Exploring Human Risk

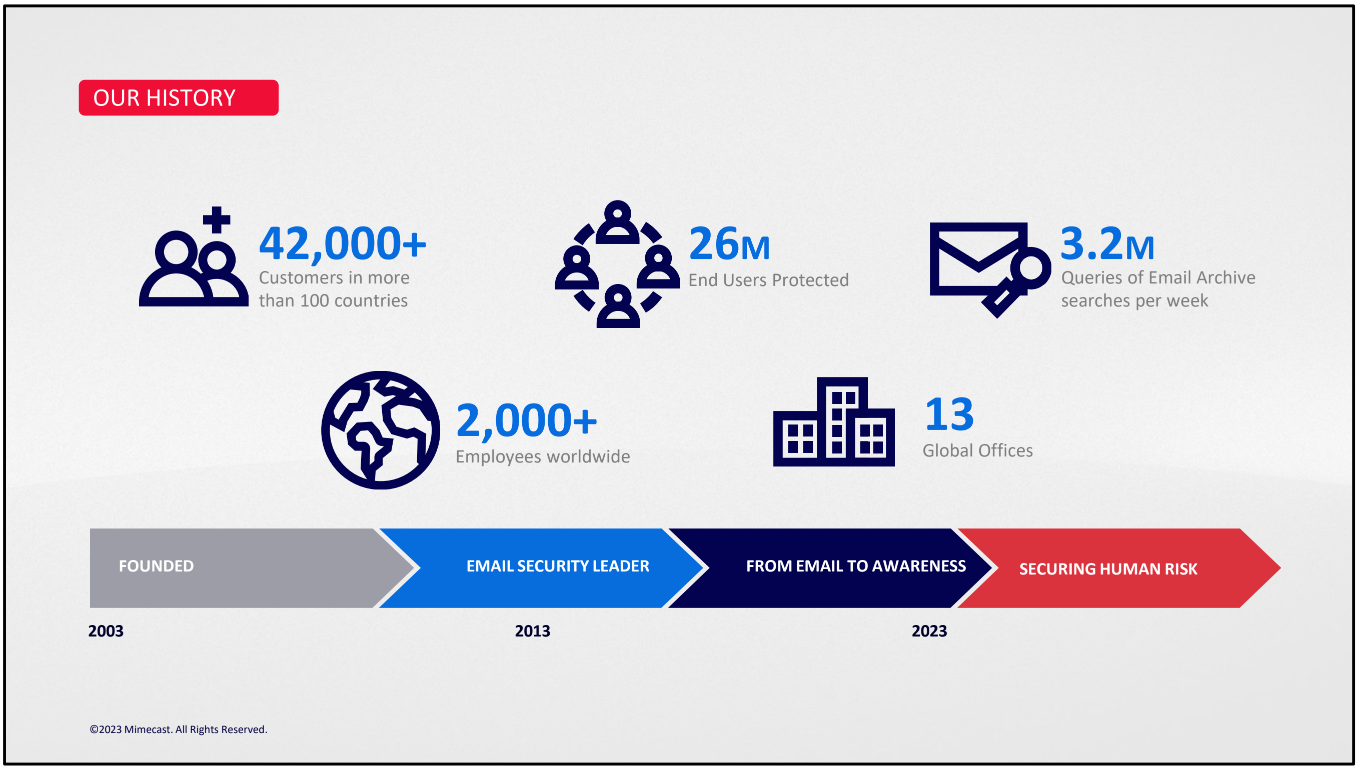
Harpreet Singh

Senior Sales Engineer

Mimecast

mimecast
PARTNER ONE

I'm Harpreet, SSE at Mimecast. Over my career, I've directly with the tech, with people and supporting sales functions and my recent roles in my career blends both together which gives me a unique view over how organisations are faced with an ever changing threat landscape. So today we will exploring everything to do with Human risk, what exactly is it, how do we expose it and what to mitigate it. But before we do that, who is Mimecast…



OUR HISTORY

42,000+
Customers in more than 100 countries

26M
End Users Protected

3.2M
Queries of Email Archive searches per week

2,000+
Employees worldwide

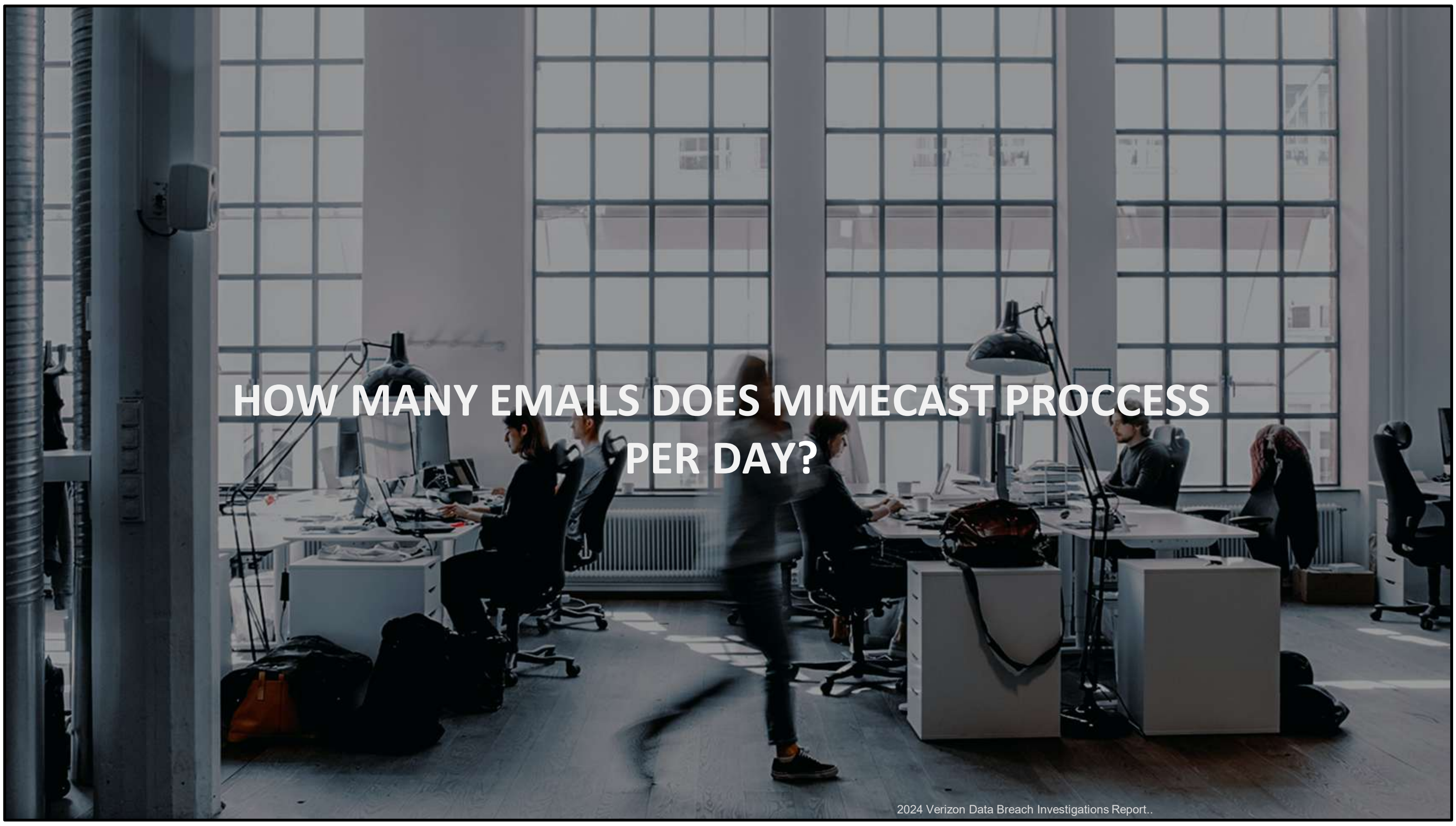
13
Global Offices

FOUNDED → EMAIL SECURITY LEADER → FROM EMAIL TO AWARENESS → SECURING HUMAN RISK

2003 2013 2023

Today, Mimecast is a human risk management platform but we didn’t start off that way. Mimecast was founded over 2 decades in 2003 as a email security solution, then as times moved on and more advanced threats were being faced by customers, we adapted with multi-layer, AI/ML enabled technologies to catch advanced threats.

since 2013, we saw that the risk was shifting from the tech to the users, humans, us guys and we moved into user awareness and human risk. Today, we secure over 42k orgs over 100 countries. Now you have some stats on the screen here and we’re going to check if the caffeine has hit your system yet as I am going to as you ladies and gents a question.. And that question is…



HOW MANY EMAILS DOES MIMECAST PROCCESS PER DAY?

