**tmatecorp.com  
legitimatecorp.com <-> legiti**r**matecorp.com  
legitimatecorp.com <-> legi**i**tmatecorp.com  
legitimatecorp.com <-> legiti**i**imate-corp.com  
legitimatecorp.com <-> legitimatecorp-**us**.com  
legitimatecorp.com <-> legitimatecorp.**co**  
legitimatecorp.com <-> legitim**ä**tecorp.com

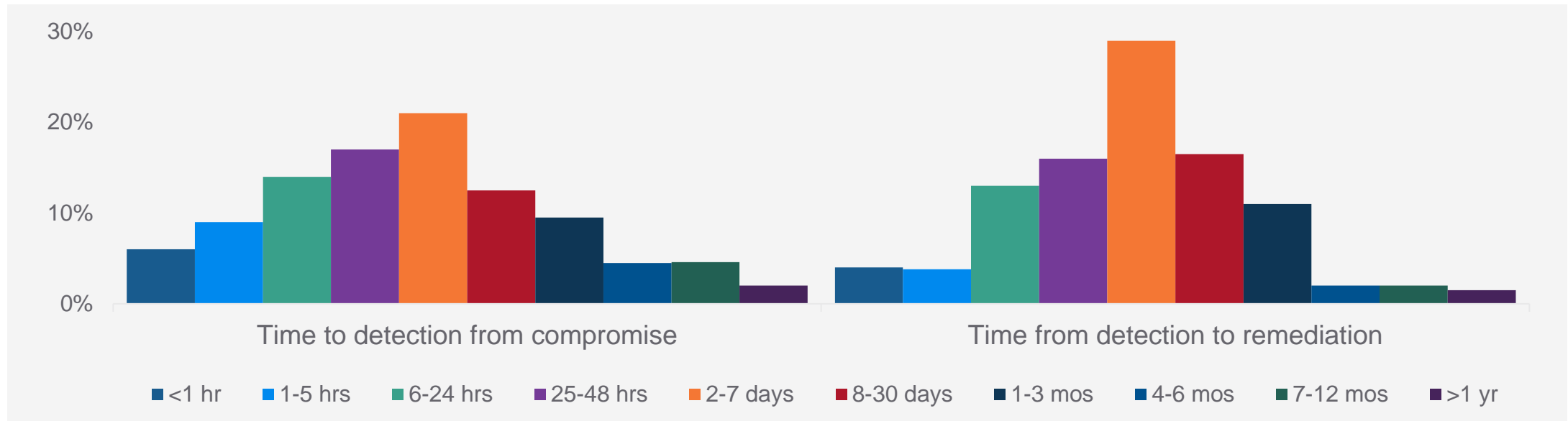
# Proactive Targeted Attack Defense—Domain Discover

- New module provides proactive defense against look alike domains
  - Email fraud attacks
  - Targeted malware and phishing attacks
  - Attacks directed at other Proofpoint customers
  - Attacks directed at consumers
- Proactively finds suspicious domain registrations
- Automatically flags suspicious and risky domains
- Powerful enforcement options
  - Across all Proofpoint customers via Protection & TAP
  - Third party reputation services
  - Third party takedown services



# Threat Response Automation & Orchestration

- Data exfiltration takes minutes, remediation takes hours or days



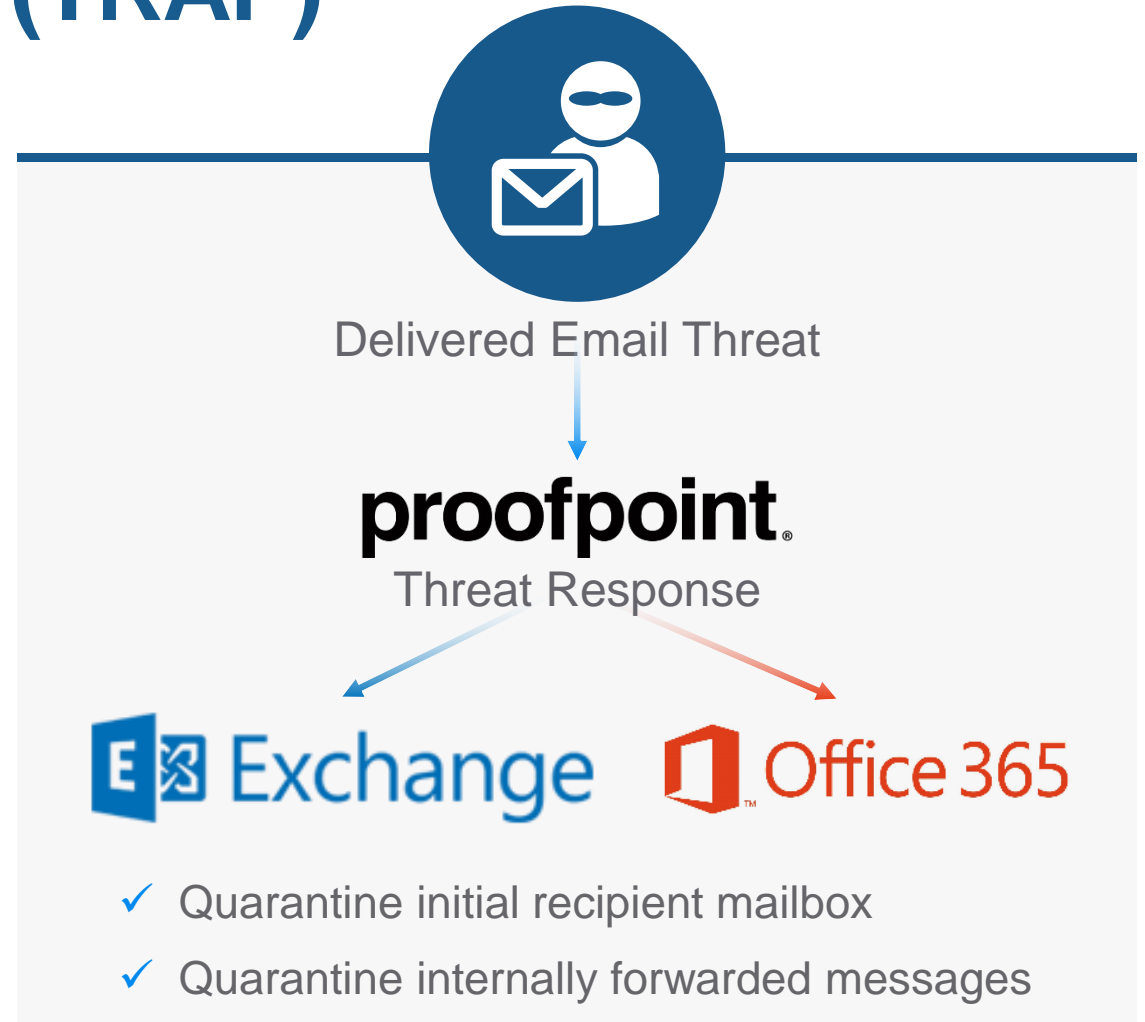
- 65% of organization report staff shortages as the biggest barrier to incident response
  - More than 300,000 open security positions in the US
- TAP provides an efficient entry-point into this market

Source: Sans Institute InfoSec Reading Room - Incident Response Capabilities in 2016: The 2016 SANS Incident Response Survey



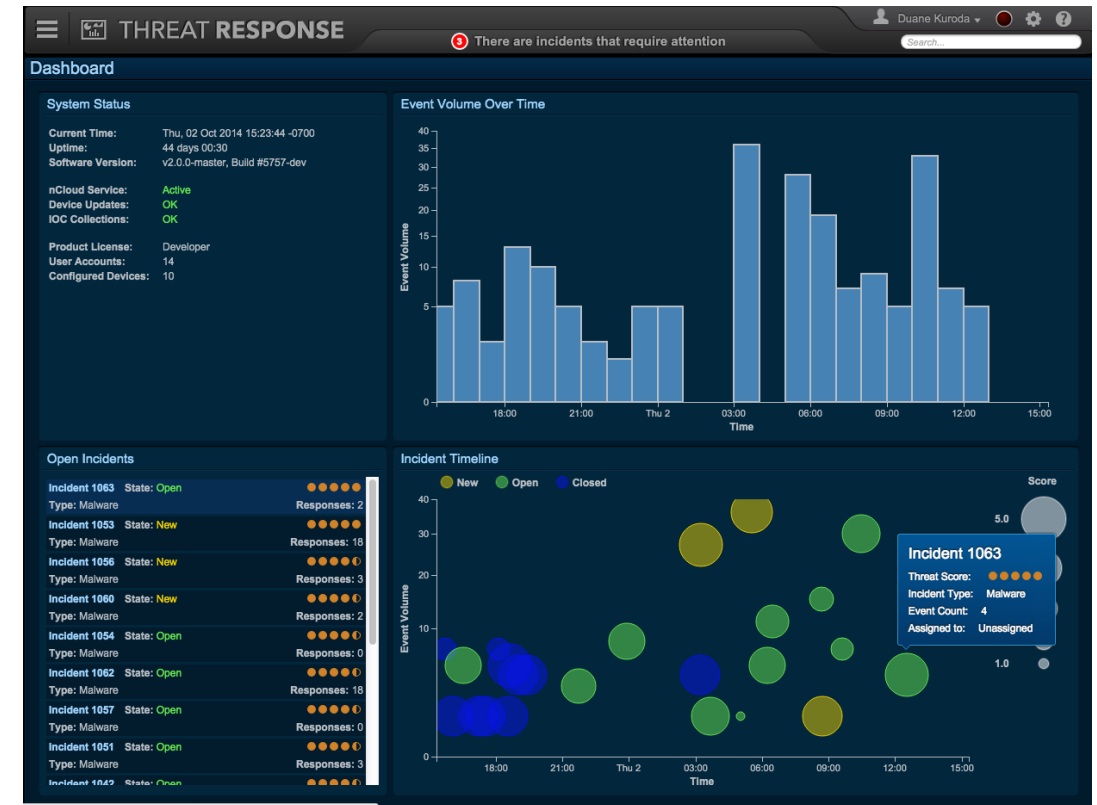
# Threat Response Auto-Pull (TRAP)

- Extends TAP momentum to threat response orchestration segment
  - Automates removal of delivered email threats
  - Provides critical intelligence & user for delivered threats & recipient(s)
  - Integrates with both Proofpoint TAP and third-party alerts
- Delivers compelling value to both security and messaging teams
- Creates upsell path to full Threat Response platform



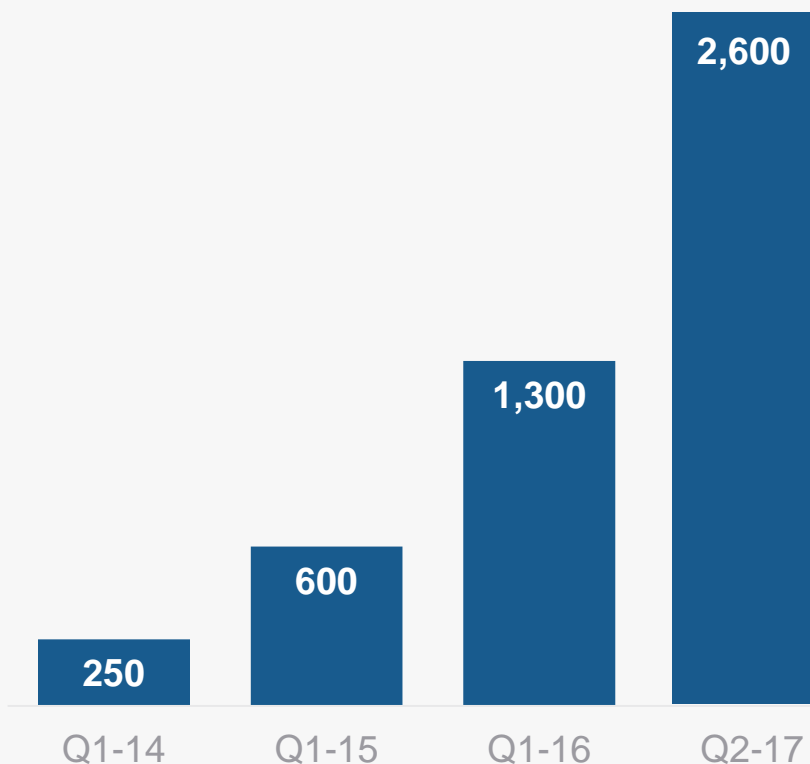
# Proofpoint Threat Response

- Powerful alert & incident management
  - Alert correlation and assignment
- Automated threat containment
  - Infection verification and isolation
- Multi-channel enforcement
  - Automatically push indicators to firewalls, proxies, or other devices
- Automated threat hunting
  - Search for indicators across the enterprise
- Open, extensible platform
  - Support for Palo Alto, Splunk, CyberArc, Imperva, Tanium, Checkpoint, FireEye, Cisco, Bluecoat, and more

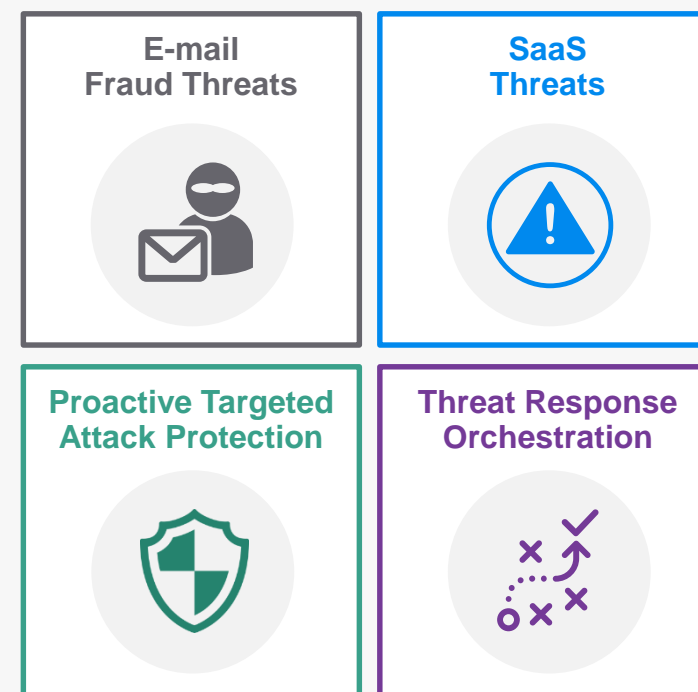


# Summary: Extending the TAP Franchise

## Growing Our Lead and Market Share with TAP



## Leveraging TAP to Drive Adoption of Emerging Products



# Threat Research & Landscape



# World-Class Threat Research

## The Team



- Significant investment
  - Global team
  - World-leading experts in critical domains
- Work with researchers across the security community
- Diverse skills
  - Malware analysis
  - Network and protocol analysis
  - Exploit kit tracking
  - Data science & machine learning
  - Language skills including Russian and Chinese
  - Actor and dark-web monitoring

## Key Responsibilities



- Threat detection
- Hunting and intelligence gathering
- Zero-day exploit identification
- Campaign, malware and actor tracking and attribution
- Threat publication
- Direct customer engagements

# Threat Research: Defensible Advantage

Great Data



Innovative Tooling



World-Class Team



Research Culture



**proofpoint.**

# Threat Landscape

Bryan Burns

VP Threat Research



**ANALYST DAY 2017**

© 2017 Proofpoint, Inc.. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners



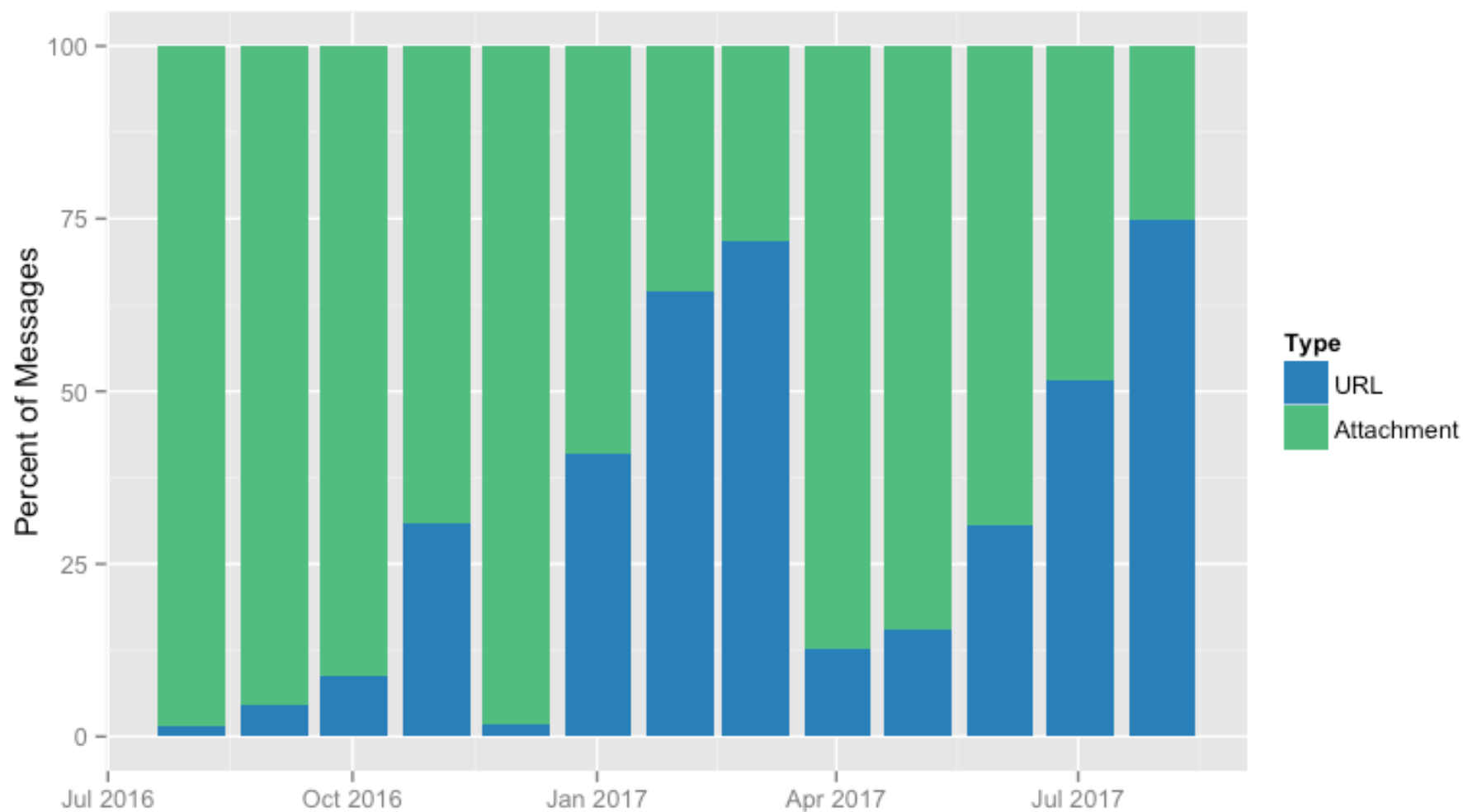
# Humans Continue to be the #1 Target

- 99+% of current threats require human interaction to succeed
  - URLs
    - Credential phishing requiring forms to be filled
    - Links to malware that require the user to save and execute file
  - Attachments
    - Macros that require user to “enable”
    - Embedded files that need to be double-clicked & accepted
- Exploit Kits are in serious decline for the 2<sup>nd</sup> year in a row
  - Several major EK-using actors have switched to using social engineering instead
- Email Fraud attacks are entirely human-focused
- Even APT actors are increasingly relying on user trickery over 0day exploits