2024 Verizon Data Breach Investigations Report..

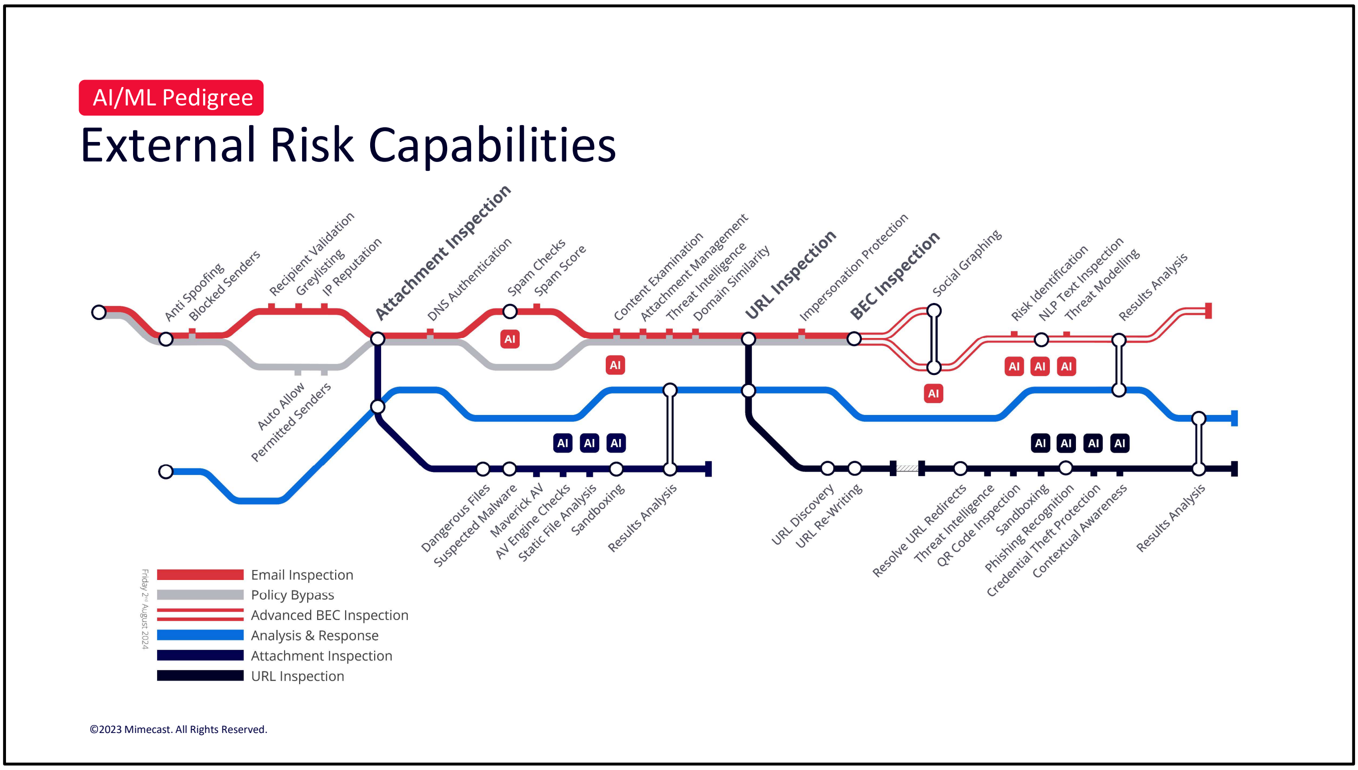
1.5 Billion

EMAILS PROCCESSED DAILY

2024 Verizon Data Breach Investigations Report..

- Which is a LOT of emails. But that also gives a great opportunity to view the treasure trove of data which we will be exploring.

- Each one of those emails goes through our AI/ML enabled multi layer scanning engines…



AI/ML Pedigree

External Risk Capabilities

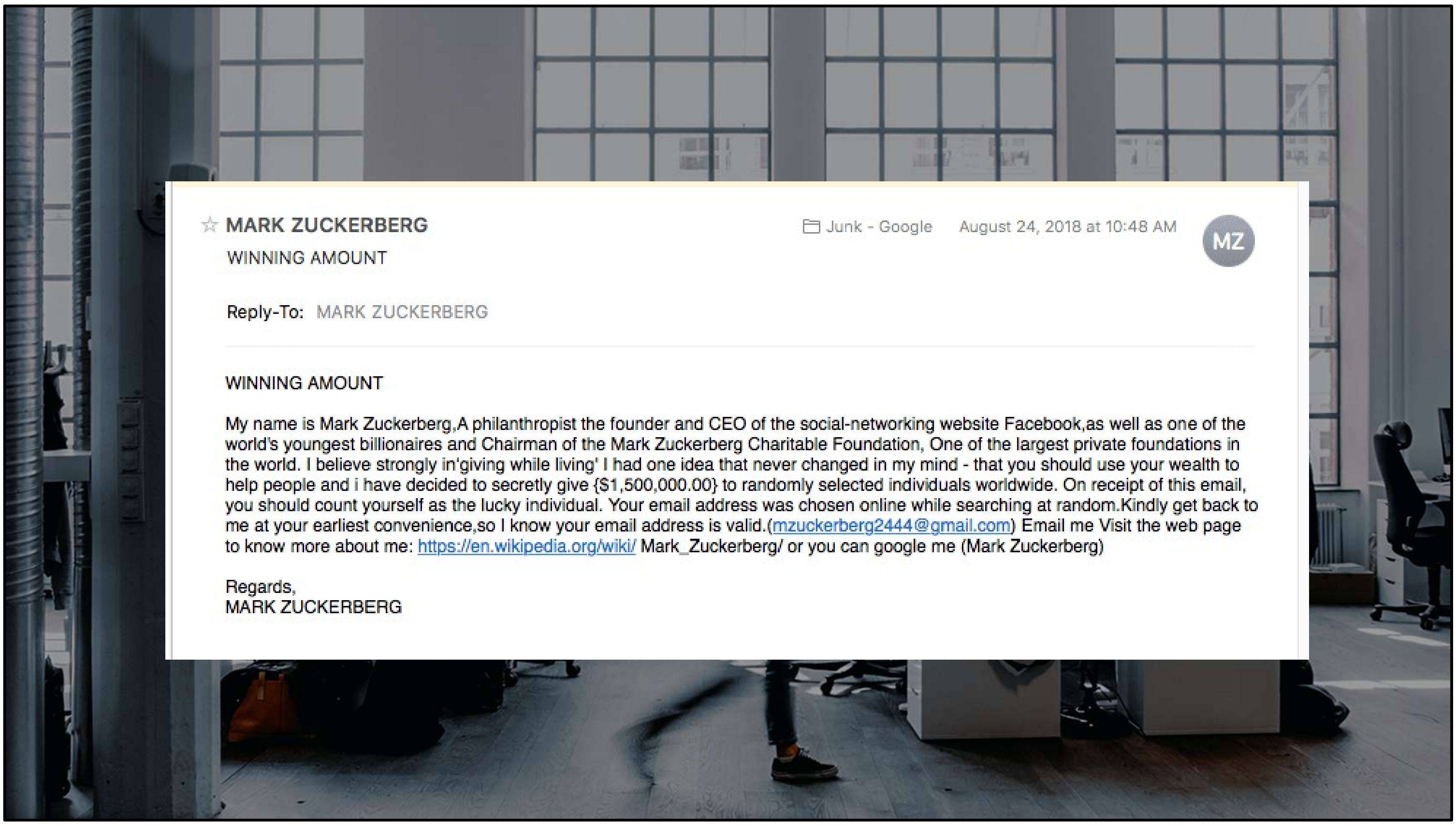
Email Inspection
Policy Bypass
Advanced BEC Inspection
Analysis & Response
Attachment Inspection
URL Inspection

Friday 2nd August 2024

Everything from sandboxing attachments to detecting advanced impersonation right down to NLP extraction to read the sentiment of an email.

AS AN ENGINEER, spend all day talking about each individual part of this but point to takeaway, an email does not have to be technically advanced to do LOT of damage. analysing threats all day everyday, we realized that the attacks that has done the most reputational and financial damage, have no attachment, a virus or URLs. They caused a major breach because what they were able to do was incite trust in the target, they knew the responsibilities of an individual, when someone was out of the office by monitoring out of office replies, alongside knowing who they worked with through siphoning off information from the likes of LinkedIn.

NOW, having said that, some of the emails coming in look like this….



☆ MARK ZUCKERBERG

WINNING AMOUNT

Junk - Google August 24, 2018 at 10:48 AM

MZ

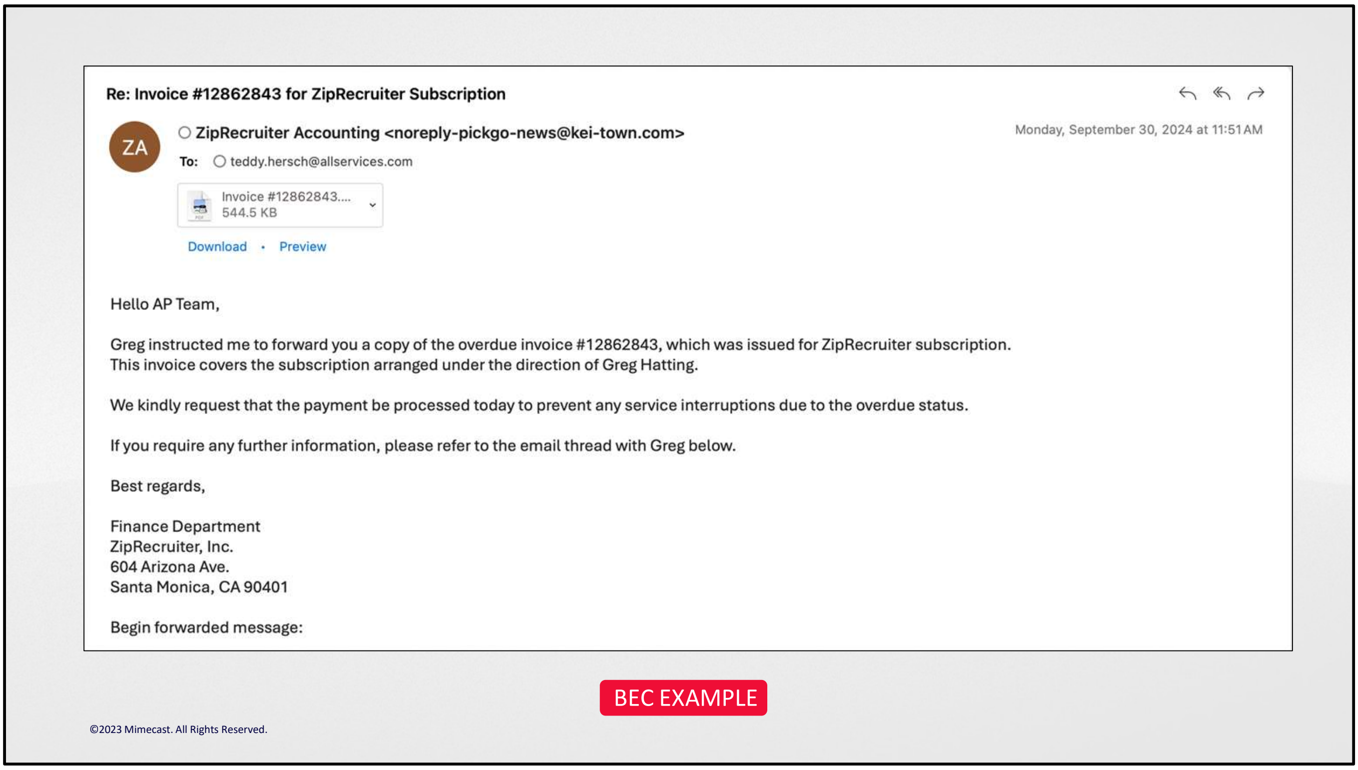
Reply-To: MARK ZUCKERBERG

WINNING AMOUNT

My name is Mark Zuckerberg,A philanthropist the founder and CEO of the social-networking website Facebook,as well as one of the world's youngest billionaires and Chairman of the Mark Zuckerberg Charitable Foundation, One of the largest private foundations in the world. I believe strongly in'giving while living' I had one idea that never changed in my mind - that you should use your wealth to help people and i have decided to secretly give {$1,500,000.00} to randomly selected individuals worldwide. On receipt of this email, you should count yourself as the lucky individual. Your email address was chosen online while searching at random.Kindly get back to me at your earliest convenience,so I know your email address is valid.(mzuckerberg2444@gmail.com) Email me Visit the web page to know more about me: https://en.wikipedia.org/wiki/ Mark_Zuckerberg/ or you can google me (Mark Zuckerberg)

Regards,
MARK ZUCKERBERG

- if I sent you an email claiming to be mr Zuckerburg himself claiming I’ve got money billions burning a hole in my pocket, would you be able to spot this email as maybe idk slightly fake? Would your users? Yes probably or we sure do hope so.
- WHAT ABOUT THIS ONE..



Re: Invoice #12862843 for ZipRecruiter Subscription

○ **ZipRecruiter Accounting <noreply-pickgo-news@kei-town.com>**

Monday, September 30, 2024 at 11:51 AM

To: ○ teddy.hersch@allservices.com

Hello AP Team,

Greg instructed me to forward you a copy of the overdue invoice #12862843, which was issued for ZipRecruiter subscription.
This invoice covers the subscription arranged under the direction of Greg Hatting.

We kindly request that the payment be processed today to prevent any service interruptions due to the overdue status.

If you require any further information, please refer to the email thread with Greg below.

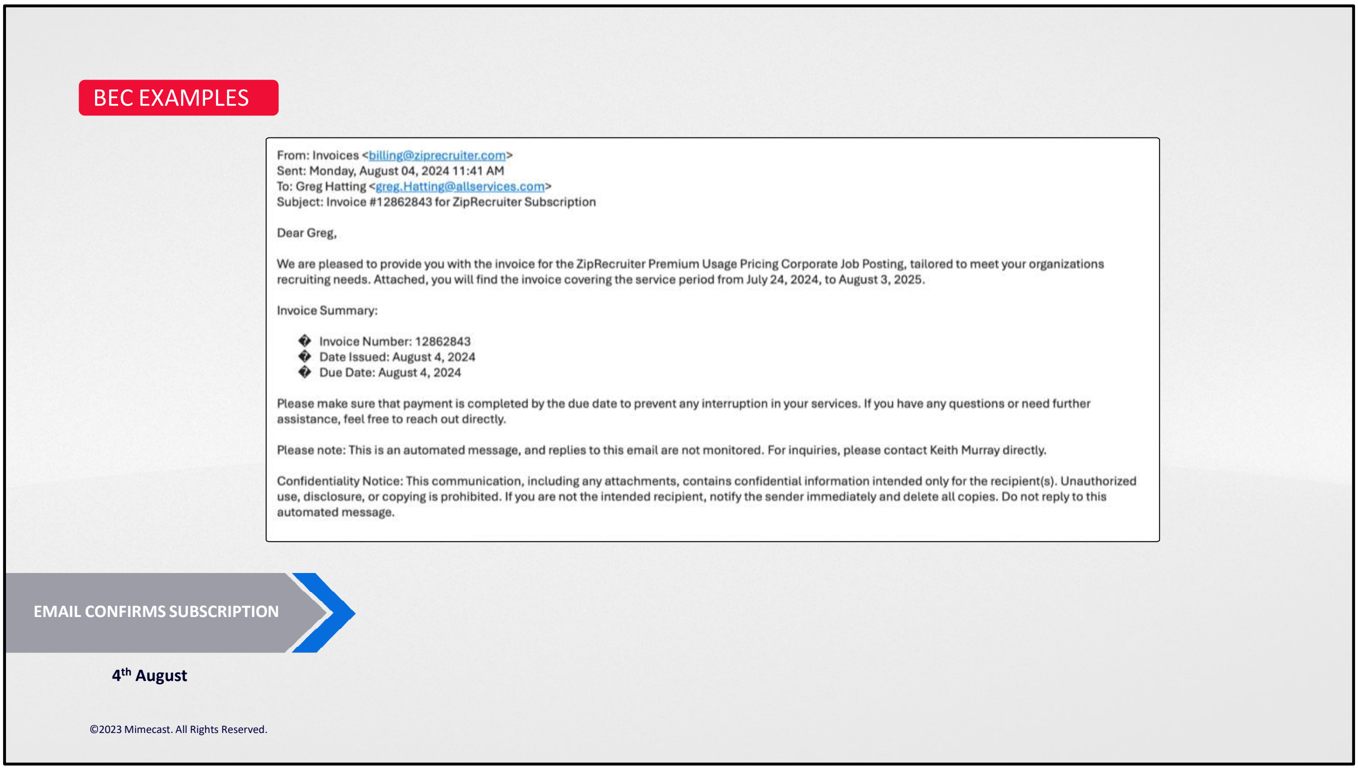
Best regards,

Finance Department
ZipRecruiter, Inc.
604 Arizona Ave.
Santa Monica, CA 90401

Begin forwarded message:

BEC EXAMPLE

Okay, it get's a lot lot trickier, This attack is making use of social engineering to refer to another internal member A lot harder to detect, and a couple second misstep replying to the wrong person and poof, there goes a healthy chunk of change, likely followed by a heart warming conversation with your HR department, So to make things tougher, let's put it into context as this was an actual attack to one of the organisations we support, it has been anonymized of course but these attacks are happening and in large numbers and THEY ARE DIFFERENT EACH TIME, WE CANNOT USE A BLACK OR WHITE RULE BASED APPROACH…



BEC EXAMPLES

From: Invoices <billing@ziprecruiter.com>
Sent: Monday, August 04, 2024 11:41 AM
To: Greg Hatting <greg.Hatting@allservices.com>
Subject: Invoice #12862843 for ZipRecruiter Subscription

Dear Greg,

We are pleased to provide you with the invoice for the ZipRecruiter Premium Usage Pricing Corporate Job Posting, tailored to meet your organizations recruiting needs. Attached, you will find the invoice covering the service period from July 24, 2024, to August 3, 2025.

Invoice Summary:

- � Invoice Number: 12862843
- � Date Issued: August 4, 2024
- � Due Date: August 4, 2024

Please make sure that payment is completed by the due date to prevent any interruption in your services. If you have any questions or need further assistance, feel free to reach out directly.

Please note: This is an automated message, and replies to this email are not monitored. For inquiries, please contact Keith Murray directly.

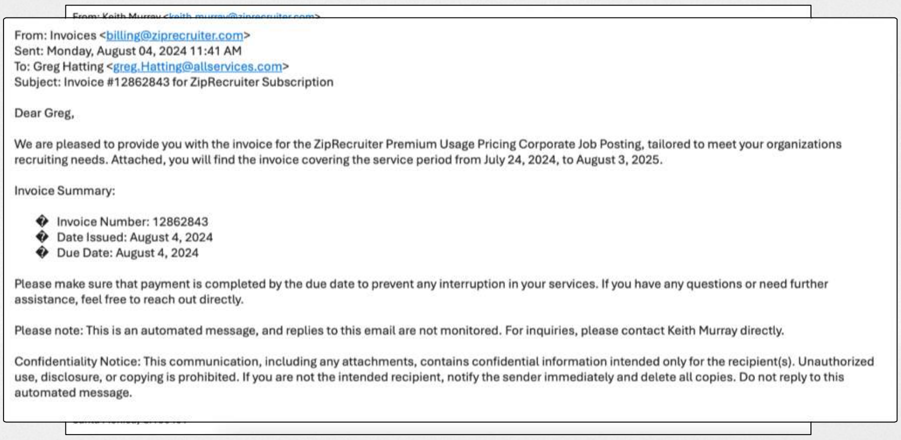
Confidentiality Notice: This communication, including any attachments, contains confidential information intended only for the recipient(s). Unauthorized use, disclosure, or copying is prohibited. If you are not the intended recipient, notify the sender immediately and delete all copies. Do not reply to this automated message.

EMAIL CONFIRMS SUBSCRIPTION

4th August

Ziprecuriter is TARGETTING all services. gentleman called Teddy however does not appearance until later. They send an email supposedly to Greg who is a legitimate employee in the business and works with Teddy.

BEC EXAMPLES



From: Keith Murray <keith.murray@ziprecruiter.com>

From: Invoices <billing@ziprecruiter.com>
Sent: Monday, August 04, 2024 11:41 AM
To: Greg Hatting <greg.Hatting@allservices.com>
Subject: Invoice #12862843 for ZipRecruiter Subscription

Dear Greg,

We are pleased to provide you with the invoice for the ZipRecruiter Premium Usage Pricing Corporate Job Posting, tailored to meet your organizations recruiting needs. Attached, you will find the invoice covering the service period from July 24, 2024, to August 3, 2025.

Invoice Summary:

- � Invoice Number: 12862843
- � Date Issued: August 4, 2024
- � Due Date: August 4, 2024

Please make sure that payment is completed by the due date to prevent any interruption in your services. If you have any questions or need further assistance, feel free to reach out directly.