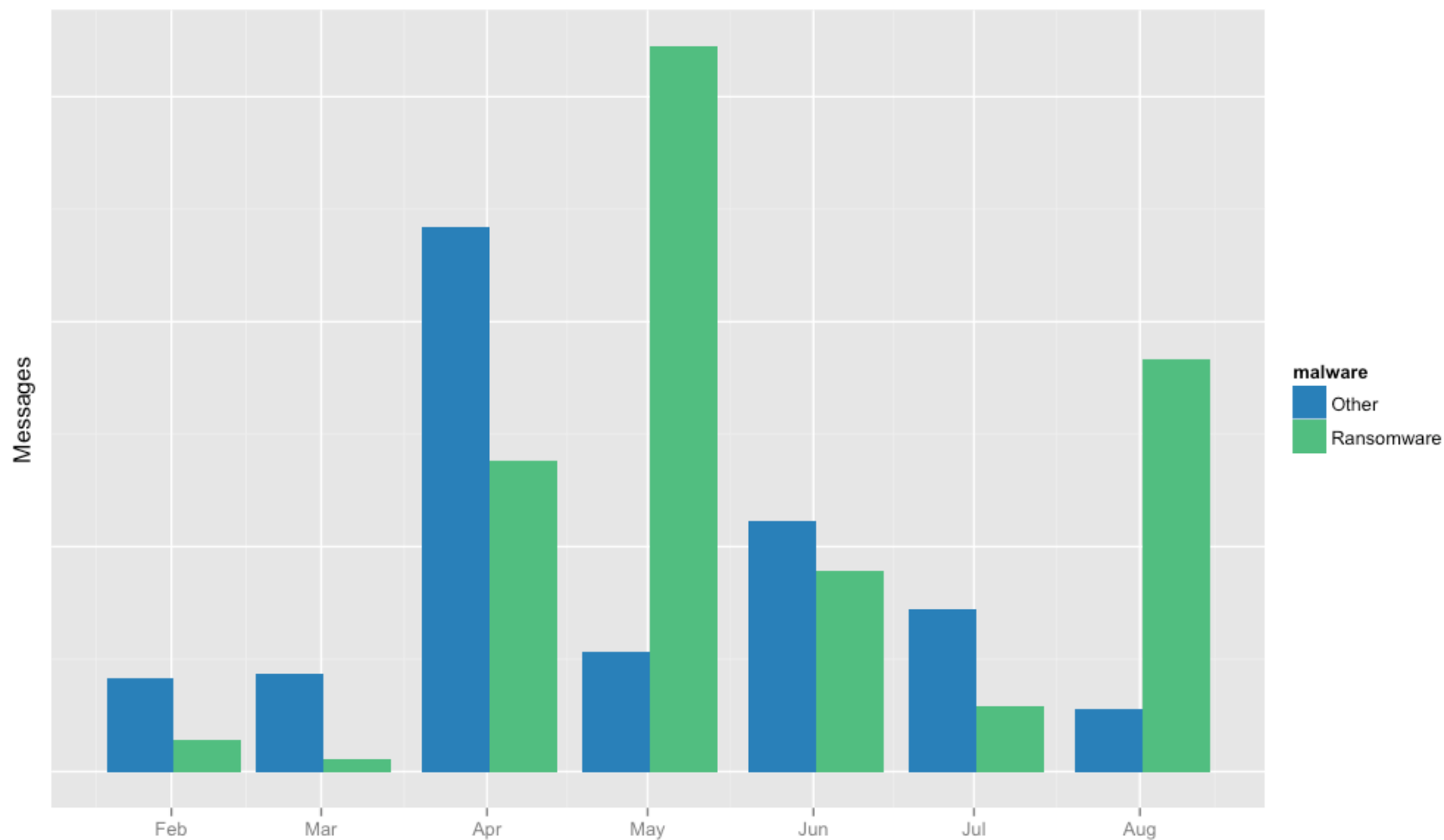




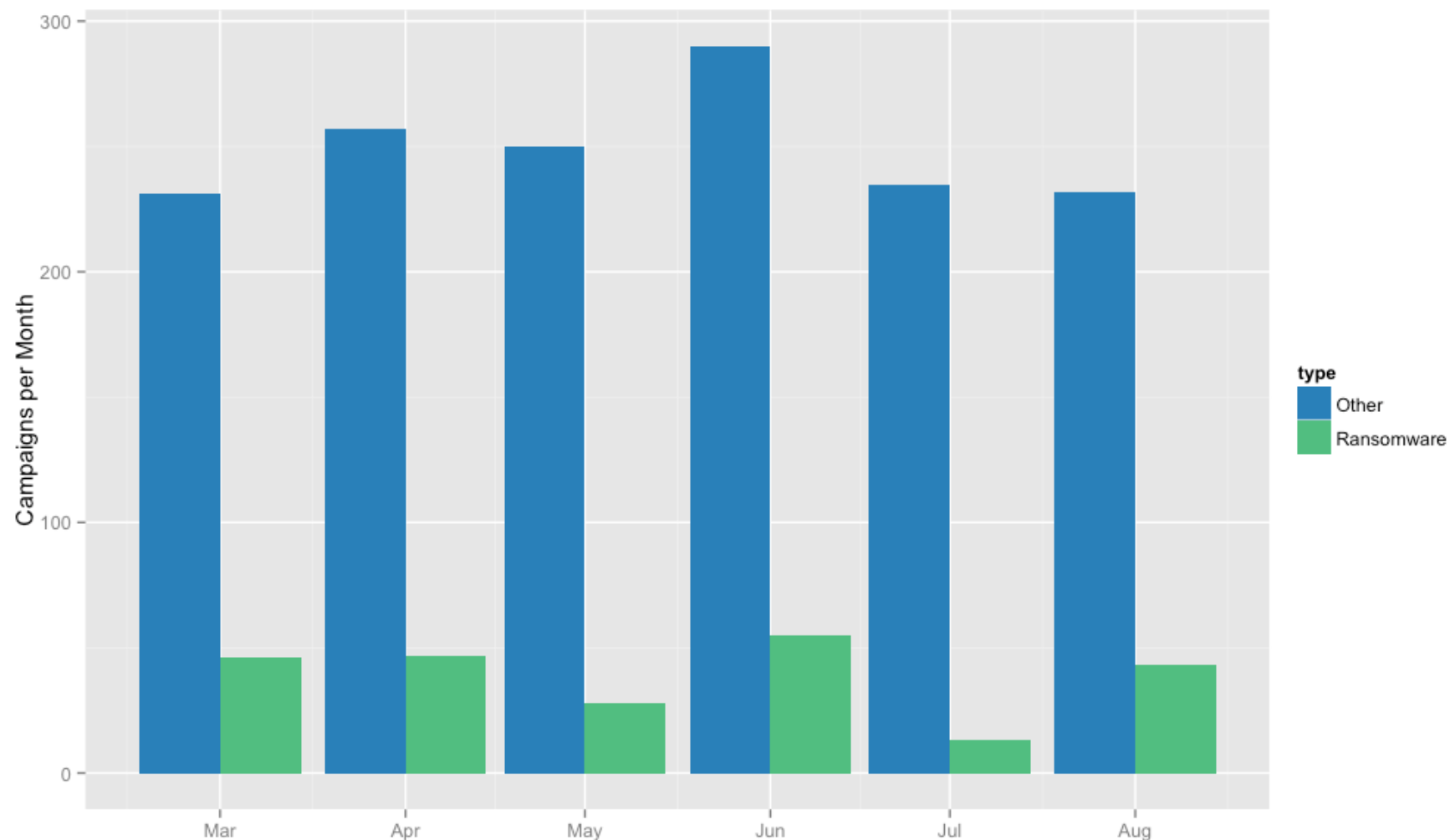
# Malicious URLs are Back in Style



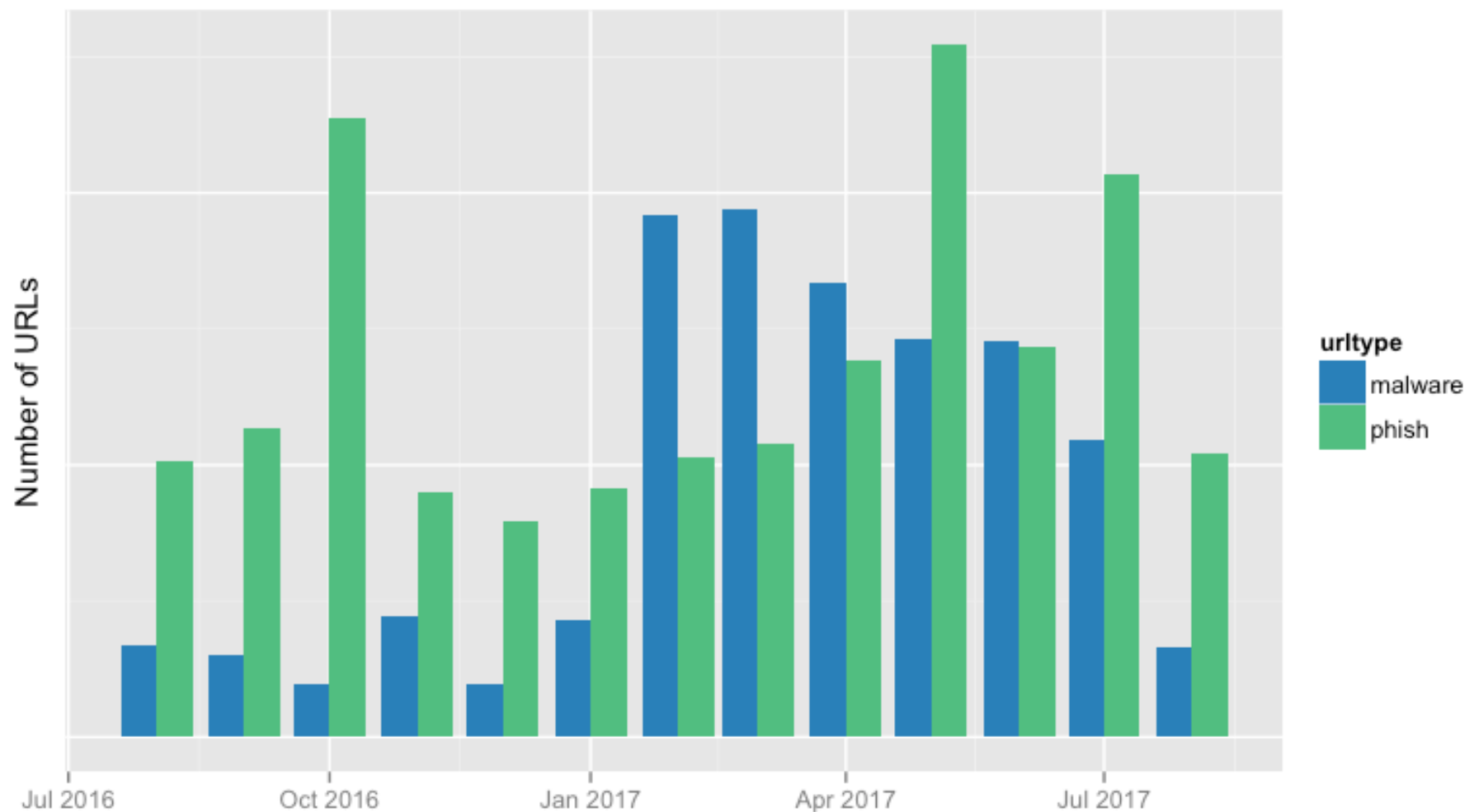
# Most Malware in Email is Ransomware



# Ransomware the Majority of Campaigns



# More Phishing than Malware URLs

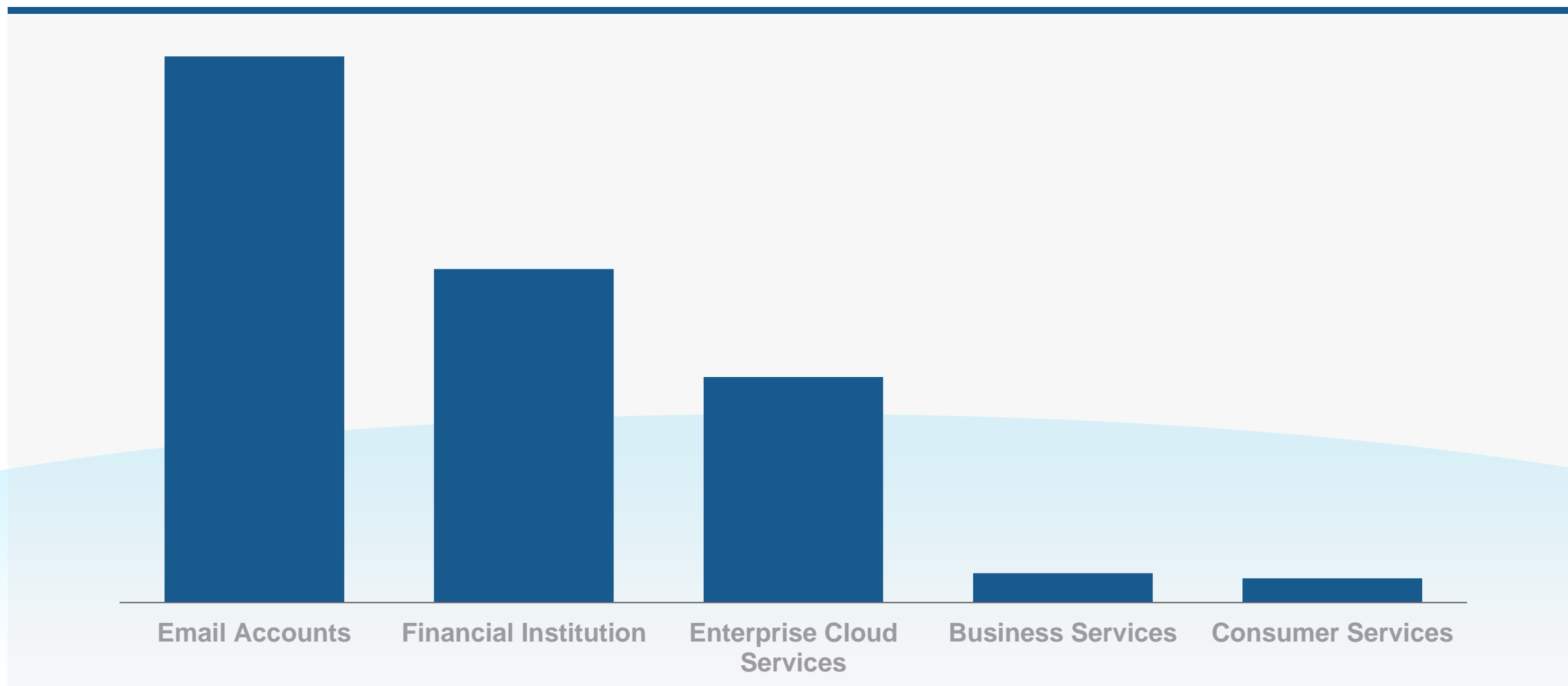


# Credential Phishing Trends

- Seeing increase in phishing of enterprise cloud services
  - e.g., Dropbox, Box, OneDrive, Salesforce, etc.
- Cryptocurrency becoming a more common target
- Attackers frequently embedding phishing URLs inside of documents to bypass traditional filters
- Certain consumer-oriented brands see high volumes of phishing via SMS and social media
- Phishing is often the first stage of a larger attack
  - e.g., extensive DNC compromise started with email credential phish
  - BEC actors can use phished credentials to perform pre-attack reconnaissance

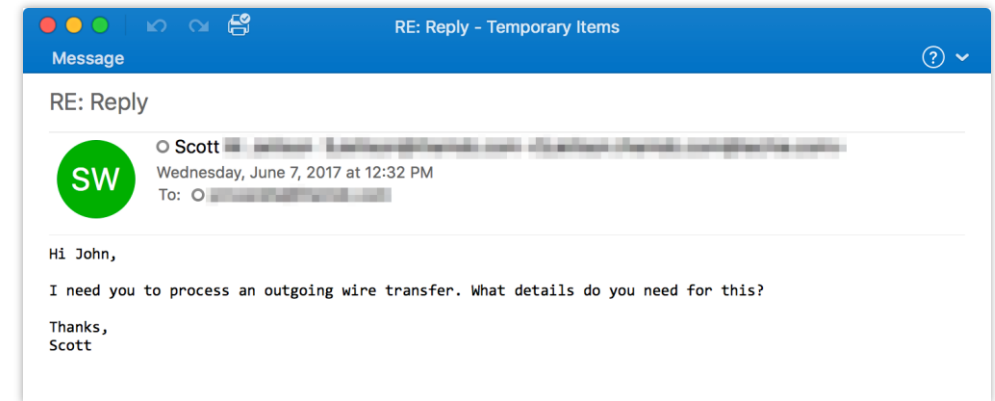
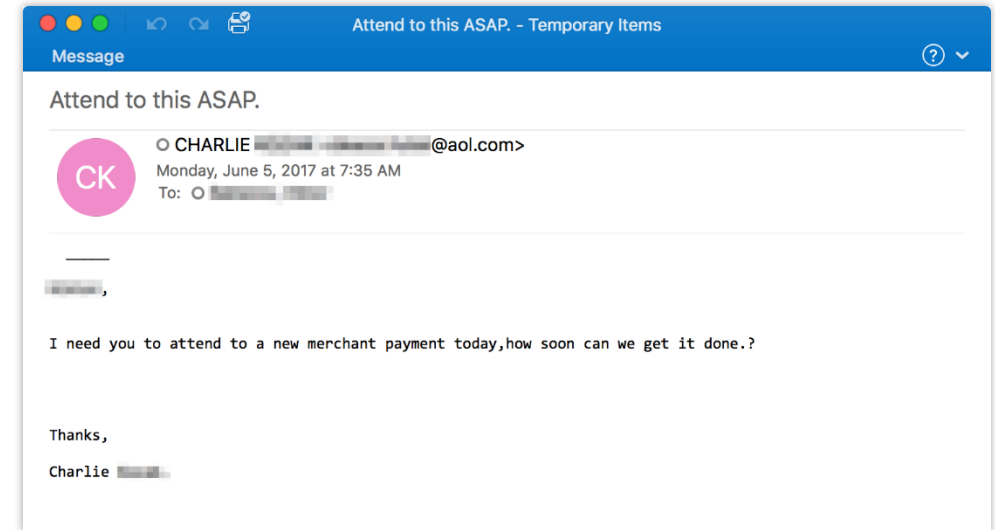


# Most Phished Credentials



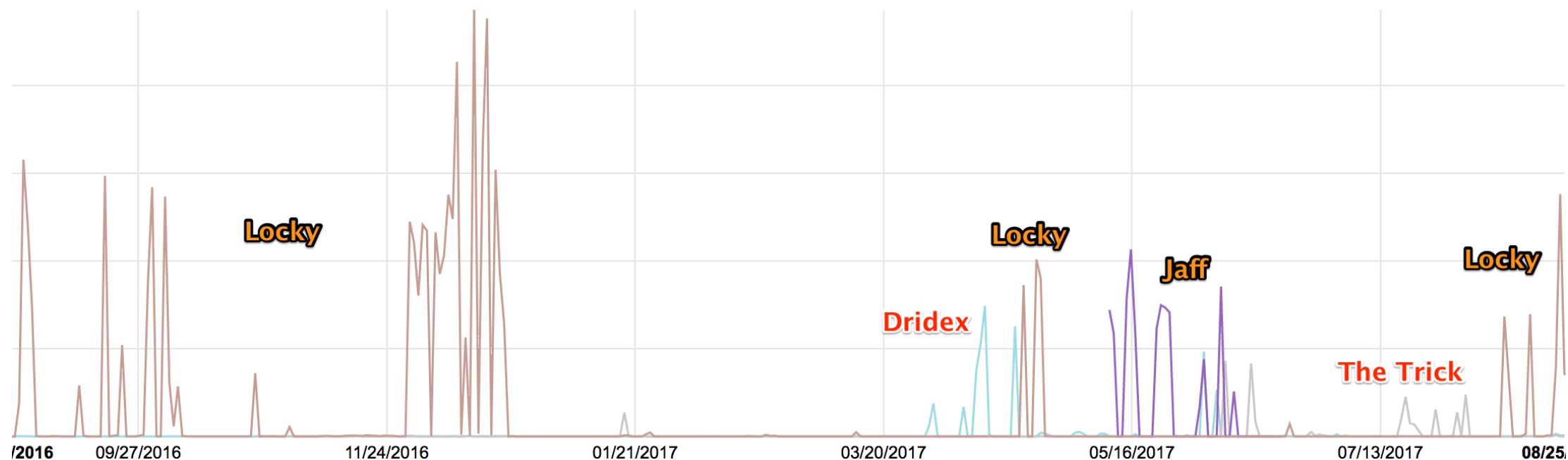
# Email Fraud Tactics

- Roles and names carefully researched in advance
  - High-level executive → payment processor typical
  - Often by successful phishing/RAT infections
- Typical attacker groups are small teams of 4+ people with specific roles
- Messages tend to be short and simple
- Attackers engage in back-and-forth conversation with their target to build legitimacy
- Most sophisticated actors infiltrate org to hijack existing conversations
- Increasingly seeing the use of look-alike domains



# Actor Spotlight: TA505

- Highest volume actor of the last year
- Responsible for Dridex banking trojan and Locky ransomware distribution
- Branching out into a broader selection of malware in 2017



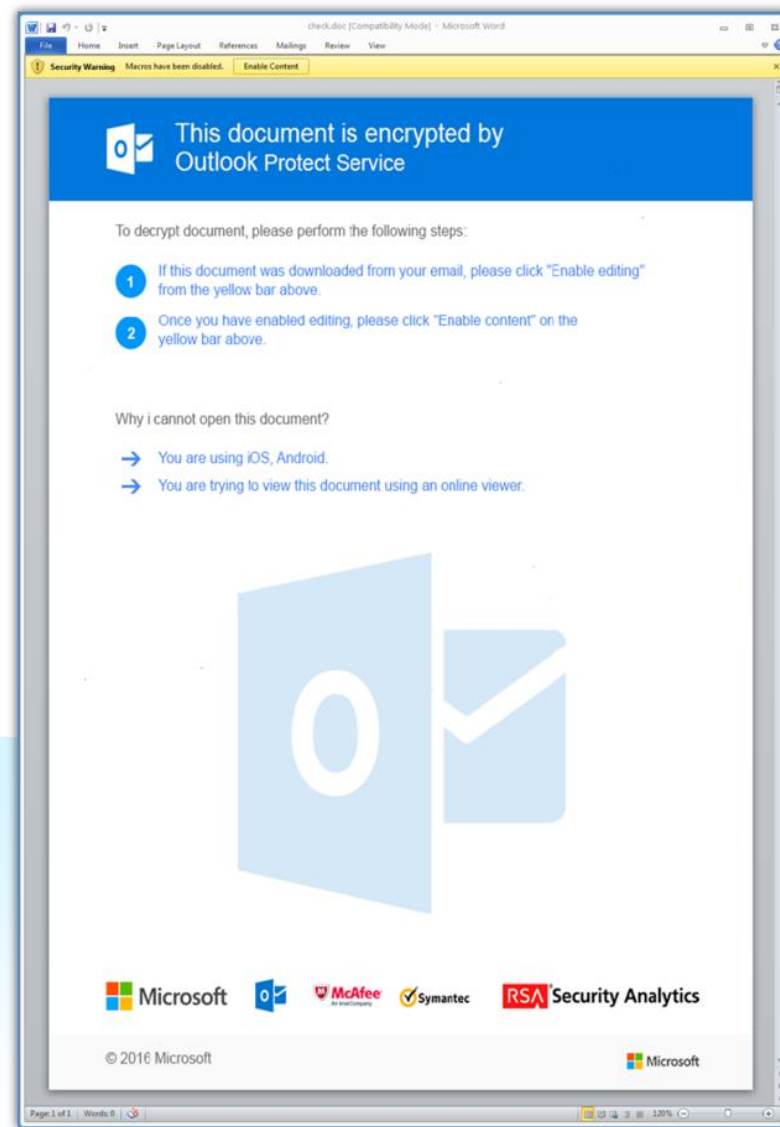
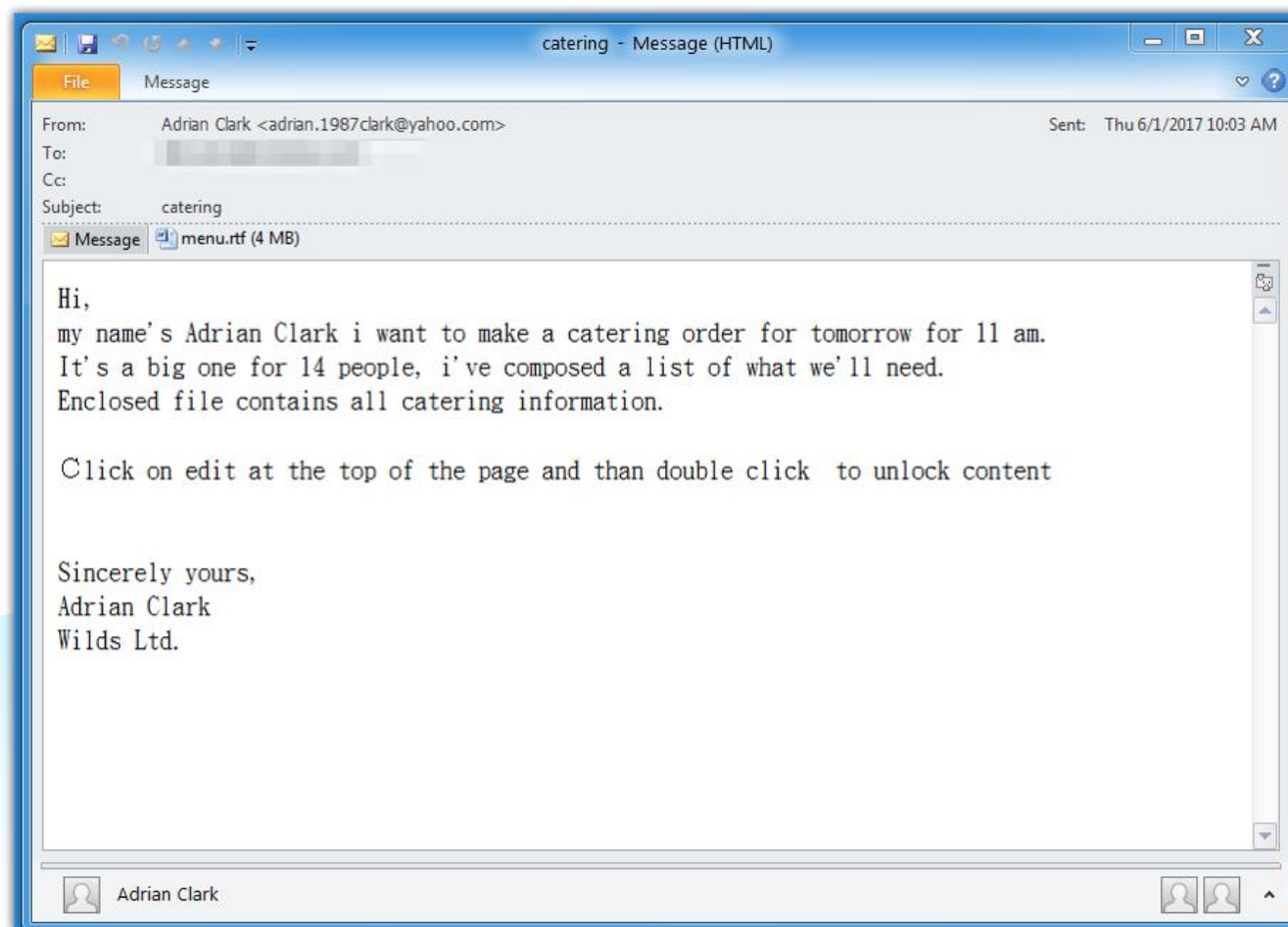


# APT Actor Spotlight: Carbanak

- Most prolific (non-nation-state) APT actor of 2017
- Recent heavy targeting of chain restaurants
- Directly attacking restaurant branches with point-of-sale malware (CC# scraping)
- Also targeting restaurant supply chain vendors
- Also observed attacking software providers and payment/payroll processing
- Typically target 1-2 companies at a time, and repeatedly attack for several weeks

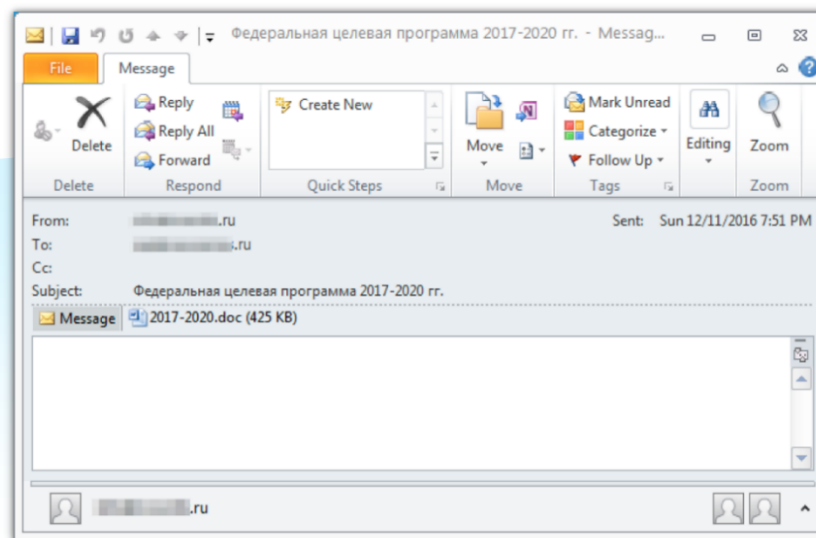


# Sample Carbanak Lures



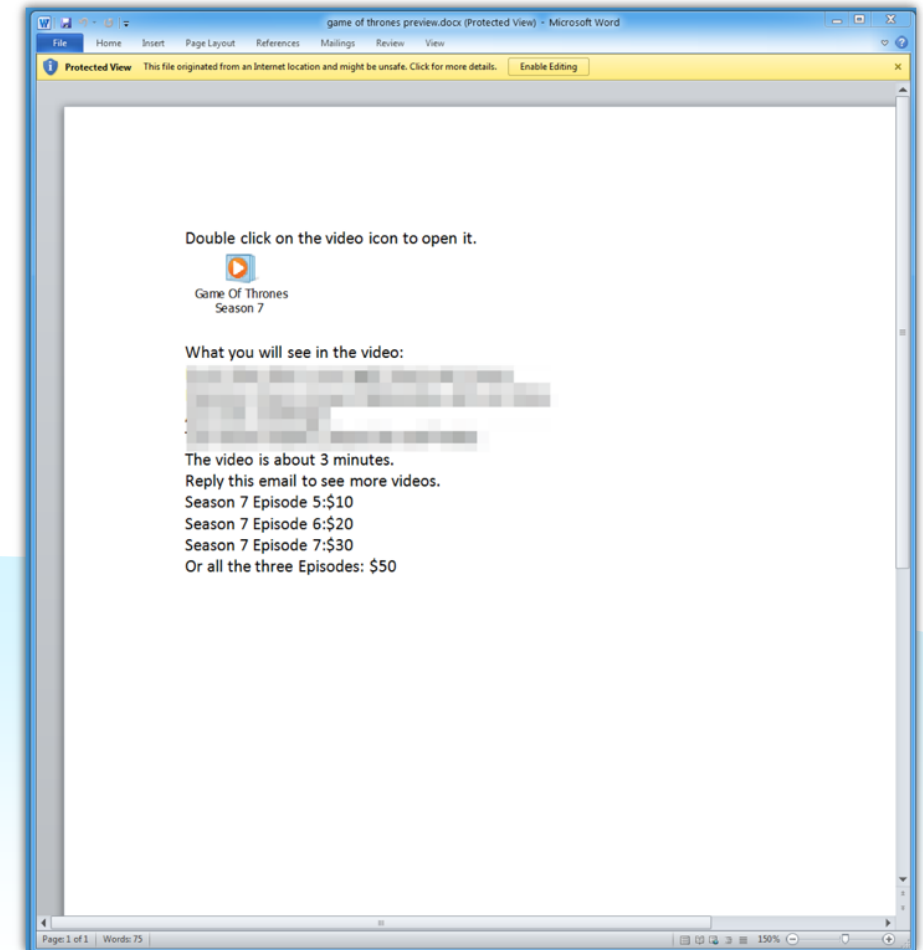
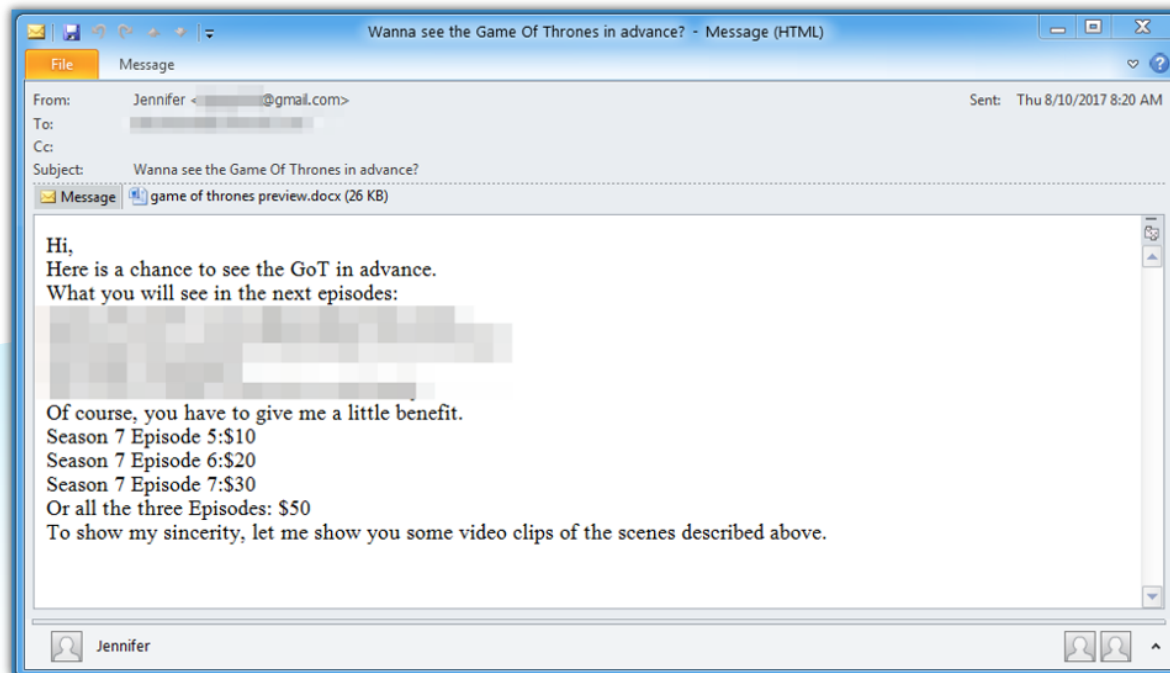
# APT Actors Continue to be Active