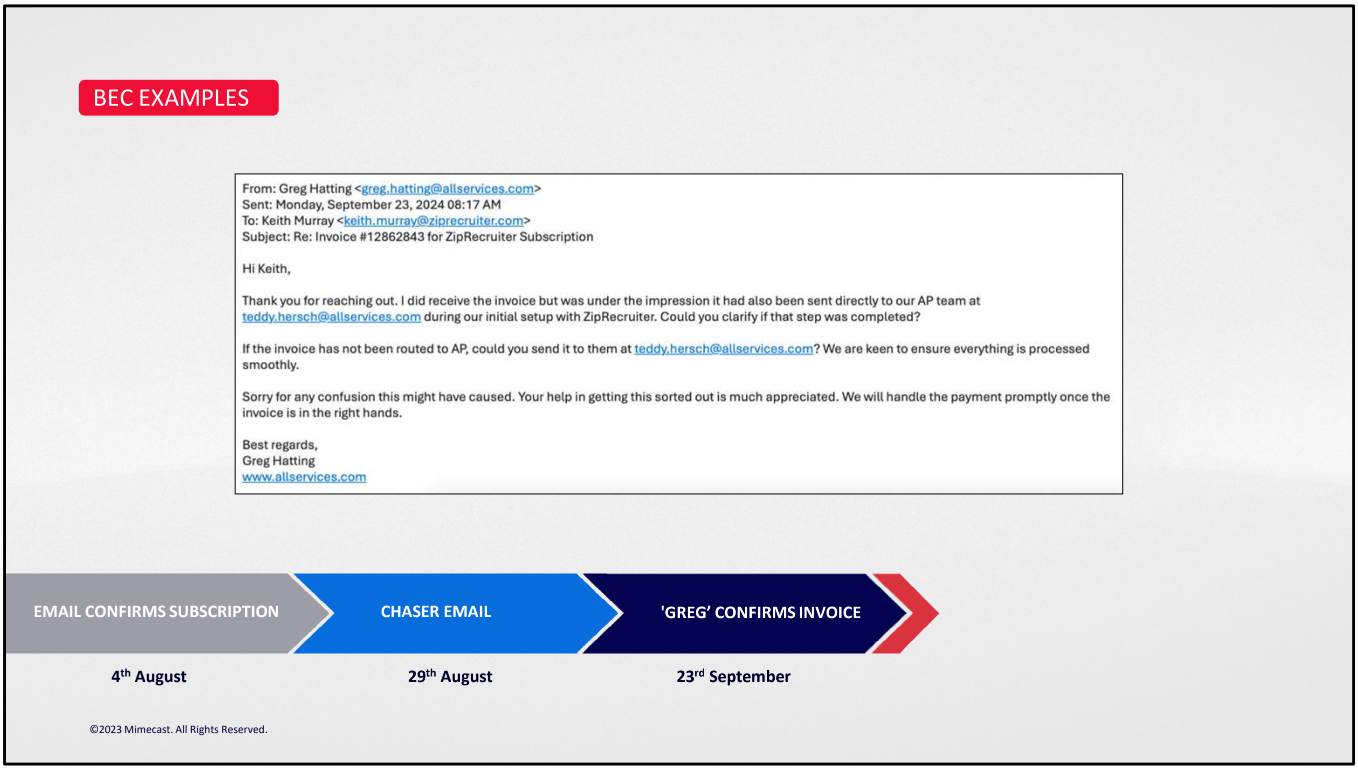
Please note: This is an automated message, and replies to this email are not monitored. For inquiries, please contact Keith Murray directly.

Confidentiality Notice: This communication, including any attachments, contains confidential information intended only for the recipient(s). Unauthorized use, disclosure, or copying is prohibited. If you are not the intended recipient, notify the sender immediately and delete all copies. Do not reply to this automated message.

EMAIL CONFIRMS SUBSCRIPTION
CHASER EMAIL

4th August **29th August**

Greg is emailed again from Ziprecruiter as a reminder to pay the invoice.



BEC EXAMPLES

From: Greg Hatting <greg.hatting@allservices.com>
Sent: Monday, September 23, 2024 08:17 AM
To: Keith Murray <keith.murray@ziprecruiter.com>
Subject: Re: Invoice #12862843 for ZipRecruiter Subscription

Hi Keith,

Thank you for reaching out. I did receive the invoice but was under the impression it had also been sent directly to our AP team at teddy.hersch@allservices.com during our initial setup with ZipRecruiter. Could you clarify if that step was completed?

If the invoice has not been routed to AP, could you send it to them at teddy.hersch@allservices.com? We are keen to ensure everything is processed smoothly.

Sorry for any confusion this might have caused. Your help in getting this sorted out is much appreciated. We will handle the payment promptly once the invoice is in the right hands.

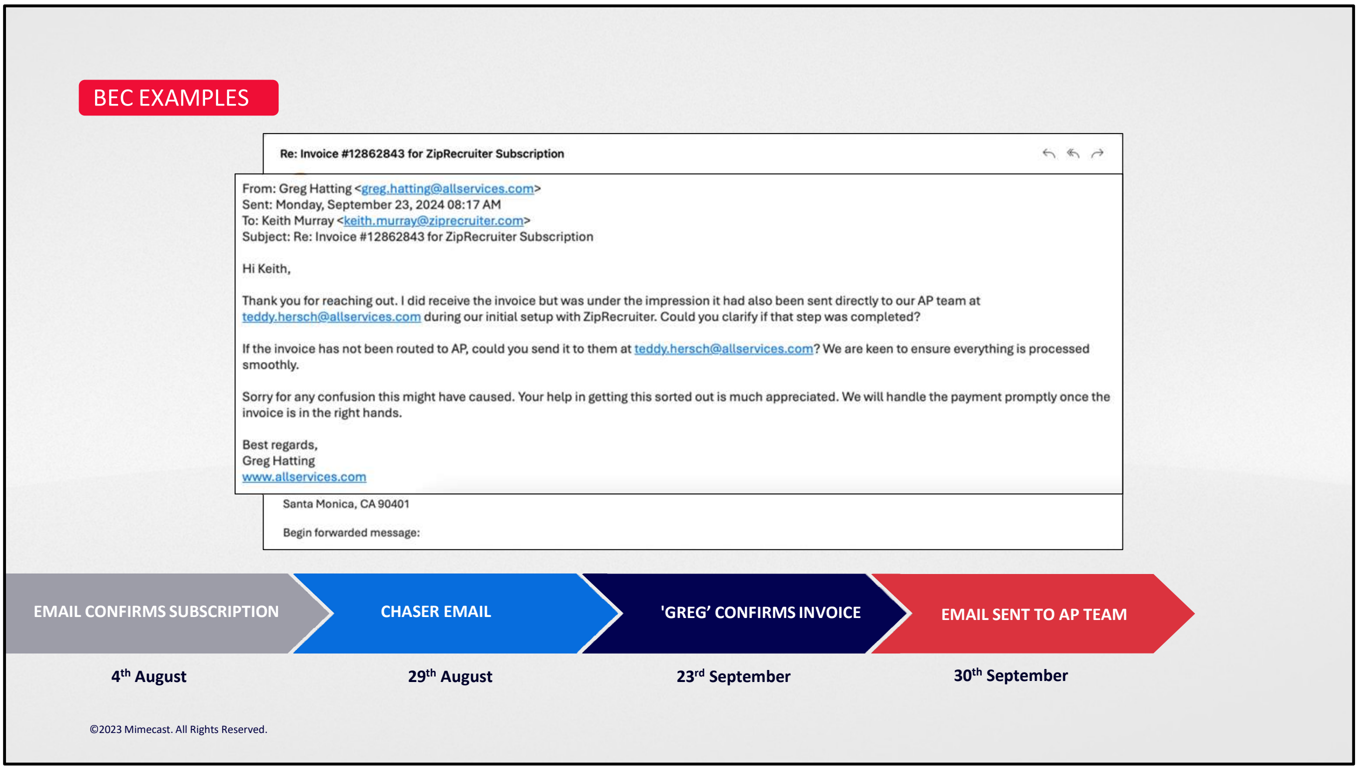
Best regards,
Greg Hatting
www.allservices.com

EMAIL CONFIRMS SUBSCRIPTION — 4th August

CHASER EMAIL — 29th August

'GREG' CONFIRMS INVOICE — 23rd September

Supposedly Greg replies back to the same thread and mentions that in the meeting with ziprecruiter, the invoice should be sent to Teddy in the AP team.



BEC EXAMPLES

Re: Invoice #12862843 for ZipRecruiter Subscription

From: Greg Hatting <greg.hatting@allservices.com>
Sent: Monday, September 23, 2024 08:17 AM
To: Keith Murray <keith.murray@ziprecruiter.com>
Subject: Re: Invoice #12862843 for ZipRecruiter Subscription

Hi Keith,

Thank you for reaching out. I did receive the invoice but was under the impression it had also been sent directly to our AP team at teddy.hersch@allservices.com during our initial setup with ZipRecruiter. Could you clarify if that step was completed?

If the invoice has not been routed to AP, could you send it to them at teddy.hersch@allservices.com? We are keen to ensure everything is processed smoothly.

Sorry for any confusion this might have caused. Your help in getting this sorted out is much appreciated. We will handle the payment promptly once the invoice is in the right hands.

Best regards,
Greg Hatting
www.allservices.com

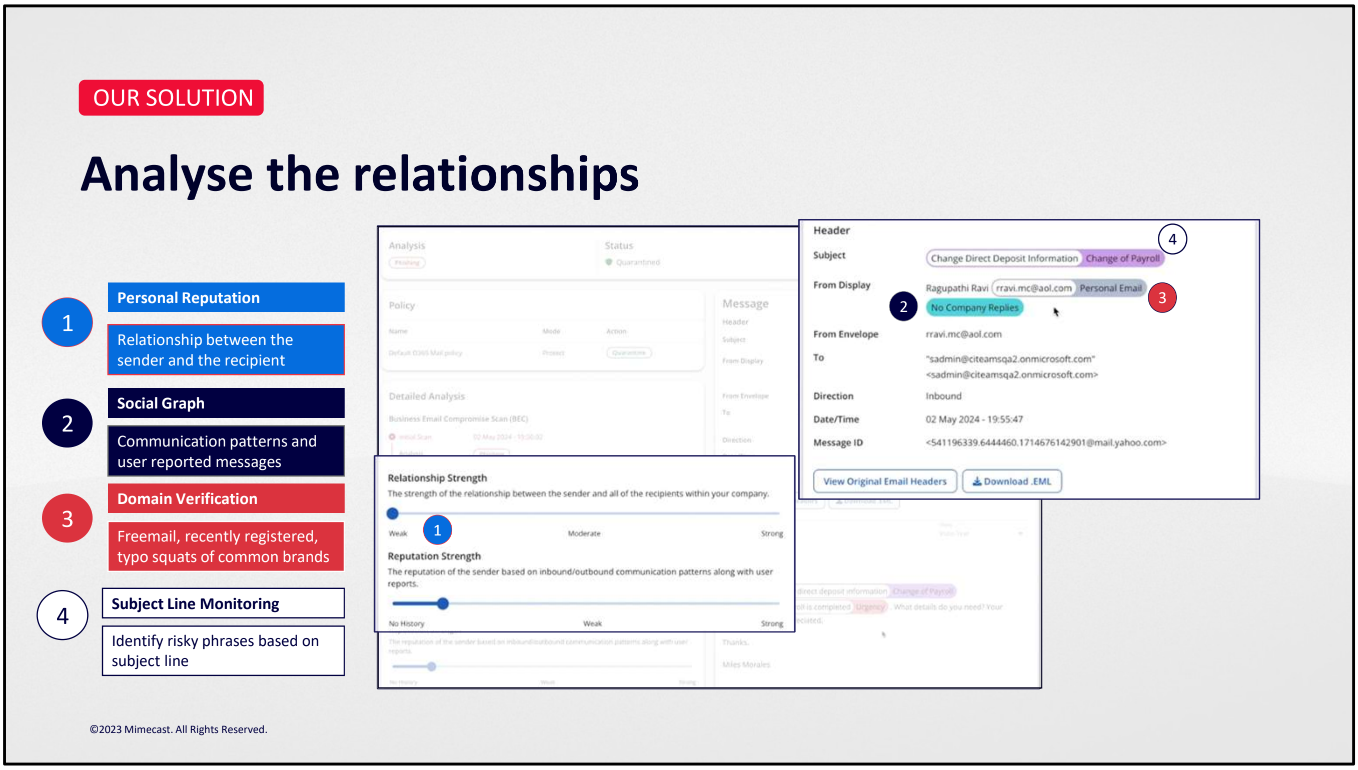
Santa Monica, CA 90401

Begin forwarded message:

An email consisting of the entire thread is sent to an accounts payable employee to finalize the payment with ‘Approval’ from Greg.

Attackers are choosing to build relationships and trust, use unique knowledge about you and everyone you work with to craft detailed email chains.

The question is, are you able to detect these style of attacks? Statistically..



OUR SOLUTION

Analyse the relationships

1 **Personal Reputation**

Relationship between the sender and the recipient

2 **Social Graph**

Communication patterns and user reported messages

3 **Domain Verification**

Freemail, recently registered, typo squats of common brands

4 **Subject Line Monitoring**

Identify risky phrases based on subject line

Relationship Strength

The strength of the relationship between the sender and all of the recipients within your company.

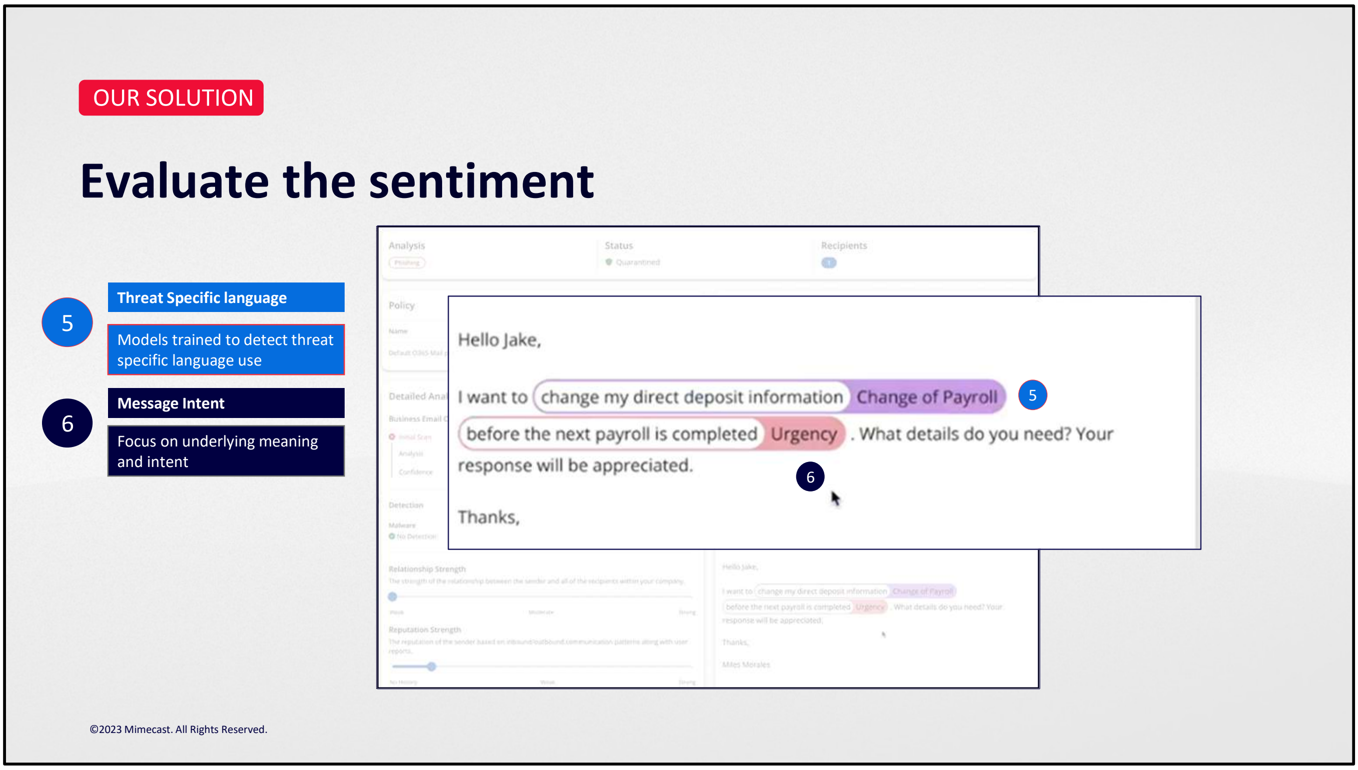
Reputation Strength

The reputation of the sender based on inbound/outbound communication patterns along with user reports.

Header

Subject	Change Direct Deposit Information Change of Payroll
From Display	Ragupathi Ravi rravi.mc@aol.com Personal Email No Company Replies
From Envelope	rravi.mc@aol.com
To	"sadmin@citeamsqa2.onmicrosoft.com" <sadmin@citeamsqa2.onmicrosoft.com>
Direction	Inbound
Date/Time	02 May 2024 - 19:55:47
Message ID	<541196339.6444460.1714676142901@mail.yahoo.com>

How can we then help in these scenarios?



OUR SOLUTION

Evaluate the sentiment

5 **Threat Specific language**

Models trained to detect threat specific language use

6 **Message Intent**

Focus on underlying meaning and intent

Hello Jake,

I want to change my direct deposit information Change of Payroll 5 before the next payroll is completed Urgency . What details do you need? Your response will be appreciated.

6

Thanks,

We have trained our models on messages reported to us by our more than 42,000 customers and have focused our detections on the semantic usage or meaning of the words along with context seen in those messages - the subject line and message body are inspected in the same way.

By using all these indicators improves our resilience to changing attack patterns but will also reduce the number of messages being incorrectly flagged just because they happen use the same keywords. This will result in our BEC protection identifying fewer false positives - which means as an admin you are spending less time releasing messages from the held queue.

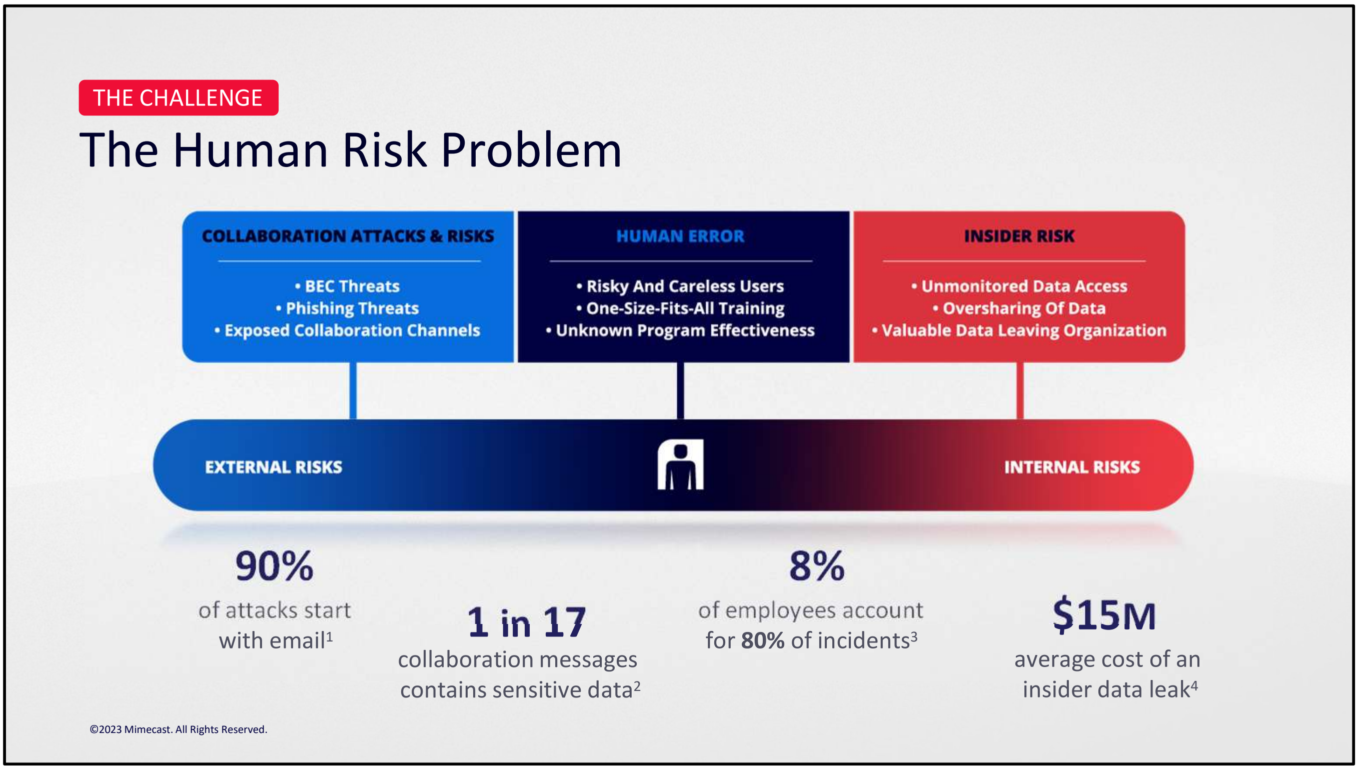
But don't think you lack control - as an admin you can take the final action; do you want to mark the message as safe or remove it?

68%

OF BREACHES INVOLVE THE HUMAN ELEMENT

2024 Verizon Data Breach Investigations Report..

- People are your primary **attack** vector.
  - **68%** of breaches involve the **human** element, and years prior showed similar staggering numbers according to the **verizon** breach report
  - But as our research teams looked closer into **where** this risk was coming from, we began to see that the risk **wasn’t distributed** evenly.