- Seeing steady activity from a variety of nation state actors
- Their techniques and toolkits continue to evolve
- Primarily using social-engineering instead of expensive exploits
- Email continues to be their preferred infection vector



# Recent Example APT Attack

- Fake “Game of Thrones” leak, leads to APT trojan
- Timed to coincide with build-up to the season finale



**proofpoint™**







**proofpoint.**

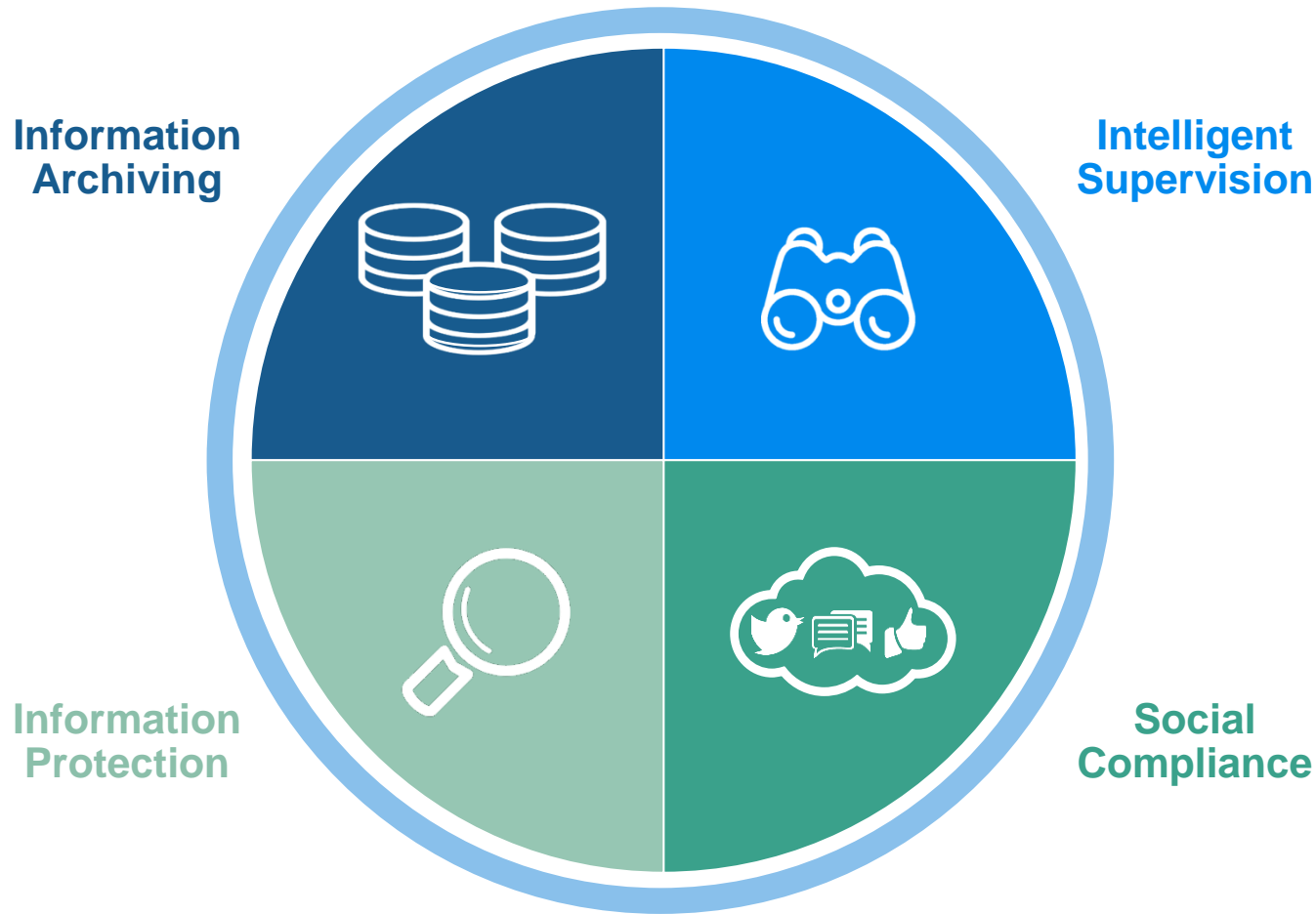
# Capturing the Compliance Market

Darren Lee  
Senior VP & GM

**ANALYST DAY 2017**

© 2017 Proofpoint, Inc.. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners

# Proofpoint Compliance Suite



## Strong business drivers

- Regulatory: 2016 Record year in fines for FINRA
- e-Discovery: Cost \$18K per GB for legal review
- Favorable competitive environment

## Solid customer traction

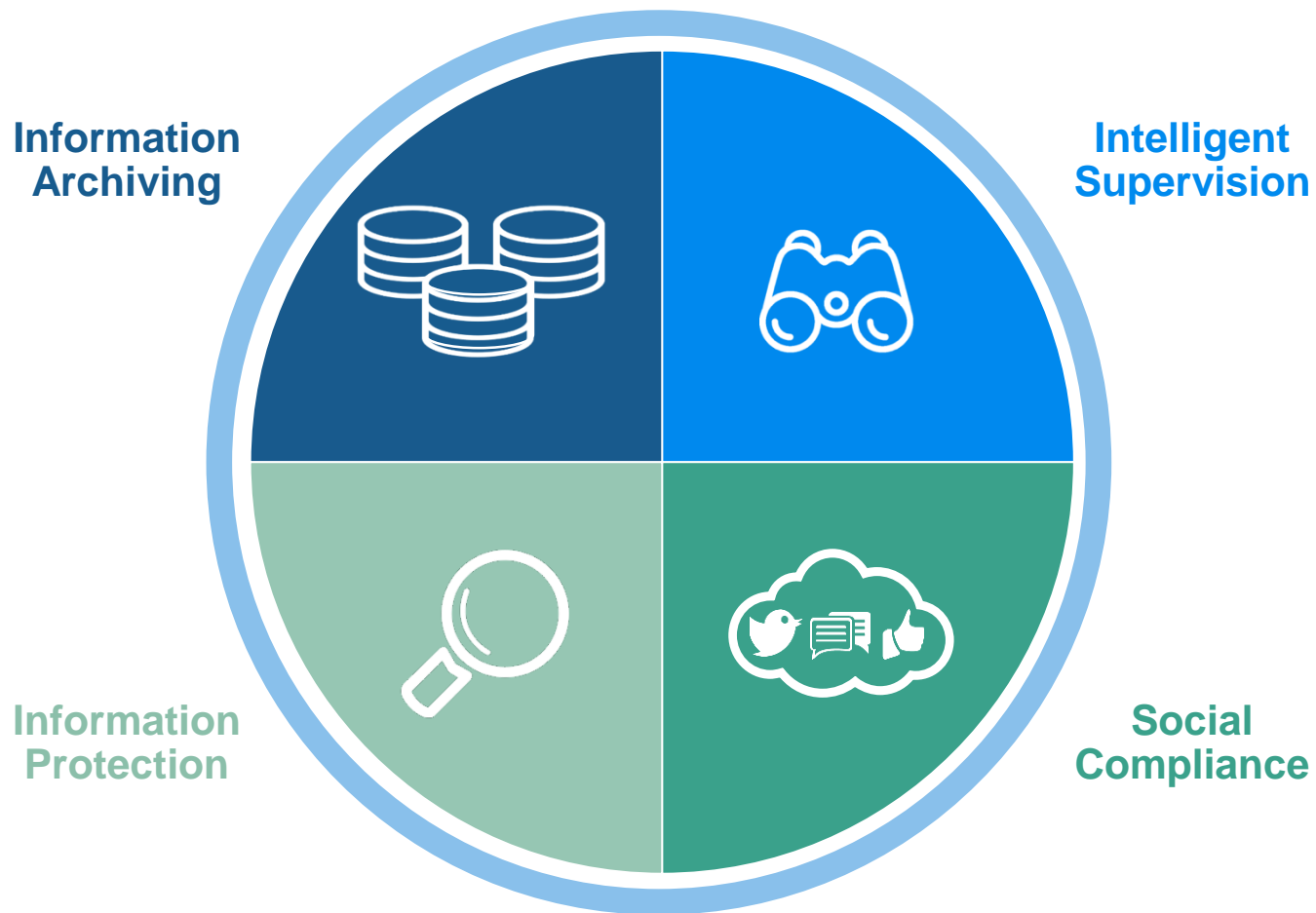
- Strong go-to-market leverage with security sale
- Largest average deal size of any Proofpoint customer

## Performing at enterprise scale

- 19+ PB total data under management in archive
- Largest customer: 140,000 seats, 600+ TB
- Average search speed 4.6 seconds

Source: Gartner IT Key Metrics Data 2012

# What Do They Buy?













Product	Price*
Archive	\$25
Intelligent Supervision	\$25
Additional Content Types	\$10
Social Compliance	\$10
Information Protection	\$10
<b>Total</b>	<b>\$80</b>

\*Price points assume a "large customer at scale"



# Why Do They Want What We Are Selling?

Compelling Reason to Buy	World-Class Products	Favorable Competitive Environment
Explosion of Regulations 	 Information Archiving  Intelligent Supervision	 → 
Growth of Data Types 	 Information Protection  Social Compliance	 → 
Significant Cost 		 → 

# Key Growth Drivers

- 1 Volume of data
- 2 Locations of where data is stored
- 3 Growing regulations...and regulatory focus
- 4 Growth in content types
- 5 Cloud disrupts legacy models

*...A Day in the Life of Sensitive Data*

# A Day in the Life of Sensitive Data

*There's a lot of it...*



# A Day in the Life of Sensitive Data

*There's a lot of it...*



*...in a lot of different places.*

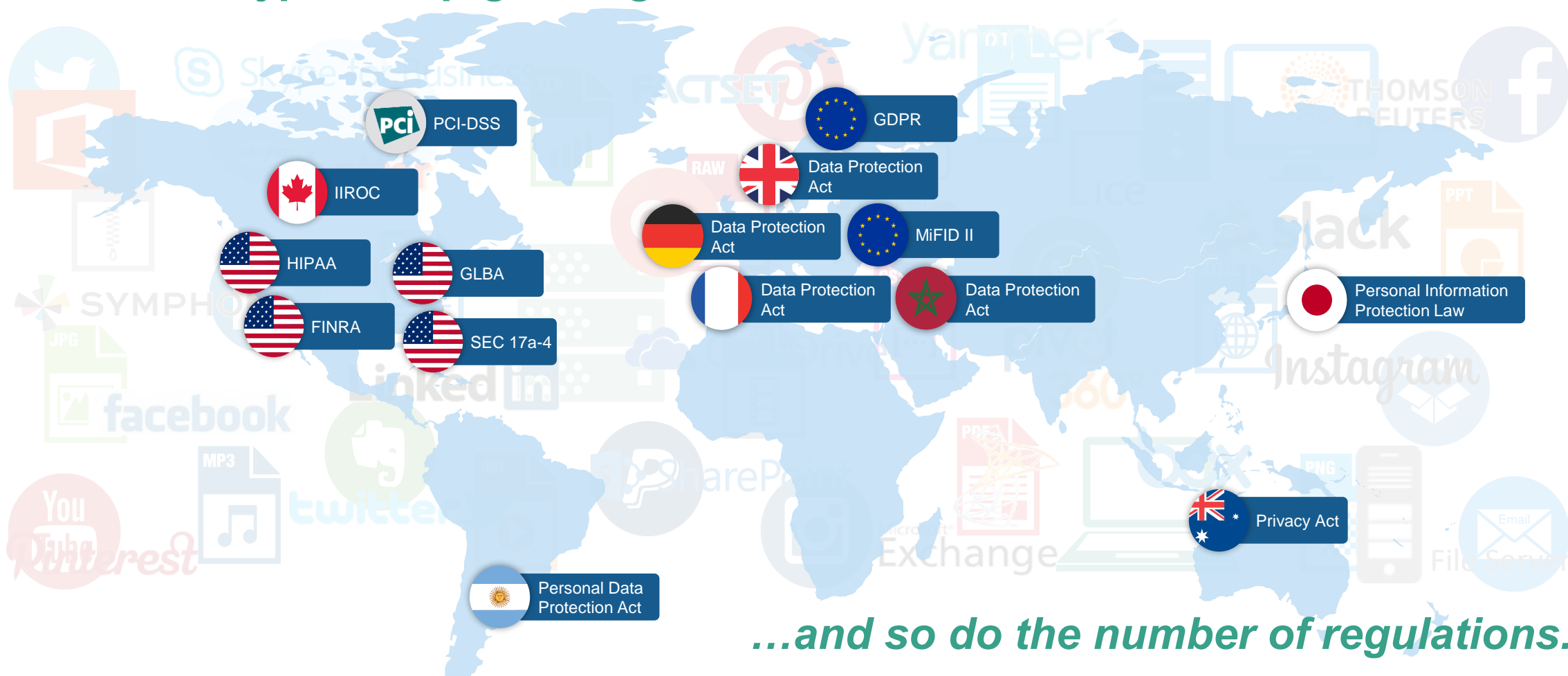
# A Day in the Life of Sensitive Data

*...and data types keep growing...*



# A Day in the Life of Sensitive Data



*...and data types keep growing...*



*...and so do the number of regulations.*

# Financial Regulatory Drivers (SEC 17a-4, FINRA, IIROC, MiFID II)

## Key Requirements

1	Records retention	
2	Supervise communication	
3	Store as read-only	
4	Produce data easily	
5	Enable third-party access	

# FINRA Examination Letter—2017

“...FINRA will review firms’ compliance with their **supervisory and record-retention obligations with respect to social media and other electronic communications** in light of the increasingly important role they play in the securities business...”



“...Cybersecurity threats remain one of the most significant risks many firms face,...Among the areas FINRA may review are **firms’ methods for preventing data loss**, ...FINRA may assess controls firms use to monitor and protect this data, for example, through **data loss prevention tools**...”



“...in multiple instances, firms have failed to ... **preserve certain records in a non-rewriteable, non-erasable format**, commonly known as write once read many (WORM) format...”

Log



“...FINRA will assess firms’ **testing of their internal supervisory controls**. Regular testing is critical to enabling firms to identify and mitigate gaps or inadequate controls...”





# GDPR Regulatory Driver

The European Union General Data Protection Regulation (EU GDPR) aims to regulate the collection, processing, storage, deletion, transfer, and use of personal data of EU residents. Any company handling EU personal data will have to comply with the new rules. GDPR also includes a tiered penalty structure of fines of up to 4% of 'annual turnover' for more serious offences.