THE CHALLENGE

The Human Risk Problem

COLLABORATION ATTACKS & RISKS

- BEC Threats
- Phishing Threats
- Exposed Collaboration Channels

HUMAN ERROR

- Risky And Careless Users
- One-Size-Fits-All Training
- Unknown Program Effectiveness

INSIDER RISK

- Unmonitored Data Access
- Oversharing Of Data
- Valuable Data Leaving Organization

EXTERNAL RISKS

INTERNAL RISKS

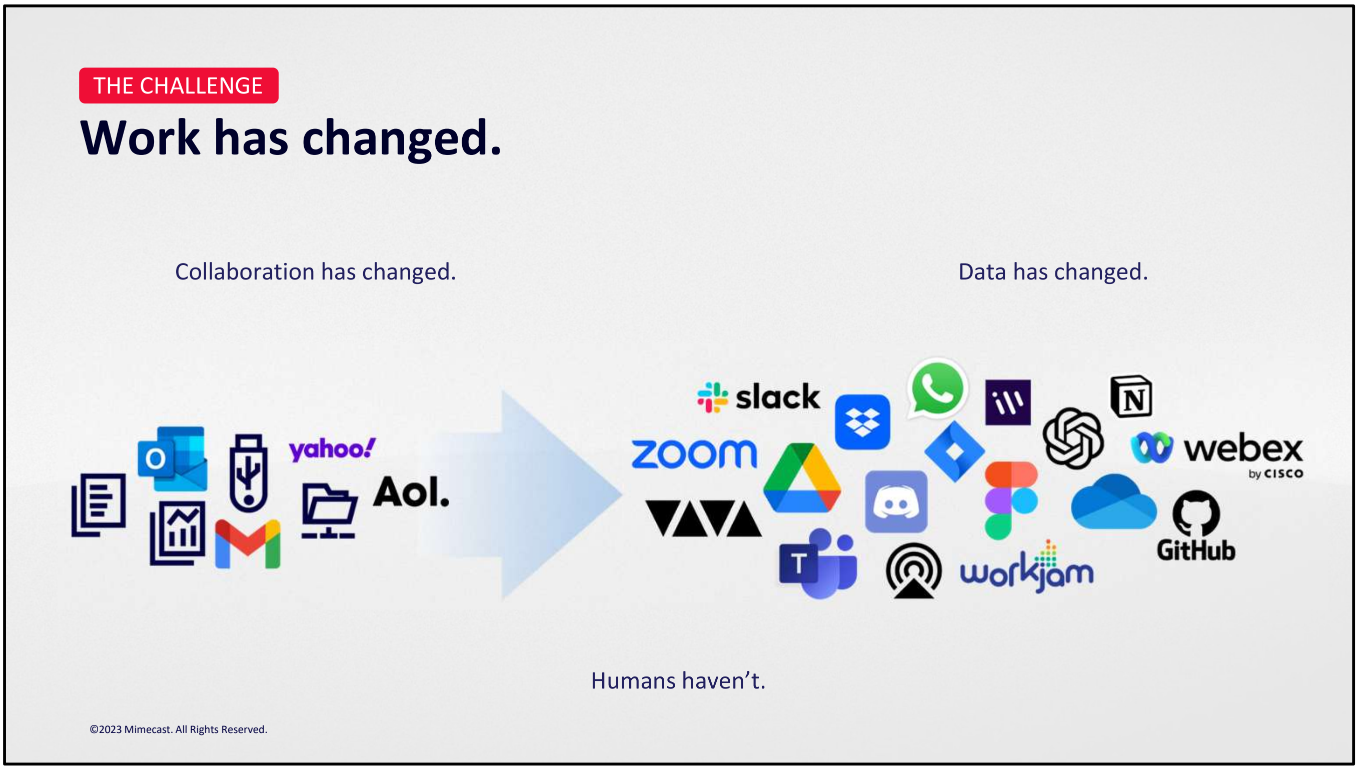
90%
of attacks start with email[1]

1 in 17
collaboration messages contains sensitive data[2]

8%
of employees account for **80%** of incidents[3]

$15M
average cost of an insider data leak[4]

And those numbers paint human risk problem. We have EXTERNAL risk, INTERNAL and center HUMAN RISK. we spoke about identifying insider risk but data leaving your organization may not be a bunch of files attached to an email that an employee who’s handed in their notice is sending to their personal gmail account, it might be a personal DROPBOX account, their ONEDRIVE .. Let me be clear, 90% of all attacks start with email but the fact is that now, with the great cough of 2020 and INCREASE in working from home policies..THE WAY WE WORK…HAS CHANGED.



THE CHALLENGE

Work has changed.

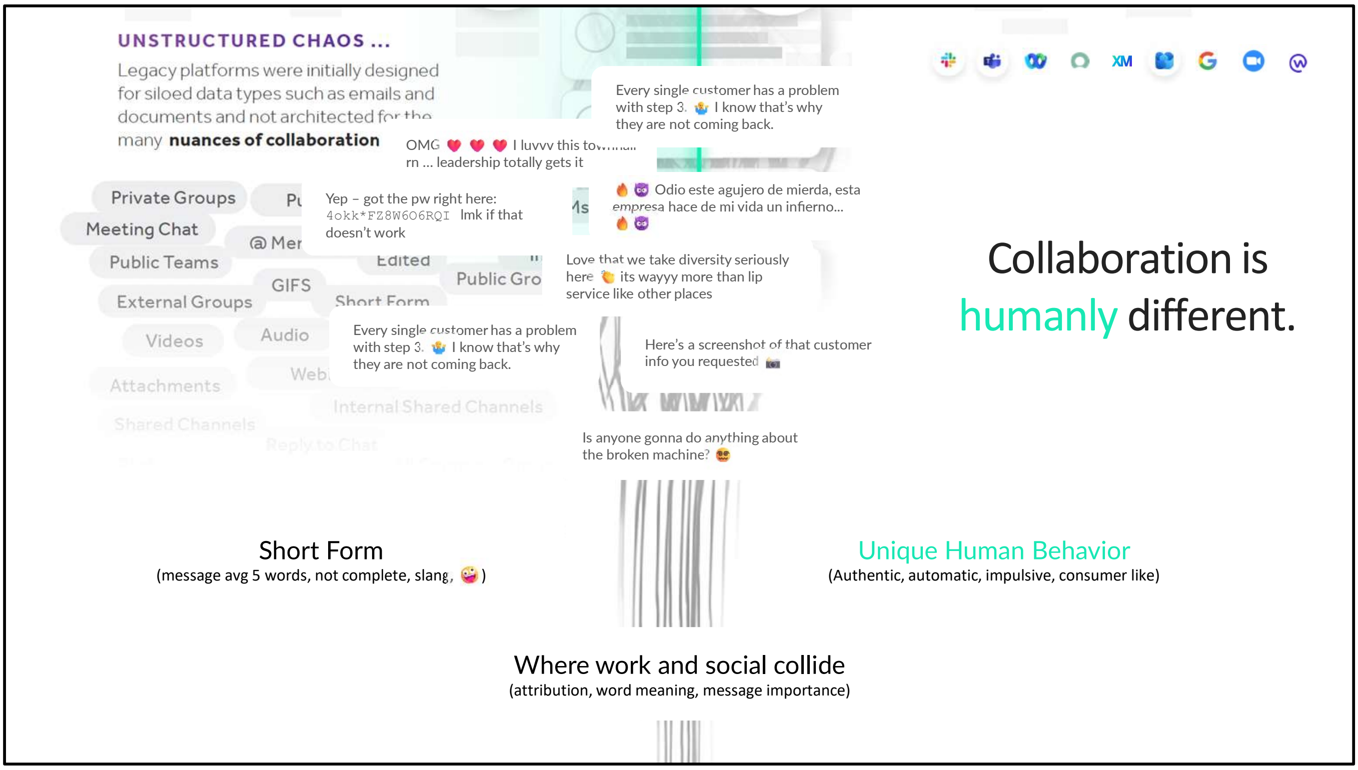
Collaboration has changed.

Data has changed.

Humans haven't.

…has changed. The way we collaborate has changed.. I regularly speak to customers on teams chats because it's quicker and easier than email, I might drop a few memes on slack to colleagues in a lukewarm attempt to be funny, in slightly more serios cases, you might share specialist data such as source code on github repositories

Where our communication is happening has significantly changes, BUT so has the way in which we communicate.. instead of sending an email saying hi Jimmy, please find an invitation for a discussion around security at 4PM. I might actually say…



UNSTRUCTURED CHAOS ...

Legacy platforms were initially designed for siloed data types such as emails and documents and not architected for the many **nuances of collaboration**

Private Groups
Pu
Meeting Chat
@ Mer
Public Teams
Edited
Public Gro
GIFS
External Groups
Short Form
Videos
Audio
Webi
Attachments
Internal Shared Channels
Shared Channels
Reply to Chat

Every single customer has a problem with step 3. 🤷 I know that's why they are not coming back.

OMG ❤️ ❤️ ❤️ I luvvv this town hall rn ... leadership totally gets it

Yep – got the pw right here: `4okk*FZ8W6O6RQI` lmk if that doesn't work

🔥 😈 Odio este agujero de mierda, esta empresa hace de mi vida un infierno... 🔥 😈

Love that we take diversity seriously here 👏 its wayyy more than lip service like other places

Every single customer has a problem with step 3. 🤷 I know that's why they are not coming back.

Here's a screenshot of that customer info you requested 📷

Is anyone gonna do anything about the broken machine? 🤓

Collaboration is humanly different.

Short Form
(message avg 5 words, not complete, slang, 🤪)

Unique Human Behavior
(Authentic, automatic, impulsive, consumer like)

Where work and social collide
(attribution, word meaning, message importance)

.. I might send jimmy a message on teams, you alright for a quick chat at 4 lmk if that works for you? And he might respond back with a thumbs up (I've always thought thumbs up to a response felt like a shutdown but that's not the point)

The point is that in our working lives and in our organisations, we have UNSTRUCTURED CHAOS, even if we could have it all, where would we even start in order to identify risk? we have gifs, emojis, screenshots, abbreviations and slang. And somewhere in there is our risk, somewhere in there are passwords being shared in plain text, somewhere in there is sensitive customer data leaving your organization. This is why Mimecast has the capability to look into all of these platforms and realise the sentiment, the context and therefore quantify high risk users. Then you can begin to put mitigation and user education initiatives in place targeting the high risk users.

8%

OF USERS

CAUSE

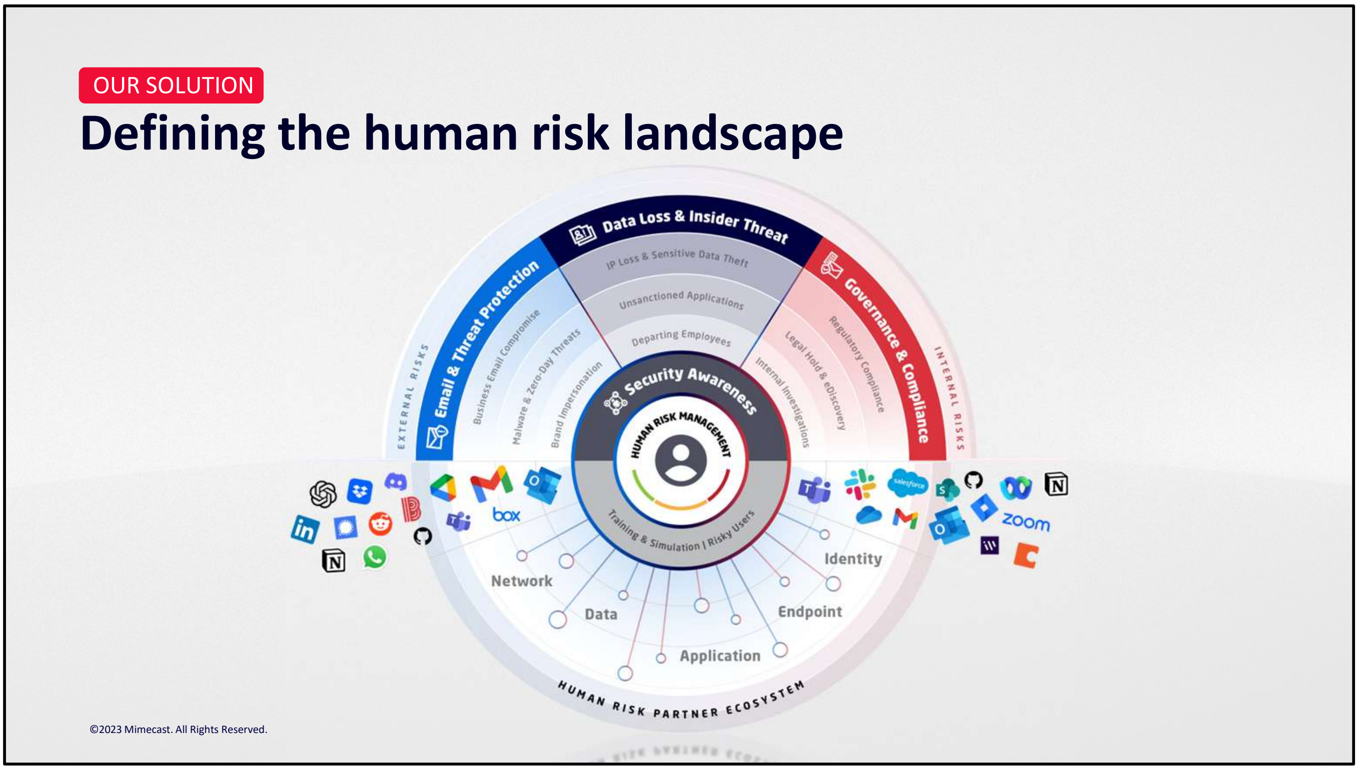
80%

OF SECURITY INCIDENTS

Size and Shape of Workforce Risk, Cyentia Institute 2023.

- In fact, what we saw was that **8%** of users cause **80%** of security incidents.
- So **one-size fits all** approaches **aren't** going to be effective.

Transition: Which is why we can start **thinking** about this problem in a **new way**.

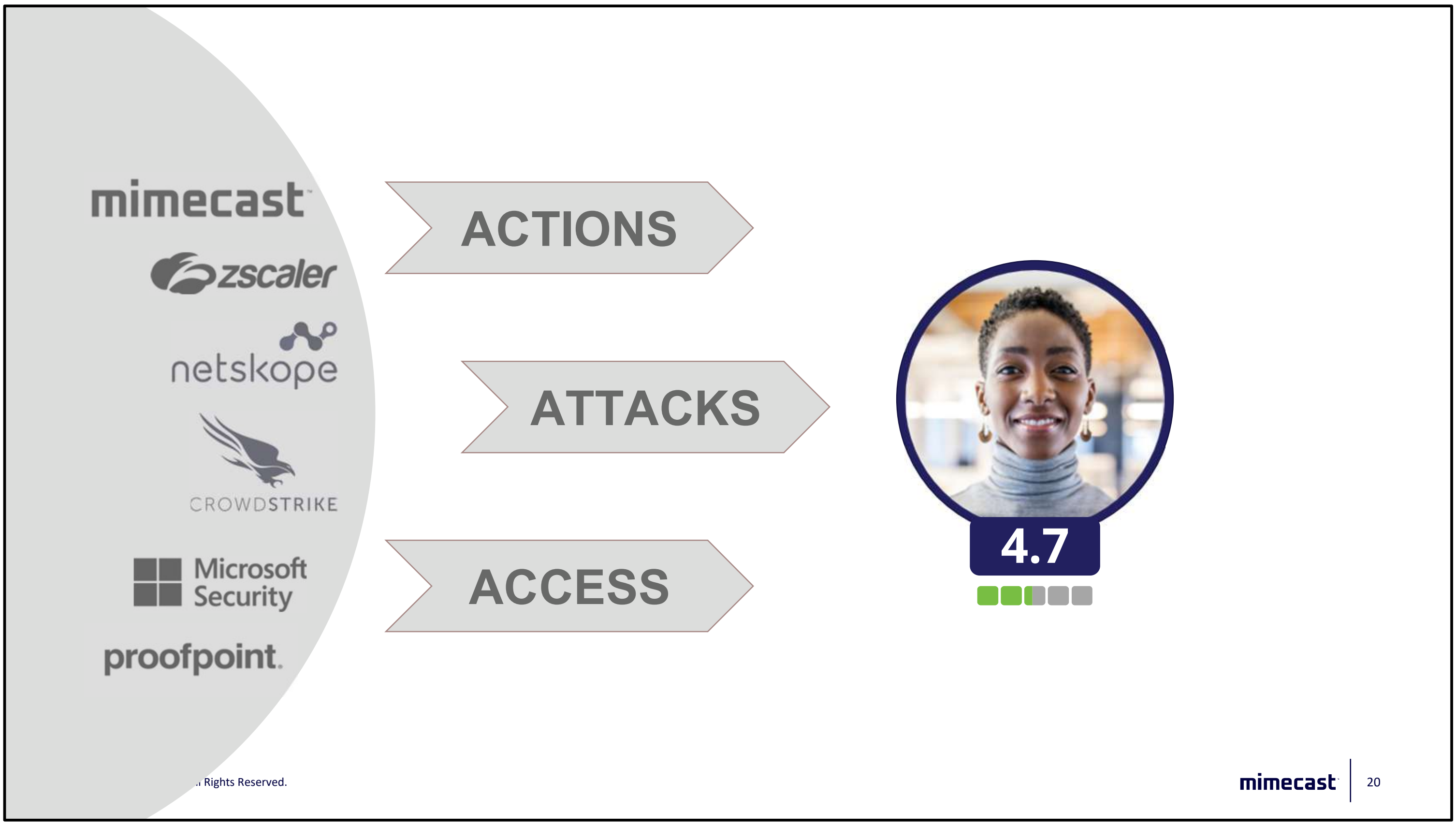


OUR SOLUTION

Defining the human risk landscape

The reality is, we don’t know what we don’t know. We cant manage and mitigate the risks, if we don’t know them in the first place? Do you wait for a breach to happen or do you spot a pattern earlier and mitigate the risk then, do you wait for you to find out that actually that employee that’s watched all the training videos and answered all the questions, gives up his credentials to an impersonated email or message? No, we want to blend the simulated risk with the actual risk data, we want to reach into all of the collaboration tools we use and scan the URLs, sandbox the attachments in your OneDrive

We’ve made it our mission to secure human risk, by putting the human beings at the center of everything we do



ACTIONS

ATTACKS

ACCESS

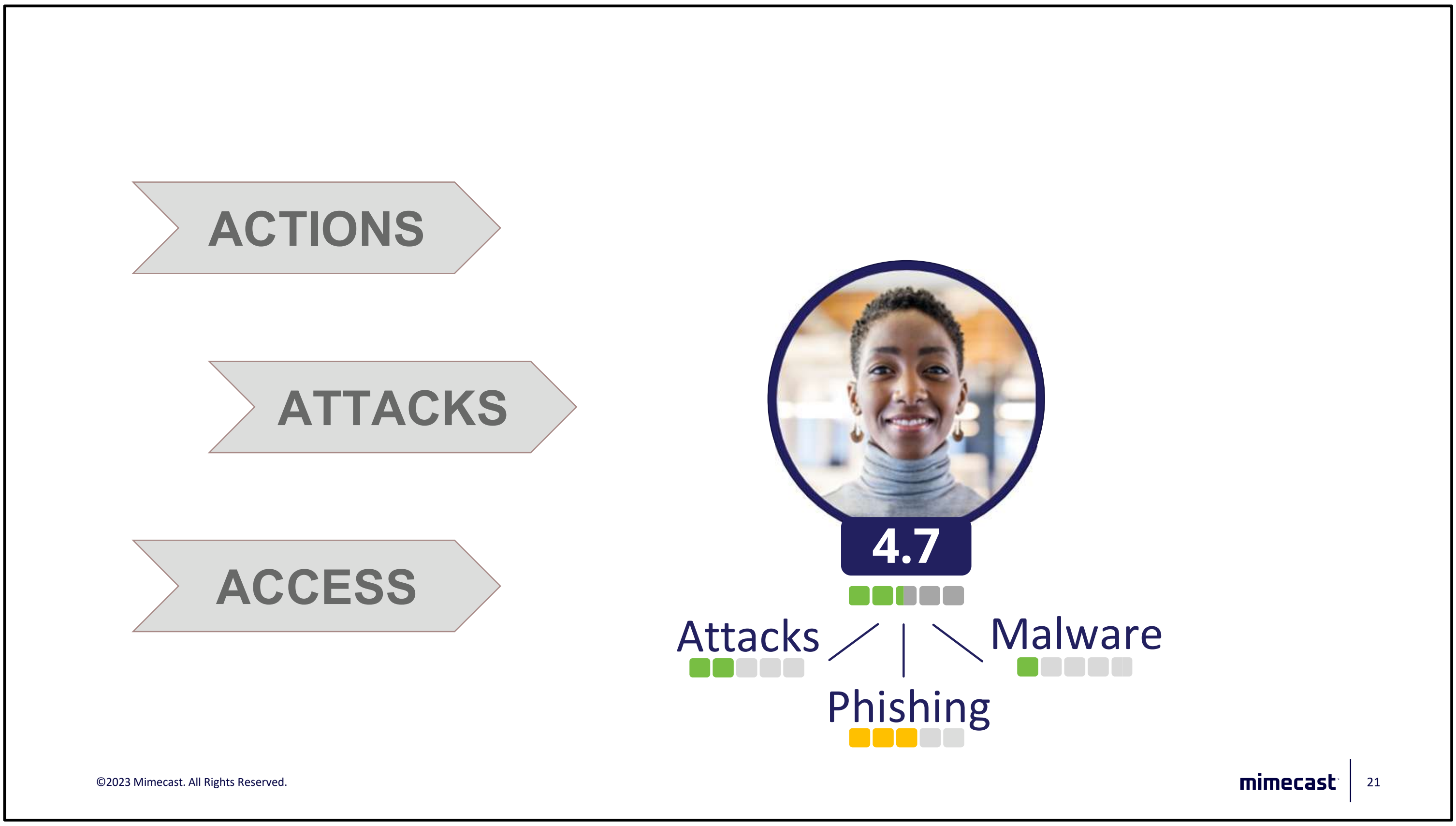
4.7

Part 1 animation:

•We **measure** the risk of an individual based on 3 factors: **their** security **decisions** (good and bad), how **frequently** they are being **attacks**, and context about their **role** and **access**.