## Key Requirements

**1**

**Compliance monitoring  
by Data Privacy Officer**



**2**

**Right to be forgotten,  
delete, limit retention**



**3**

**Notify within 72 hours  
of breach**



# Proofpoint Compliance Suite



Information  
Archiving



Information  
Protection



Intelligent  
Supervision



Social  
Compliance

# Proofpoint Compliance Suite



Information  
Archiving



Information  
Protection



Intelligent  
Supervision



Social  
Compliance

# Proofpoint Compliance Suite



Information  
Archiving



Information  
Protection



Intelligent  
Supervision



Social  
Compliance

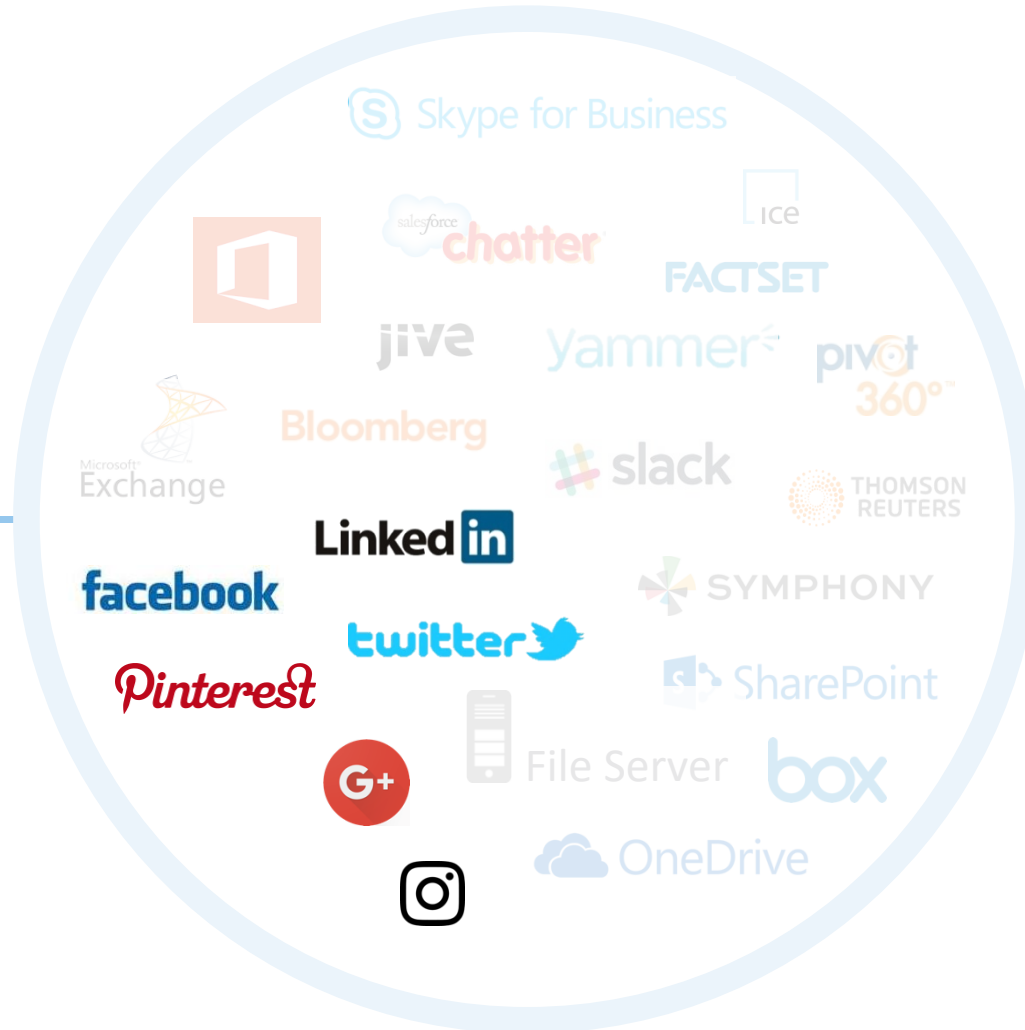
# Proofpoint Compliance Suite



Information  
Archiving



Information  
Protection



Intelligent  
Supervision



Social  
Compliance

# Proofpoint Compliance Suite



Information  
Archiving



Information  
Protection



Intelligent  
Supervision



Social  
Compliance



# Case Study: Financial Services

## About

- Diversified financial services company
- Over 20,000 employees
- Global

## Requirement

- Protect data and employees from security threats
- Capture and preserve data in a compliant archive
- Comply with data privacy regulations at gateway and on-prem
- Supervise all communications of regulated employees
- Monitor social channels for compliant marketing

## Solution

- Protection & TAP
- Information Archive
- Information Protection
- Intelligent Supervision
- Social Compliance

**proofpoint**<sup>TM</sup>





**proofpoint.**

# **Intermission Webcast to Resume at Approximately 3:50 PM ET**

**ANALYST DAY 2017**

© 2017 Proofpoint, Inc. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners

A blurred background image showing three people in a meeting. A man in a grey sweater is pointing at a whiteboard, while a woman in a black top and another man in a dark shirt stand nearby. In the foreground, a wooden desk holds a white tablet, a smartphone, and a white mug with a spoon on a wooden coaster.

**proofpoint.**

# Driving Growth

Tracey Newell  
EVP Worldwide Field Operations

**ANALYST DAY 2017**

© 2017 Proofpoint, Inc.. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners

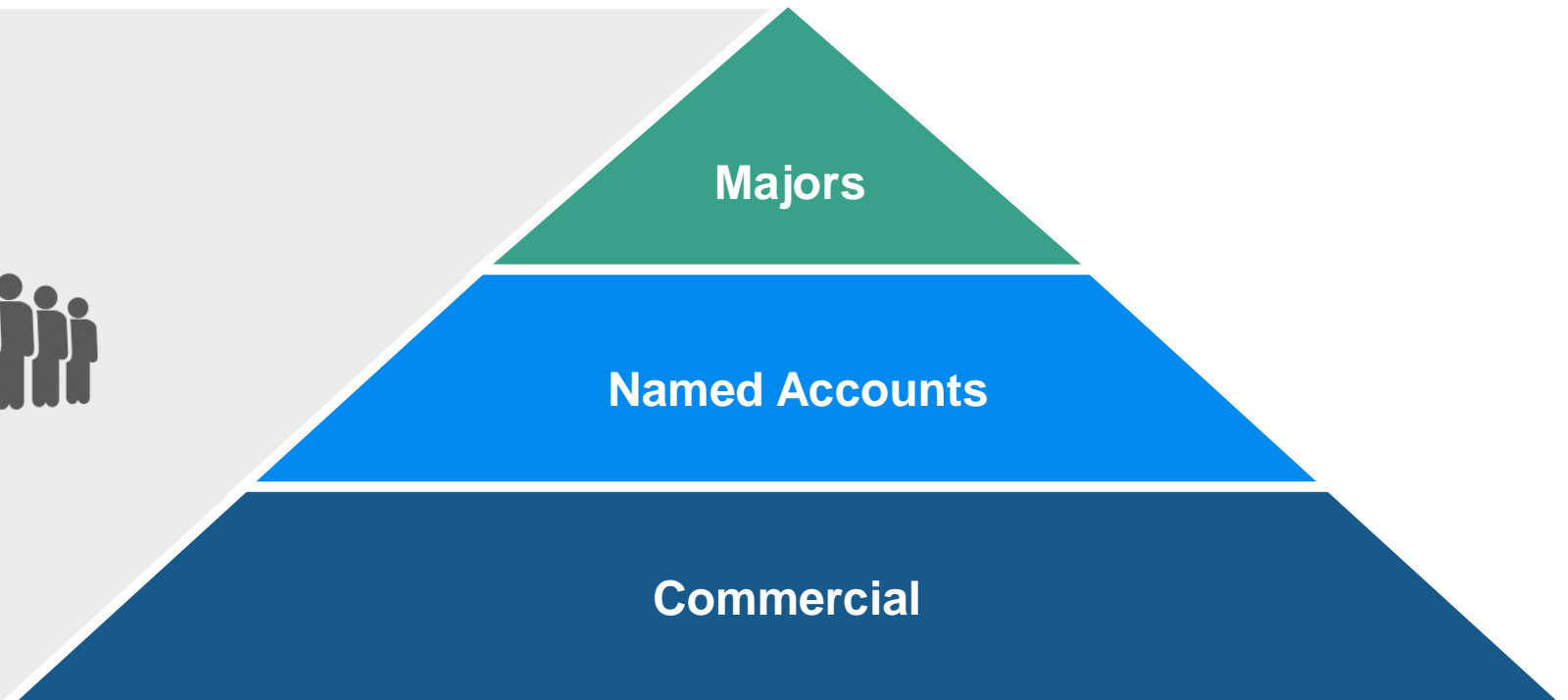
# Driving Growth

- 1 ➤ Broaden customer base
- 2 ➤ Increase sales to existing customers
- 3 ➤ Leverage strategic channel and ecosystem partners
- 4 ➤ Expand internationally
- 5 ➤ Focus on customer success

# Enterprise Go-to-Market

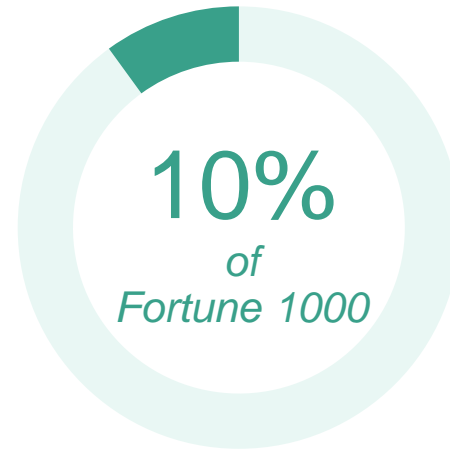


Channel Partners

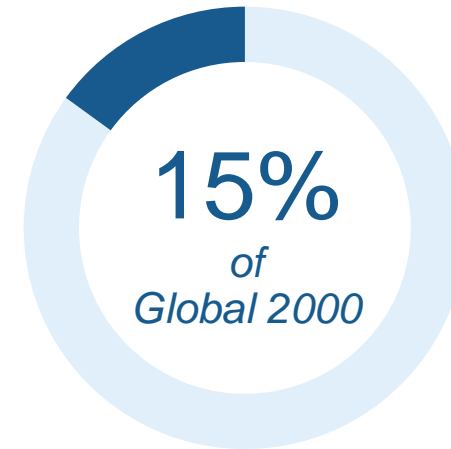
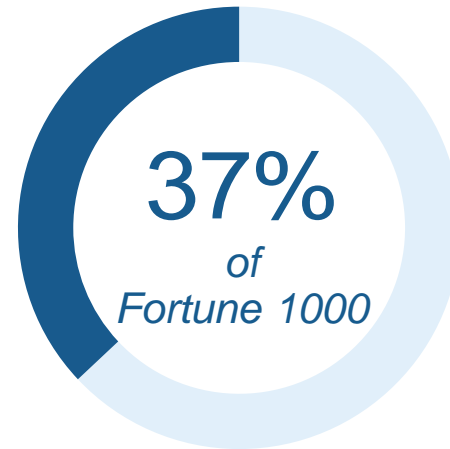
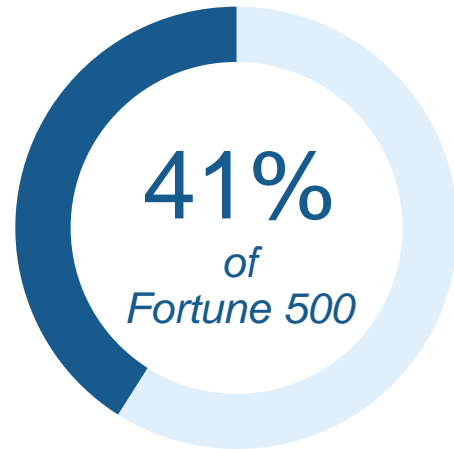


# Accelerate Market Share:

2012  
IPO

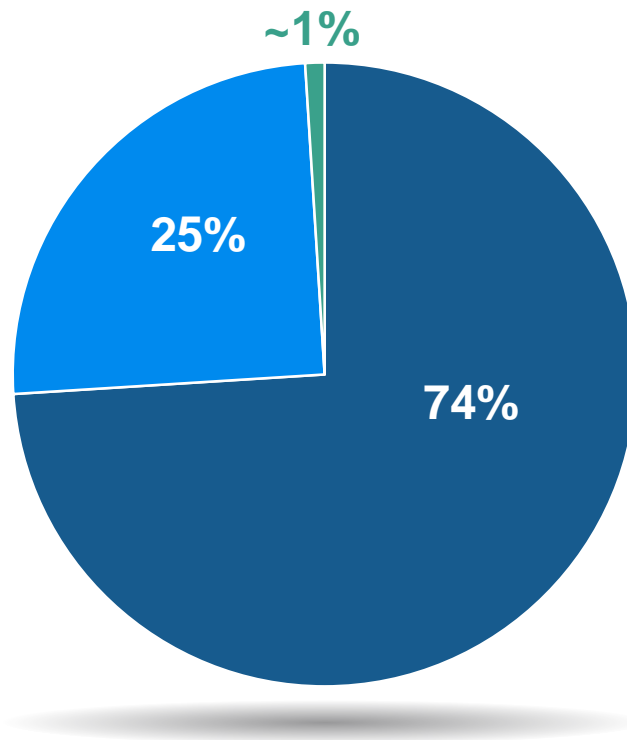


Q2  
2017

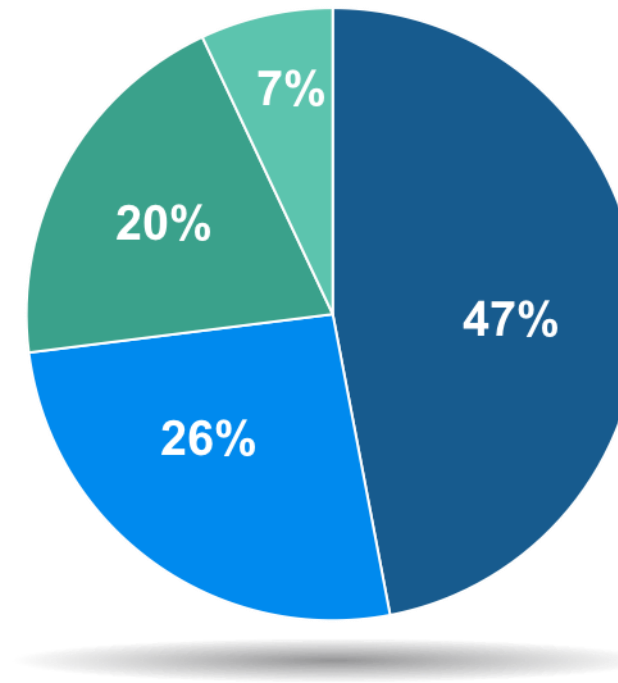


# Add-on Opportunity:

**At Time of 2012 IPO**  
(~2,400 Customers)



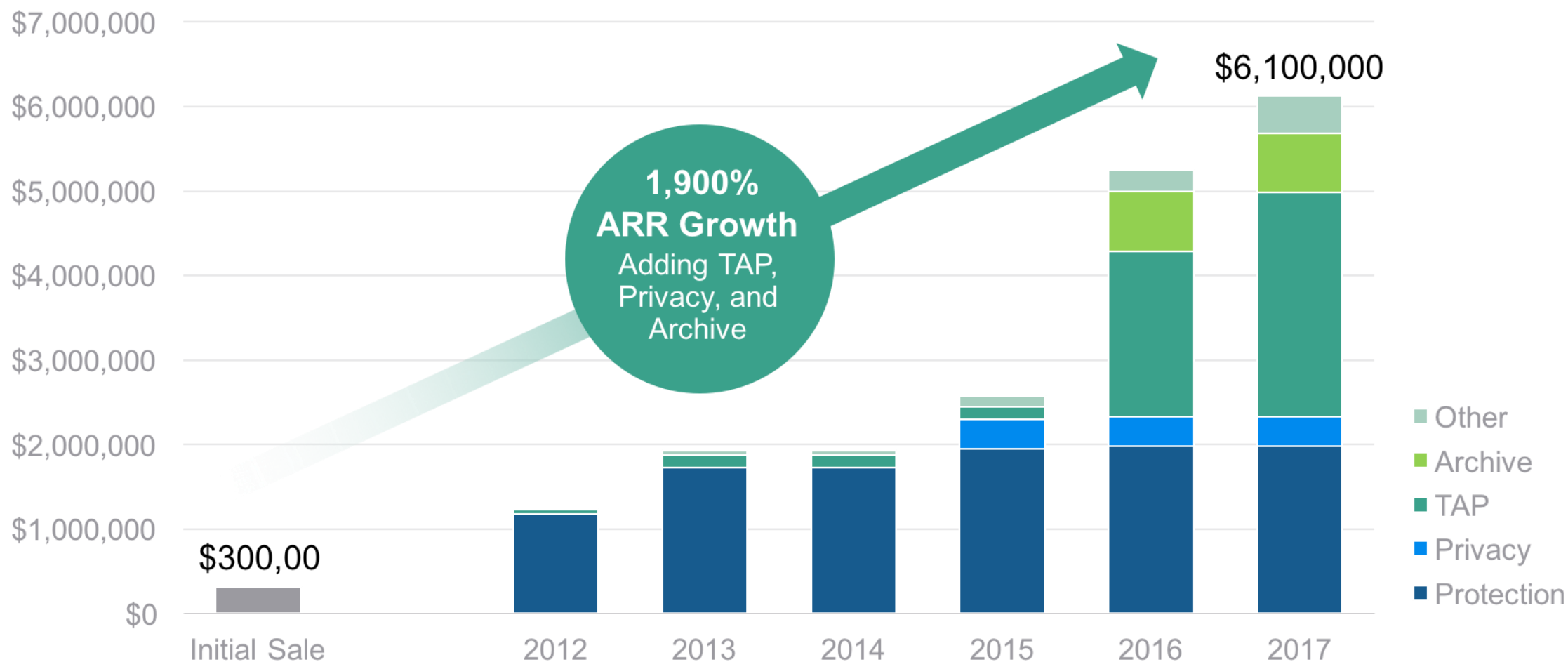
**Q2 2017**  
(~5,900 Customers)



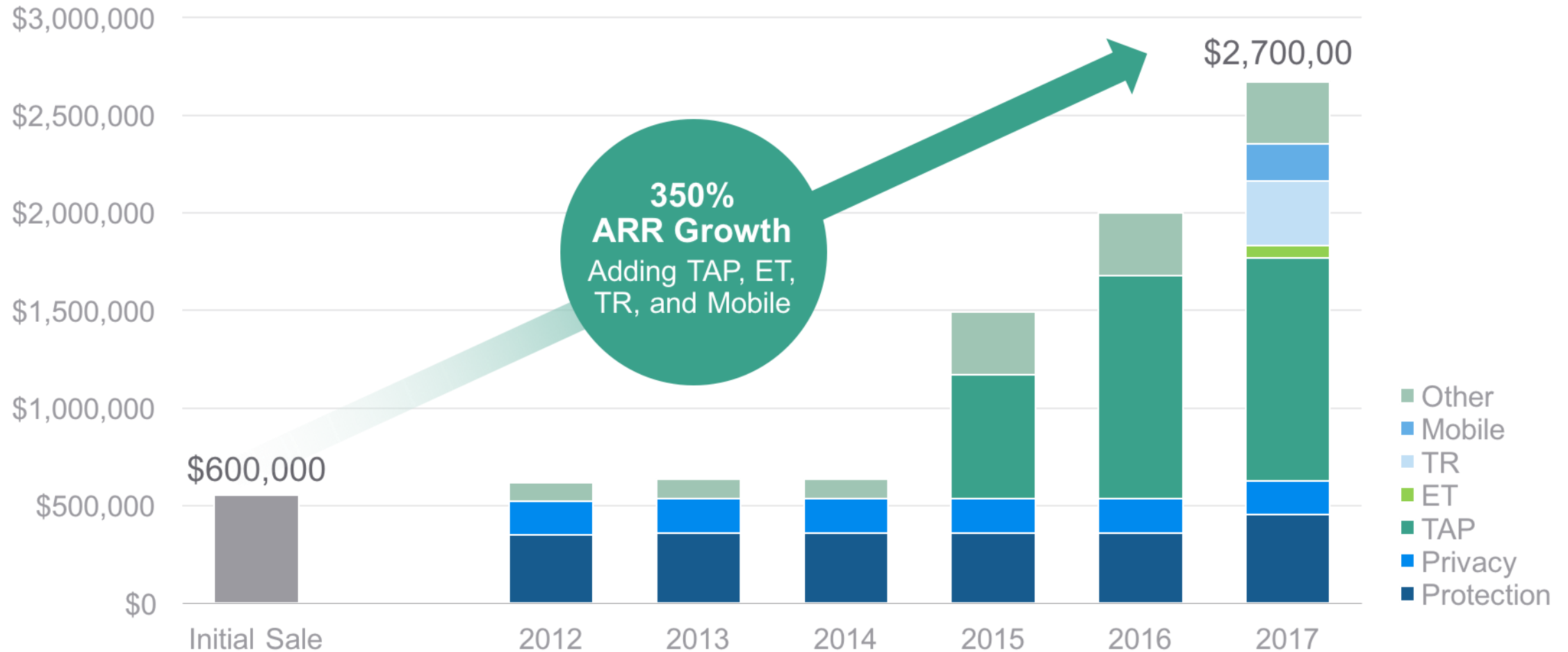
- 1 Product
- 2 Products
- 3 Products
- 4+ Products



# Fortune 500 Financial Services Customer



# Fortune 500 Aerospace and Defense Firm

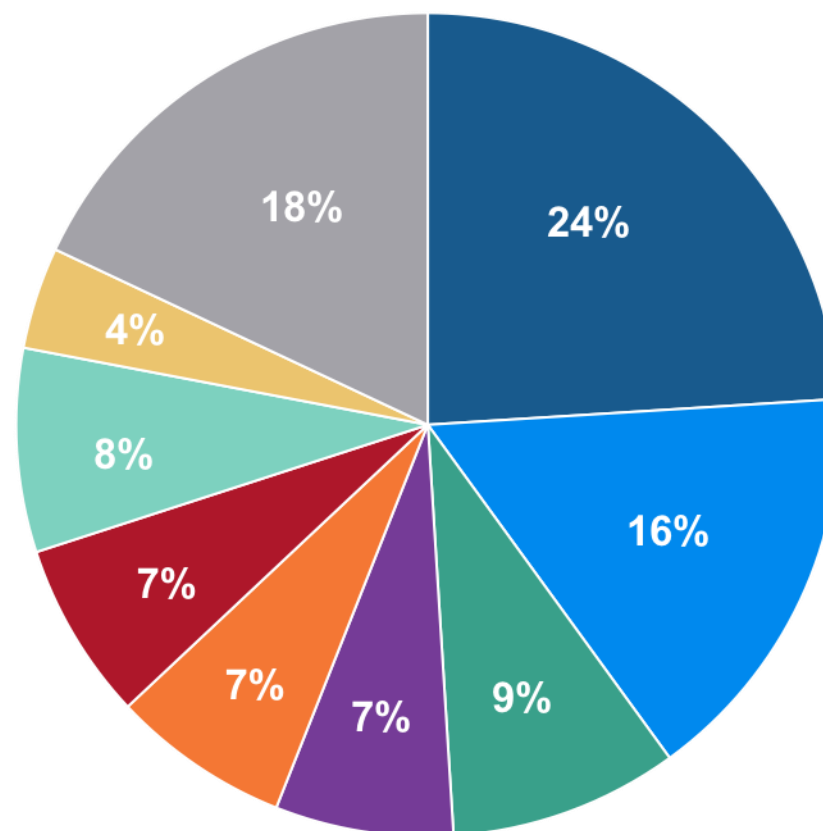




# Annual Contract Value by Vertical

## Investing in:

- Financial services
- Healthcare
- State, local and education
- Federal government



ACV based on customers under contract as of 6/30/17.

# Commitment to Channel

- 1 Channel partner program
- 2 Focus on strategic partners
- 3 90%+ renewal rates
- 4 Sales and technical enablement
- 5 Ease of doing business

# Focus on Strategic Channel Partners



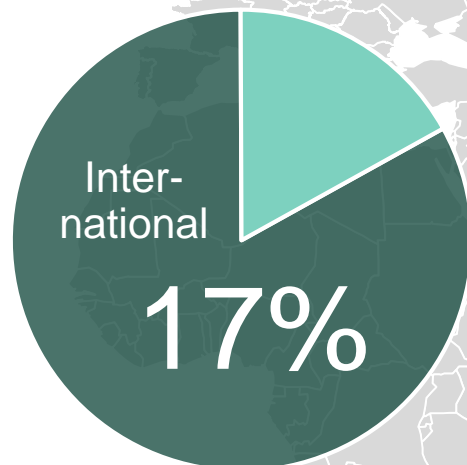
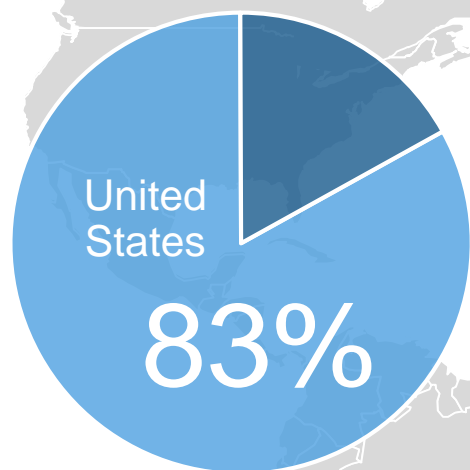
As of 6/30/17

# Focus on Channel and Ecosystem Partners



As of 6/30/17

# International Expansion

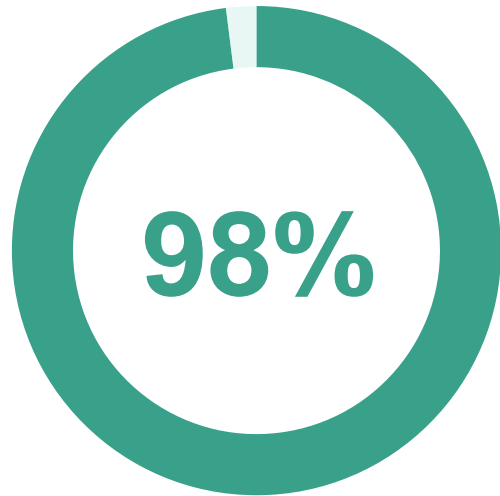


Reflects Q2 2017 International split.

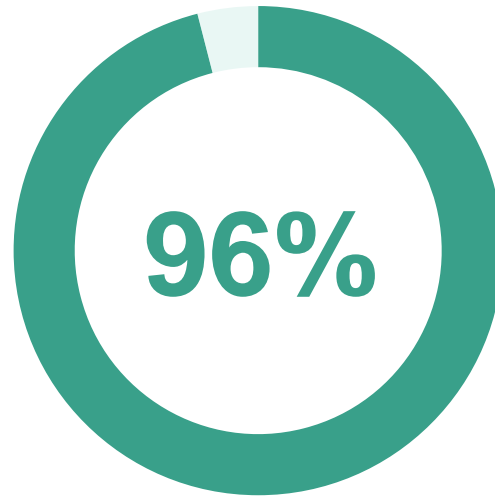
## Momentum in Europe:

- Inside and field sales momentum
- Large enterprise wins
- Channel build-out
- Expansion into new countries

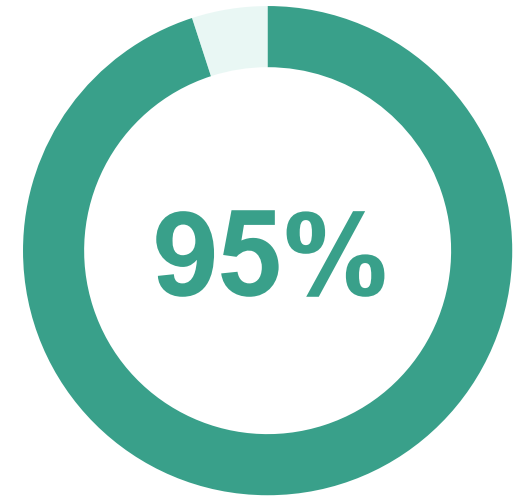
# Customer Success



**Service Provided  
by Tech Support**



**Support Engineer  
Product Knowledge**



**Overall Customer  
Satisfaction**

Data source: Based on 3rd party CSAT survey for Q2 2017.

A close-up, high-angle shot of a fountain pen nib. The nib is silver-colored with intricate engravings, including a circular logo near the top and a stylized leaf or feather design below it. The nib is positioned diagonally, with its tip touching the paper and creating a dark, ink-filled loop. The background is a light-colored, textured surface, possibly paper, with some faint, out-of-focus lines suggesting previous writing. The lighting is soft, highlighting the metallic sheen of the nib and the texture of the paper.

**What I'm Hearing  
from Customers....**



# *Thank You*

**“Your product appears to be really unique  
in that it actually does what you said it  
would do.”**

CISO Global 2000



# Thank You

**“We’re at a 99.89% block rate.  
Not too shabby 😊 180 messages  
delivered in just a little over a month,  
.....I’m thrilled with the results.”**

**Security Analyst, Fortune 500**

# *Thank You*

**“I want to thank you. This is the best rollout of new technology we’ve ever done. We literally have received thank you notes from our end users.”**

**VP of Cyber, Fortune 500**

# In Closing

- 1 Focus on market share
- 2 Accelerate share of wallet with installed base
- 3 Scale through channel and ecosystem partners
- 4 International expansion
- 5 World-class customer service

**proofpoint**<sup>TM</sup>





**proofpoint.**

# Financial Update

Paul Auvil  
Chief Financial Officer

Index ▲ 1.56 ▼ 0.78

**ANALYST DAY 2017**

© 2017 Proofpoint, Inc. All rights reserved and proprietary. Proofpoint is a registered trademark of Proofpoint, Inc. All logos and trademarks are the property of their respective owners

# SAFE HARBOR

This presentation contains “forward-looking” statements that involve risks, uncertainties and assumptions. If the risks or uncertainties ever materialize or the assumptions prove incorrect, our results may differ materially from those expressed or implied by such forward-looking statements. All statements other than statements of historical fact could be deemed forward-looking, including, but not limited to, any projections of financial information; any statements about historical results that may suggest trends for our business and results of operations; any statements of the plans, strategies and objectives of management for future operations; any statements of expectation or belief regarding future events, potential markets or market size, or technology developments; and any statements of assumptions underlying any of the foregoing.

These statements are based on estimates and information available to us at the time of this presentation and are not guarantees of future performance. Actual results could differ materially from our current expectations as a result of many factors, including but not limited to: quarterly fluctuations in our business and results of operations; our ability to address market needs and sell our applications and services successfully; integration of acquisitions; acquisition-related liabilities and charges; the general market conditions; and the effects of competition. These and other risks and uncertainties associated with our business are described in our Quarterly Report on Form 10-Q for the three months ended June 30, 2017, and the other reports we file with the SEC, copies of which are available free of charge at the SEC's website at [www.sec.gov](http://www.sec.gov) or upon request from our investor relations department. All forward-looking statements herein reflect our opinions only as of the date of this presentation and Proofpoint undertakes no obligation, and expressly disclaims any obligation, to update forward-looking statements herein in light of new information or future events.

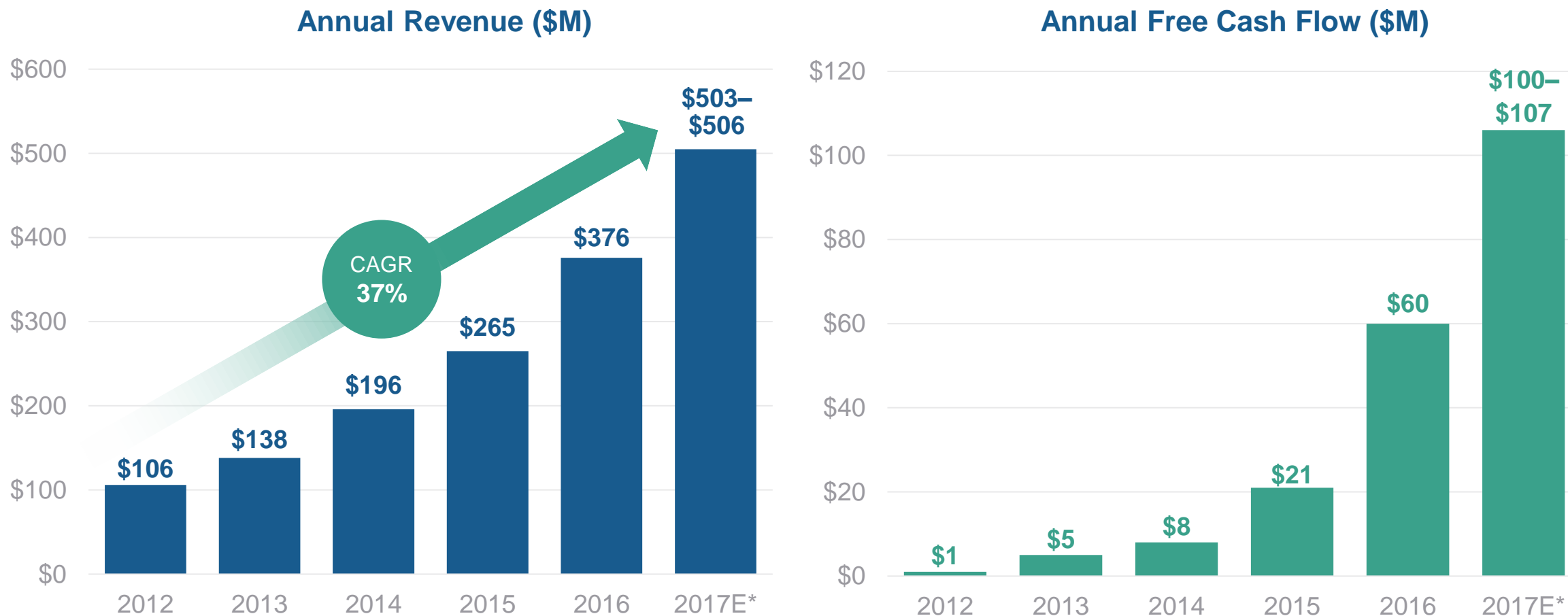
In addition to U.S. GAAP financials, this presentation includes certain non-GAAP financial measures. These historical and forward-looking non-GAAP measures are in addition to, not a substitute for or superior to, measures of financial performance prepared in accordance with GAAP. The most directly comparable GAAP information and a reconciliation between the non-GAAP figures are provided on slides at the back of this presentation.

Proofpoint is a registered trademark of Proofpoint, Inc. This presentation also contains additional trademarks and service marks of ours and of other companies. We do not intend our use or display of other companies' trademarks or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.

# Reaffirming Guidance Provided July 27, 2017

We are officially reaffirming guidance, both for the third quarter and the full year 2017, as provided on our earnings call on July 27, 2017.

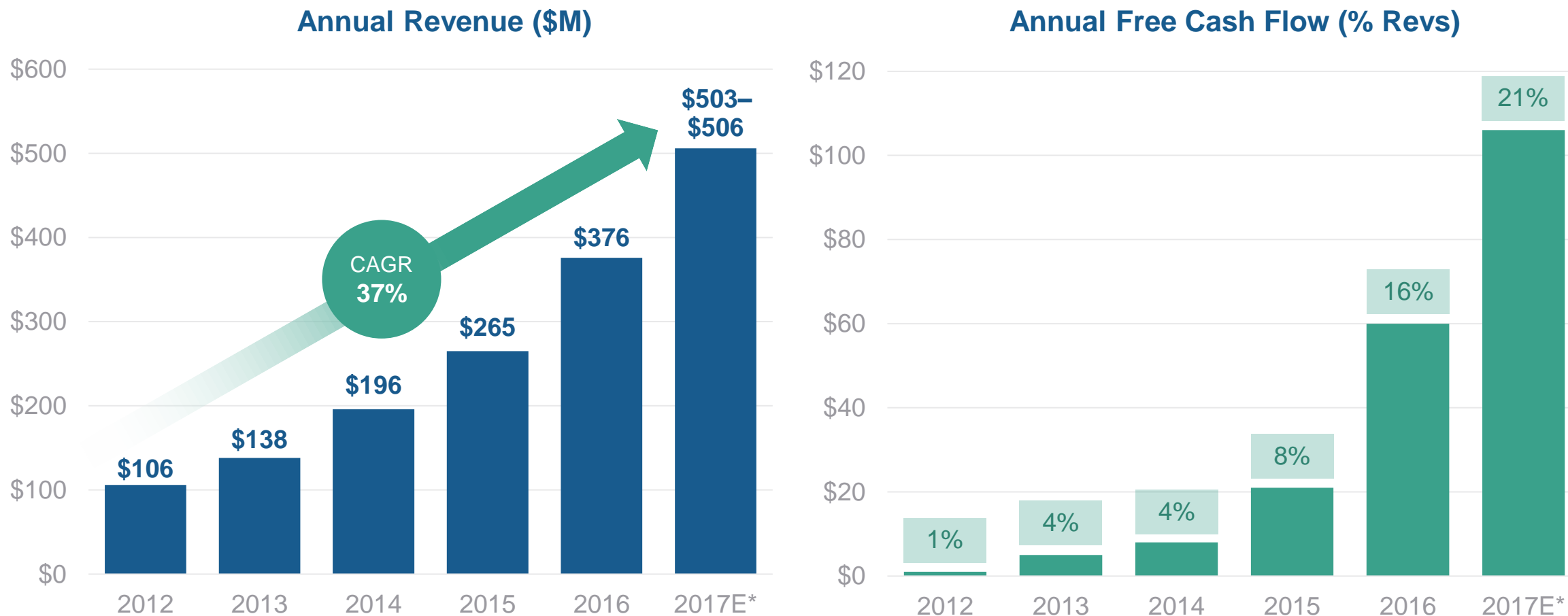
# Highly Visible Revenue Drives Free Cash Flow



\*2017E provided on Form 8K July 27, 2017. 2017E FCF % of revenue assumes midpoint of guidance range. Free Cash Flow defined as net cash provided by operating activities minus capital expenditures.



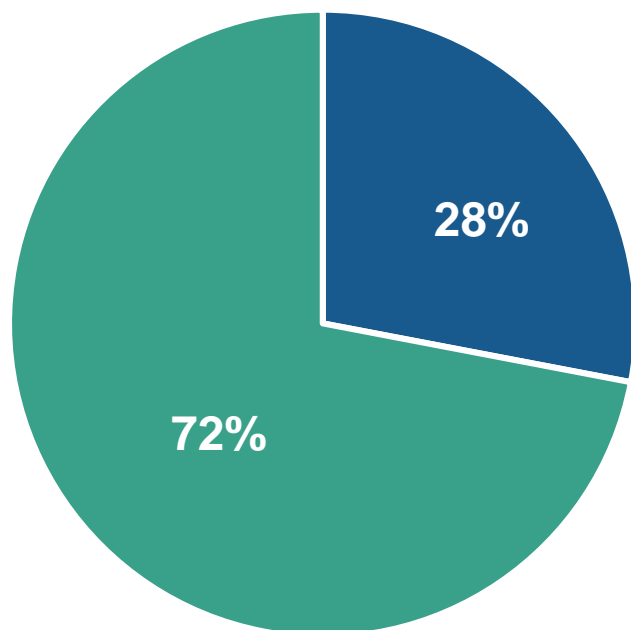
# Highly Visible Revenue Drives Free Cash Flow



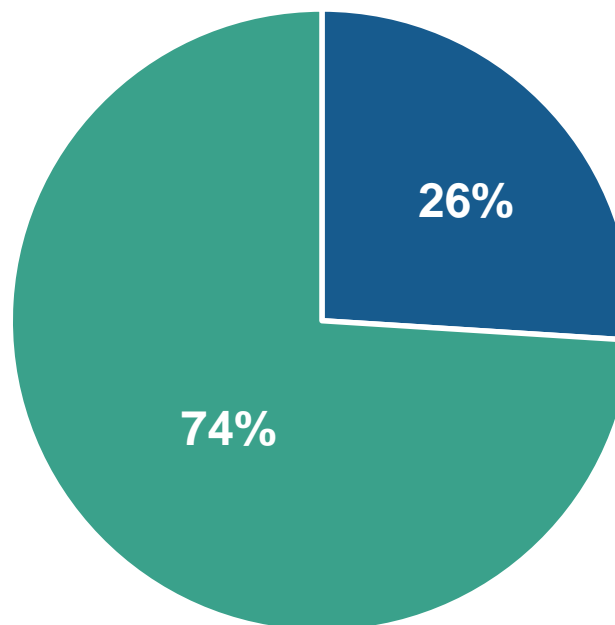
\*2017E provided on Form 8K July 27, 2017. 2017E FCF % of revenue assumes midpoint of guidance range. Free Cash Flow defined as net cash provided by operating activities minus capital expenditures.

# Revenue by Segment

First Half 2016



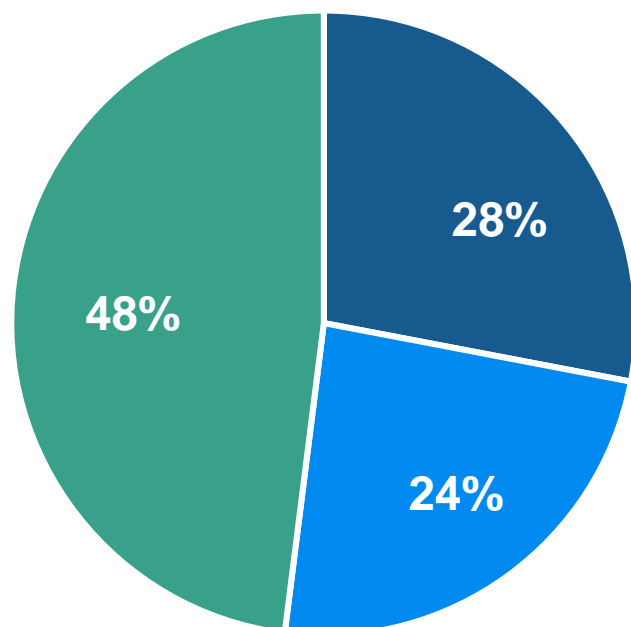
First Half 2017



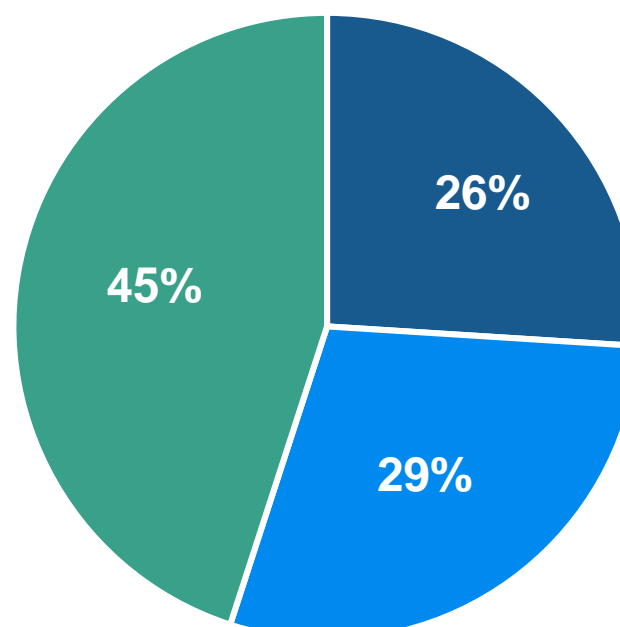
Reflects first half revenue by segment and as reported on Form 8-K on July 27, 2017.

# Revenue by Segment – Advanced Threat Breakout

First Half 2016

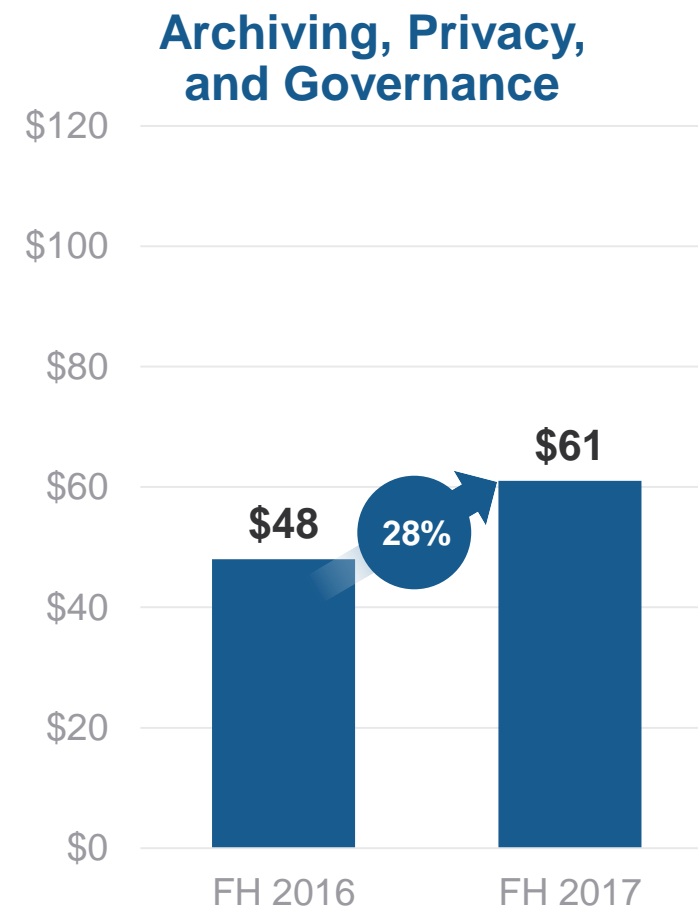
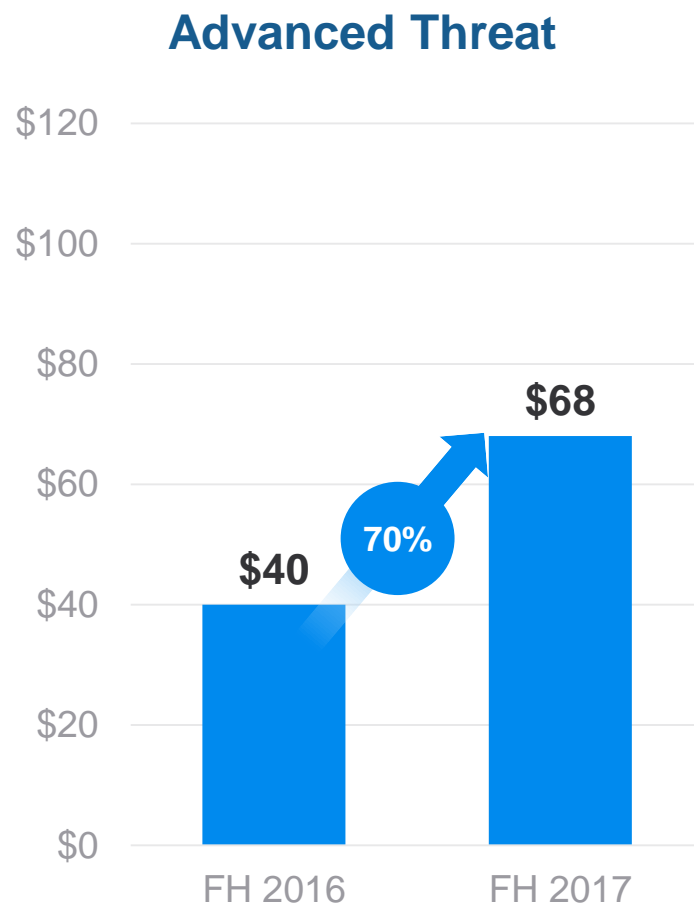
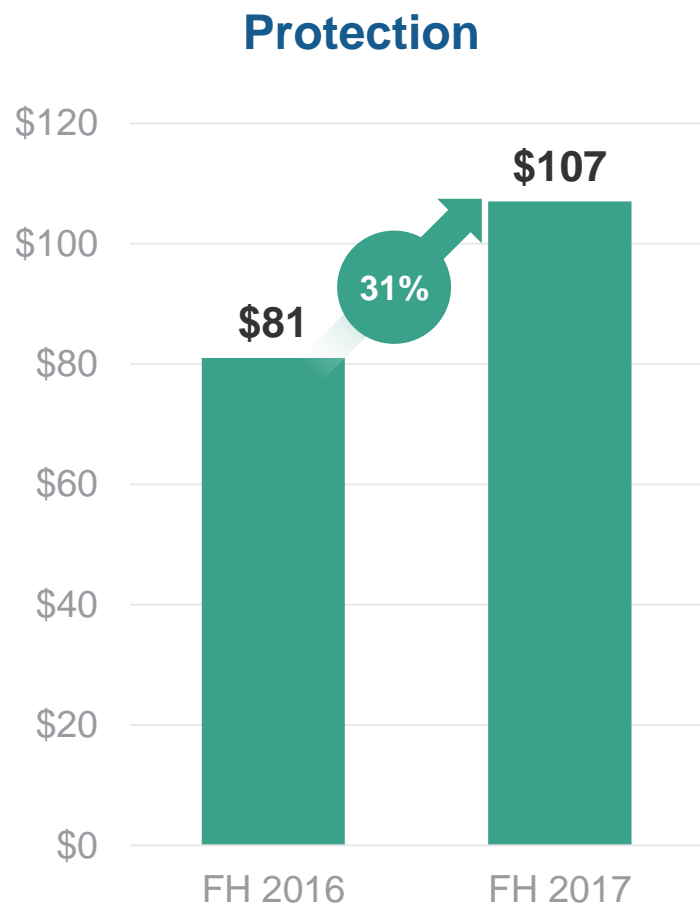


First Half 2017



Advanced Threat breakout represents best estimate for relative distribution of revenue within the Protection and Advanced Threat revenue segment reported on Form 8K on July 27, 2017.

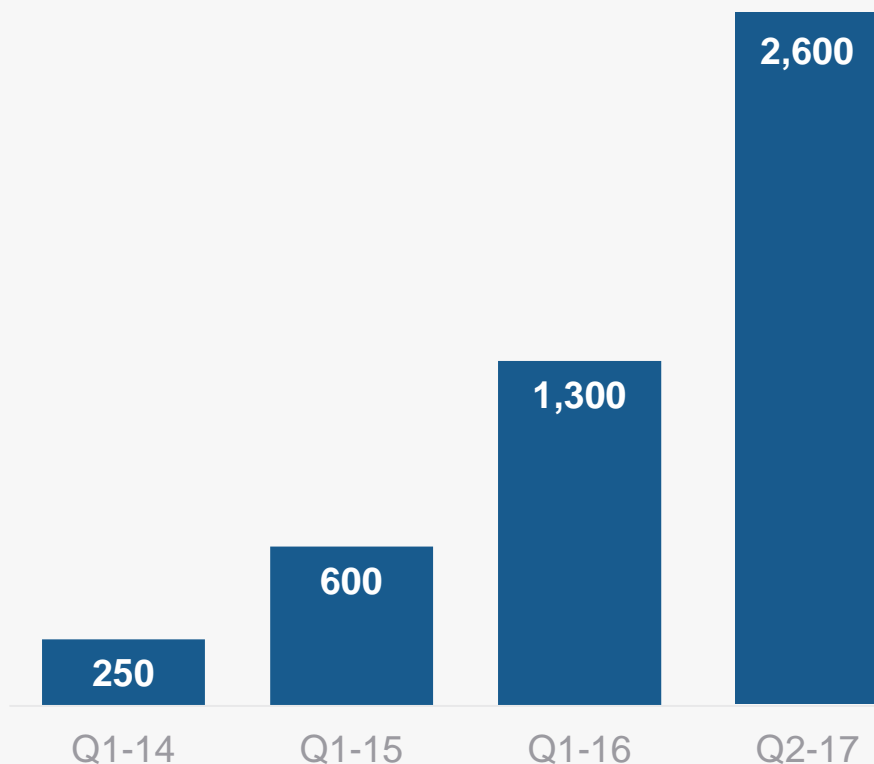
# Revenue by Segment



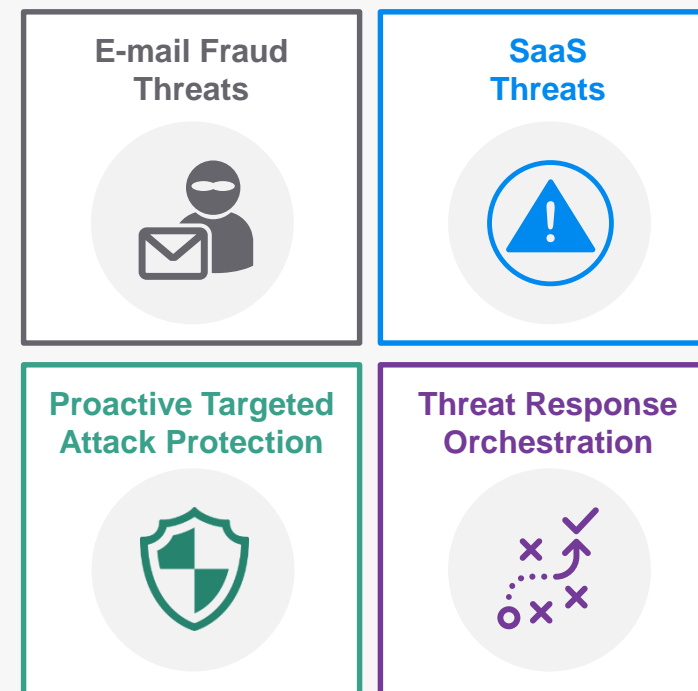
Advanced Threat breakout represents best estimate for revenue within the Protection and Advanced Threat revenue segment reported on Form 8K on July 27, 2017. All numbers in \$ millions.

# Summary: Extending the TAP Franchise

## Growing Our Lead and Market Share with TAP



## Leveraging TAP to Drive Adoption of Emerging Products



# Emerging Products – Driving \$4B Opportunity

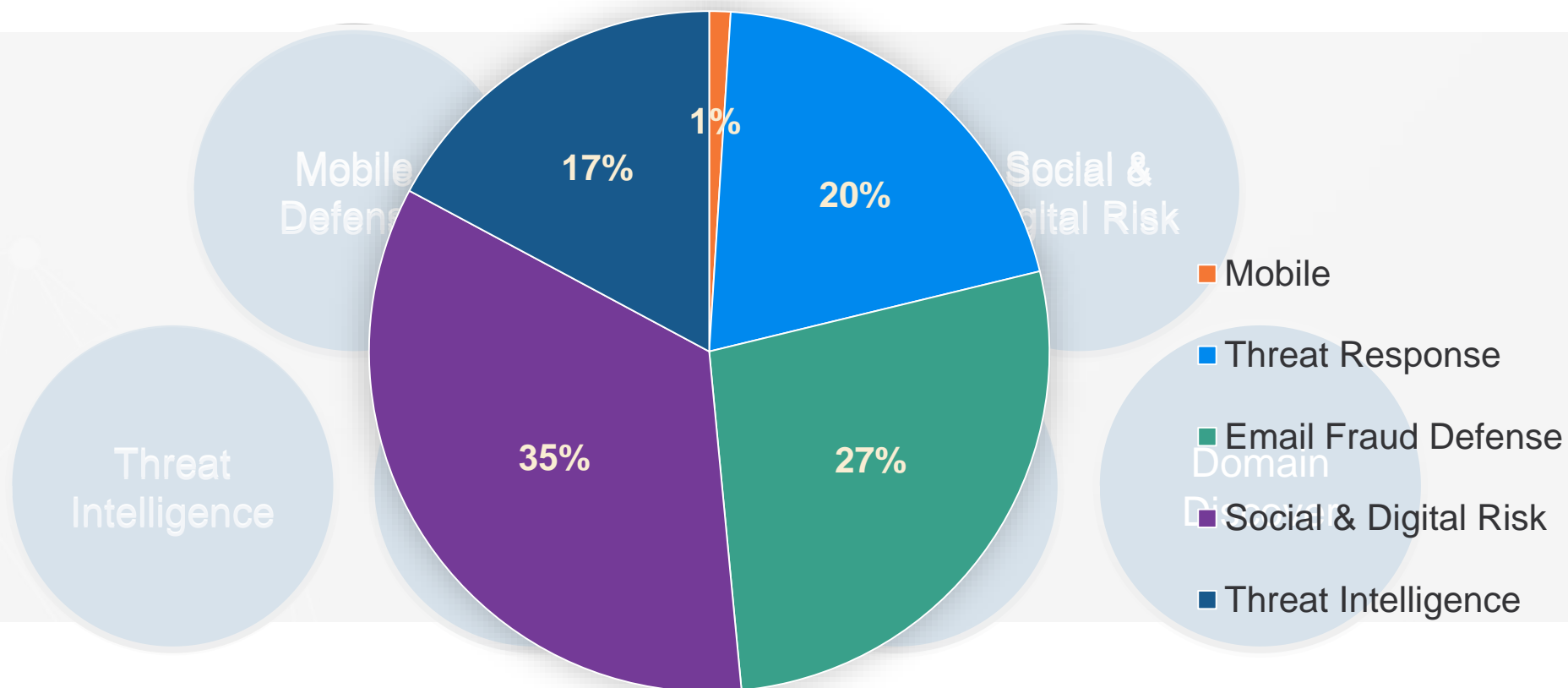
> 10% of new ARR added past 3 quarters and up over 100% Y/Y



# Emerging Products – Driving \$4B Opportunity

> 10% of new ARR added past 3 quarters and up over 100% Y/Y

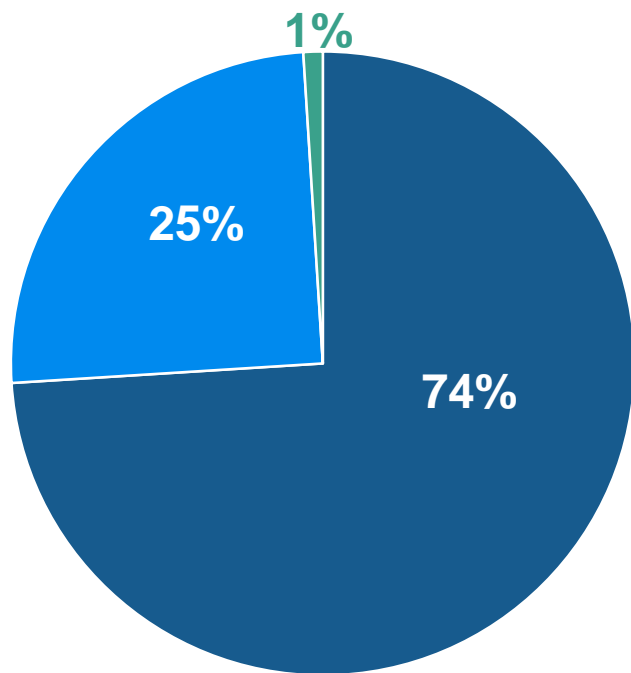
% ARR Split Within Emerging Products



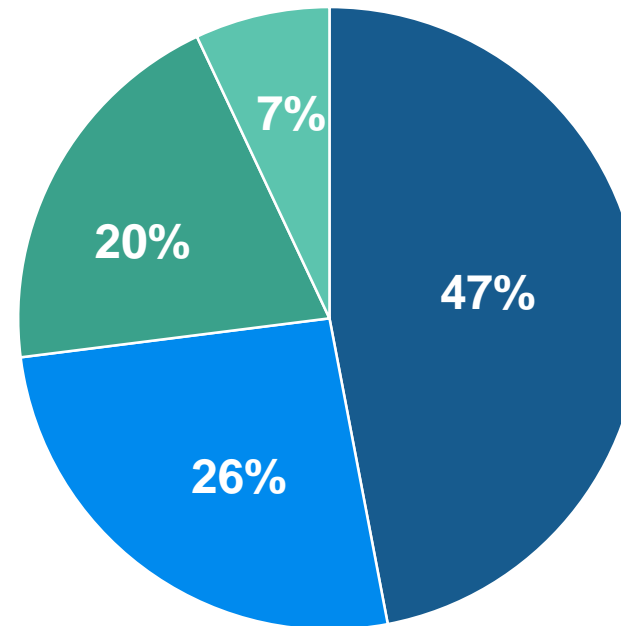
# Blue Chip Customers with Significant Growth

Strong attach rate of additional products into the customer base since IPO

**At Time of 2012 IPO**  
(~2,400 Customers)



**Q2 2017**  
(~5,900 Customers)



- 1 Product
- 2 Products
- 3 Products
- 4 Products



# Blue Chip Customers with Significant Growth

Strong attach rate of additional products into the customer base since IPO

**At Time of 2012 IPO**  
(~2,400 Customers\*)


**Q2 2017**  
(~5,900 Customers)

1 Product	74% (~1,800)		47% (~2,800)
2 Products	24% (~600)		26% (~1,500)
3 Products	1% (~25)		20% (~1,200)
4+ Products	N/A		7% (~400)

\*Numbers don't tie due to rounding.

# Blue Chip Customers with Significant Growth

Strong attach rate of additional products into the customer base since IPO

	At Time of 2012 IPO % New ARR Booked		Q2 2017 % New ARR Booked
	1H 2012		1H 2017
1 Product	77%		27%
2 Products	22%		30%
3+ Products	1%		43%

# Significant Opportunity to Fill in Whitespace

**\$1 Billion**

opportunity to sell deeper  
into existing customer base of ~5,900

**47%** have **one** product

**26%** have **two** products

**27%** have **three** or more products

**~\$500M**

ARR Under Contract

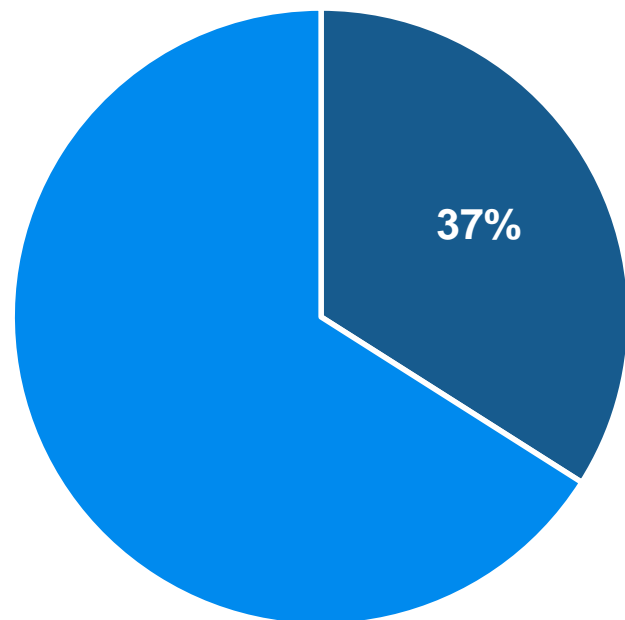
**\$1.0B**

ARR Still Available

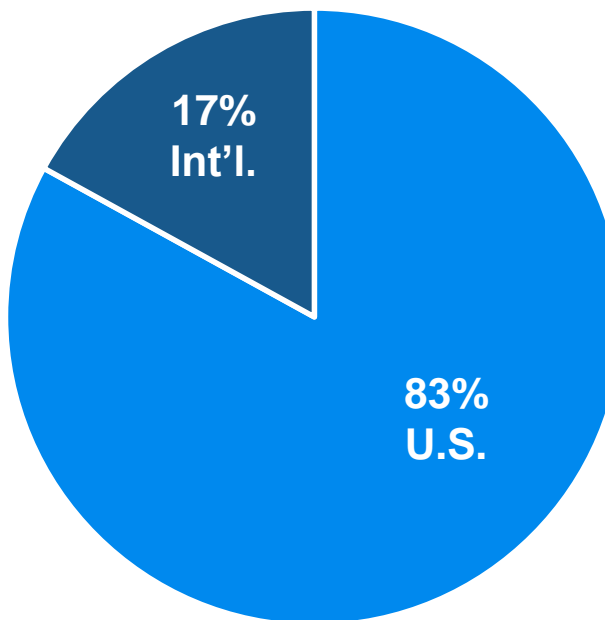
# Blue Chip Customers with Significant Growth

Strong attach rate of additional products into the customer base since IPO

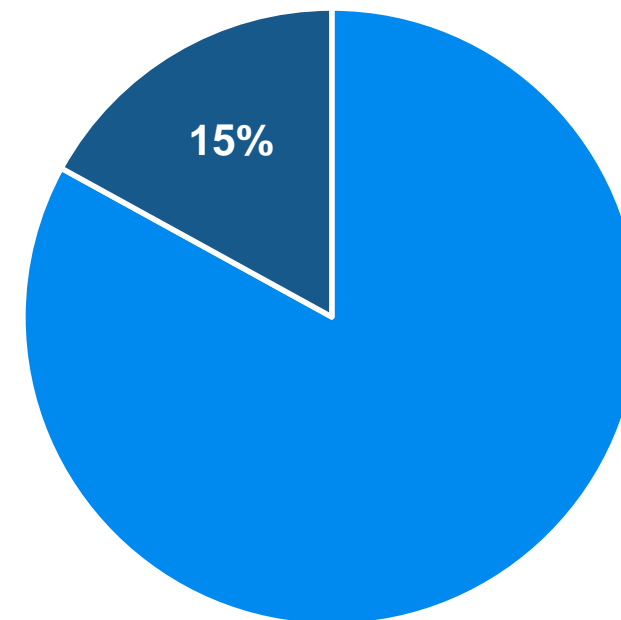
F-1000 Penetration



U.S. vs. International Revenue



Global 2000



Reflects Q2 2017 results.

# 2020 Operating Model

	2020E (2016 Analyst Day)	2020E (2017 Analyst Day)
Revenue	\$950M - \$1,050M	\$1,025M - \$1,100M
Non-GAAP Gross Margin	77%–79%	77%–79%
Non-GAAP Operating Margin	13%–15%	13%–15%
Free Cash Flow As % of revenue	\$250M 24–26%	~\$266M 24–26%

- 2020E provided at 2016 Analyst and Investor Day on June 8, 2016.
- Non-GAAP Gross Profit is defined as GAAP Gross Profit, adjusted to exclude stock-based compensation expense and the amortization of intangibles associated with acquisitions; see appendix for reconciliation.
- Non-GAAP Operating Margin is defined as GAAP Operating Margin, adjusted to exclude stock-based compensation expense and the amortization of intangibles and costs associated with acquisitions and litigation; see appendix for reconciliation.
- Free Cash Flow is defined as net cash provided by operating activities minus capital expenditures.
- With available NOLs we should not be a regular tax cash taxpayer in the US through 2020 – AMT cash taxes may apply.
- 2020E Free Cash Flow calculated at the midpoint of the revenue range.
- We are not providing a GAAP to Non-GAAP reconciliation to the 2020 Operating Model update because we are not able to present reconciling items without unreasonable effort due to potentially high variability, complexity and low visibility as to the items that would be excluded from the GAAP measures, such as stock-based compensation expenses, the impact and timing of potential acquisitions, potential litigation expenses, and capital expenditures. The actual amounts of such reconciling items will have a significant impact on the company's GAAP results.

# 2020 Prospective Revenue Mix by Segment

	2020 Revenue (\$M) (2016 Analyst Day)	2020 Revenue (\$M) (2017 Analyst Day)	Market Share
Protection and Advanced Threat	\$650–\$700	\$650–\$700	17%–18%
Archiving, Privacy, and Governance	\$205–\$225	\$205–\$225	6%–7%
Emerging Products	\$85–\$105	\$155–\$160	
Hardware and Services	\$10–\$20	\$10–\$20	
<b>Total</b>	<b>\$950–\$1,050</b>	<b>\$1,025–\$1,100</b>	

# In Closing

- 1** Consistent track record of execution over the past 22 quarters as a public company
- 2** Compelling business model, with 98% recurring revenues and duration in the low teens
- 3** Strong operating discipline, delivering both growth and expanding free cash flow margins
- 4** Broad customer base with renewal rates consistently over 90%
- 5** Emerging products create yet another catalyst for growth

A photograph of two men in a modern office environment. The man on the left, wearing a white button-down shirt, is leaning over a laptop. The man on the right, wearing a light blue button-down shirt and glasses, is holding a pen and looking at the laptop. A black coffee cup is on the table. The background shows large windows with a view of a city.

**proofpoint.**

# Closing Remarks

Gary Steele  
Chief Executive Officer

**ANALYST DAY 2017**



# Summary of Highlights from the Day

Leading the industry in protecting the way people work today

Leveraging the cloud to deliver a robust suite of security and compliance capabilities, all based on a common platform

Consistently executing with compelling growth and increasing cash flow and profitability

Continuing to innovate with new products delivering additional growth catalysts

**proofpoint**<sup>TM</sup>



# Non-GAAP Reconciliations

## Reconciliation of Non-GAAP Measures (In millions) (Unaudited)

	Twelve Months Ending December 31, 2017E
GAAP gross profit	\$359.7 - \$362.9
GAAP gross margin (%)	72%
Plus:	
Stock-based compensation expense	14.8 - 14.0
Intangible amortization expense	12.8 - 12.7
Non-GAAP gross profit	\$387.3 - \$389.6
Non-GAAP gross margin (%)	77.0%
GAAP operating loss	
Plus:	
Stock-based compensation expense	
Intangible amortization expense	
Acquisition-related expenses	
Litigation-related expenses	
Non-GAAP operating income	
Revenues	\$503.0 - \$506.0
Non-GAAP Operating Margin (%)	

# Non-GAAP Reconciliations

## Reconciliation of GAAP Cash Flows from Operations to Free Cash Flows

(in millions)

(Unaudited)

Twelve Months Ended  
December 31,

	2012	2013	2014	2015	2016	2017E
GAAP cash flows provided by operating activities	\$ 6.8	\$ 12.6	\$ 22.6	\$ 46.5	\$ 94.2	\$144.0 - \$153.0
Less:						
Purchases of property and equipment	\$ (5.9)	\$ (7.6)	\$ (15.0)	\$ (25.8)	\$ (34.4)	\$(44.0) - \$(46.0)
Non-GAAP free cash flows	\$ 0.9	\$ 5.0	\$ 7.6	\$ 20.7	\$ 59.8	\$100.0 - \$107.0
GAAP revenue	\$ 106.3	\$ 137.9	\$ 195.6	\$ 265.4	\$ 375.5	\$503.0 - \$506.0
Free Cash Flows as percentage of Revenue	1%	4%	4%	8%	16%	21%

# Appendix

## Source Data for Market Size Estimates on Slides 17 and 18

### Sources:

1. IDC: Worldwide IT Security Products Forecast, 2017–2020: Comprehensive Security Products Forecast Review (March 2017)
2. IDC: Worldwide Archiving Software Forecast, 2017–2021: Generating Growth Through Higher-Value Engagements (May 2017)
3. Gartner: Forecast: Information Security, Worldwide, 2015-2021, 1Q17 Update (Q1 2017)
4. Markets and Markets: Email Encryption Market by Deployment Type - Global Forecast to 2020 (November 2015)
5. IDC: Worldwide Specialized Threat Analysis and Protection Forecast, 2016–2020: Enterprises Modernize Security Infrastructure (Dec 2016)
6. IDC: Worldwide Mobile Enterprise Security Software Forecast, 2016-2020 (May 2016)
7. IDC: Worldwide Threat Intelligence Security Services Forecast, 2016–2020: Strength in Numbers (March 2016)
8. IDC: Worldwide Security and Vulnerability Management Forecast, 2016–2020: Enterprises Continue Focus on Security Operations (December 2016)
9. Gartner: Forecast Snapshot: Cloud Access Security Broker, Worldwide, 2017 (March 2017)
10. Management Estimate of Social and Digital Risk - \$500 million (September 2017)
11. Management Estimate for Email Authentication - over \$500 million (September 2017)

**proofpoint**<sup>TM</sup>