•The risk **profile** takes into context security actions like does Jean **click on links**, browse to **blocked sites**, attempt **malware downloads**, or **mishandle sensitive data**, just to name a few.

•We gain an understanding of factors by **integrating** with security tools you **already** have in place today.



ACTIONS

ATTACKS

ACCESS

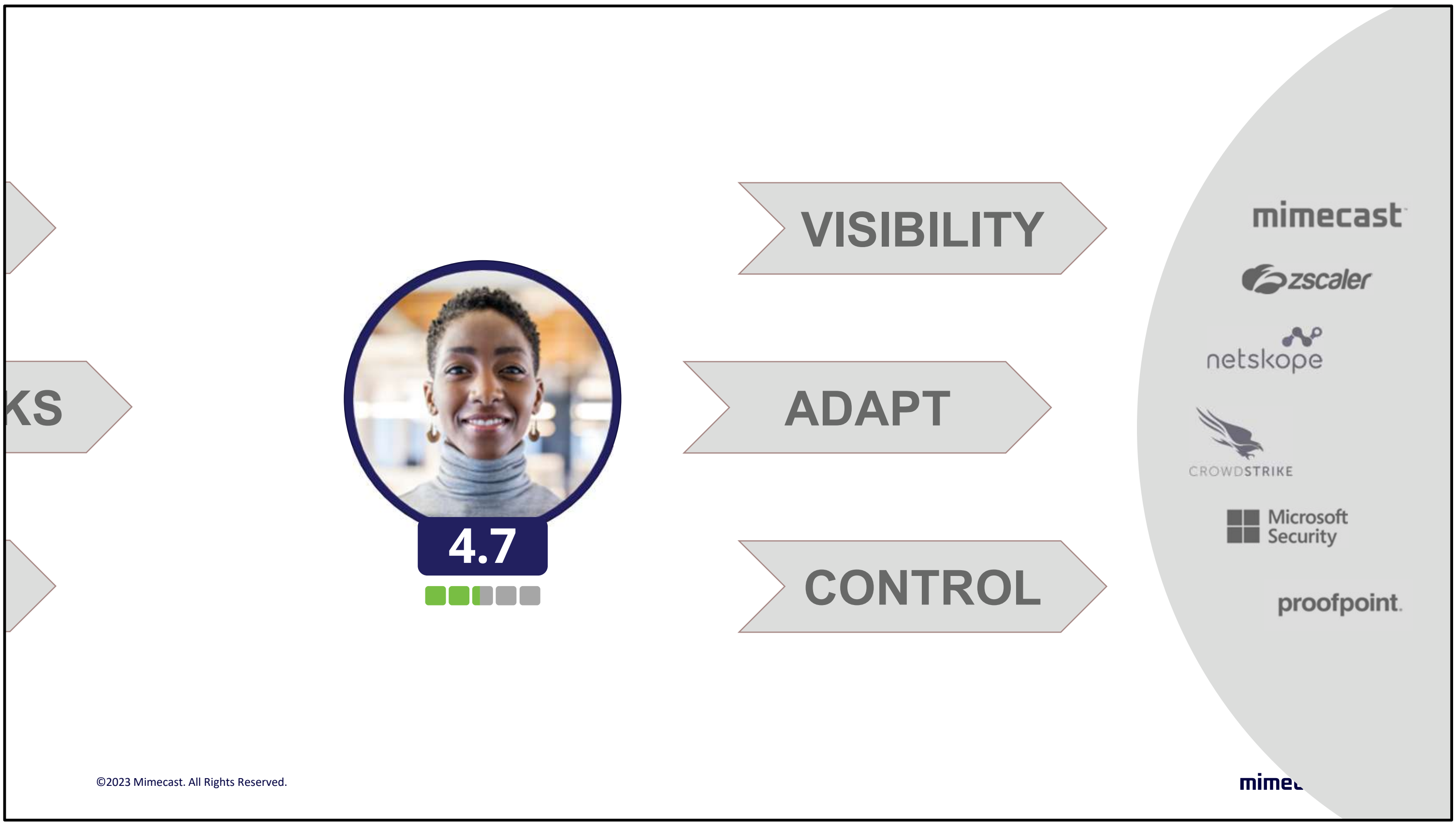
4.7

Attacks

Malware

Phishing

- We pull this information back, **correlated** with your **HR data** to give you insights into **individual risk**.
- This will let you **understand** your **human risk** like never before. You are able to gain insights like riskiest **departments**, **geographies**, and **individuals**. You'll understand your **repeat** offenders and who your security **champions** are in a single dashboard.



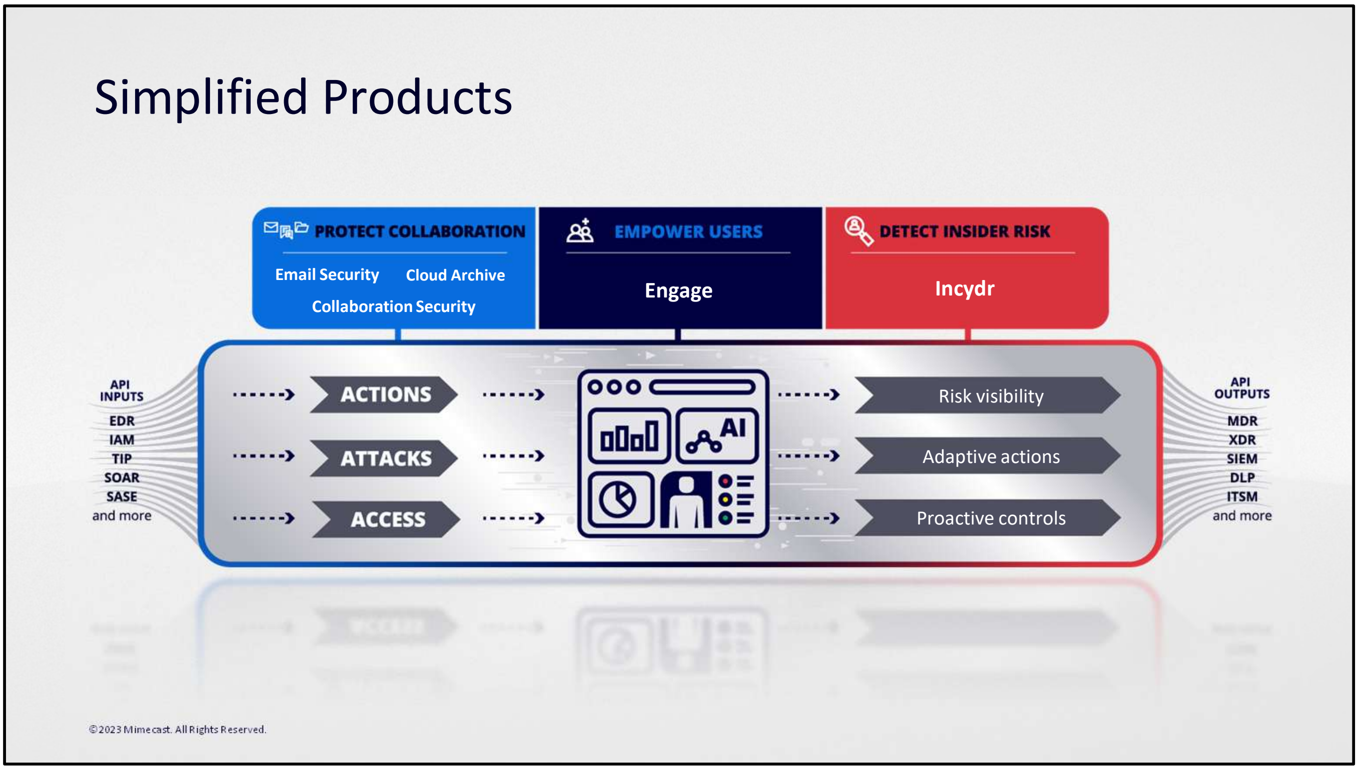
VISIBILITY

ADAPT

CONTROL

- •But we dont just equip you with the **visibility**. The platform also lets you **take action** on the findings through pre-built **playbooks** and automated **workflows**.
- •an example of these workflows include the ability to **assign training**, send personalized **scorecard** to individuals and managers, and provide real time **nudges** via slack/teams.

- •We are also **incorporating** this risk insight into our secure email **gateway** solutions, giving you recommended **policies** based on user risk.
- •We also understand that you and your team make security decisions in a variety of **other technologies**, so this user risk data can be pushed to other partner technologies, helping making more **context rich decisions** in workflows the **access reviews**, **incident response**, and others.



Simplified Products

PROTECT COLLABORATION

Email Security

Cloud Archive

Collaboration Security

EMPOWER USERS

Engage

DETECT INSIDER RISK

Incydr

API INPUTS

EDR

IAM

TIP

SOAR

SASE

and more

ACTIONS

ATTACKS

ACCESS

Risk visibility

Adaptive actions

Proactive controls

API OUTPUTS

MDR

XDR

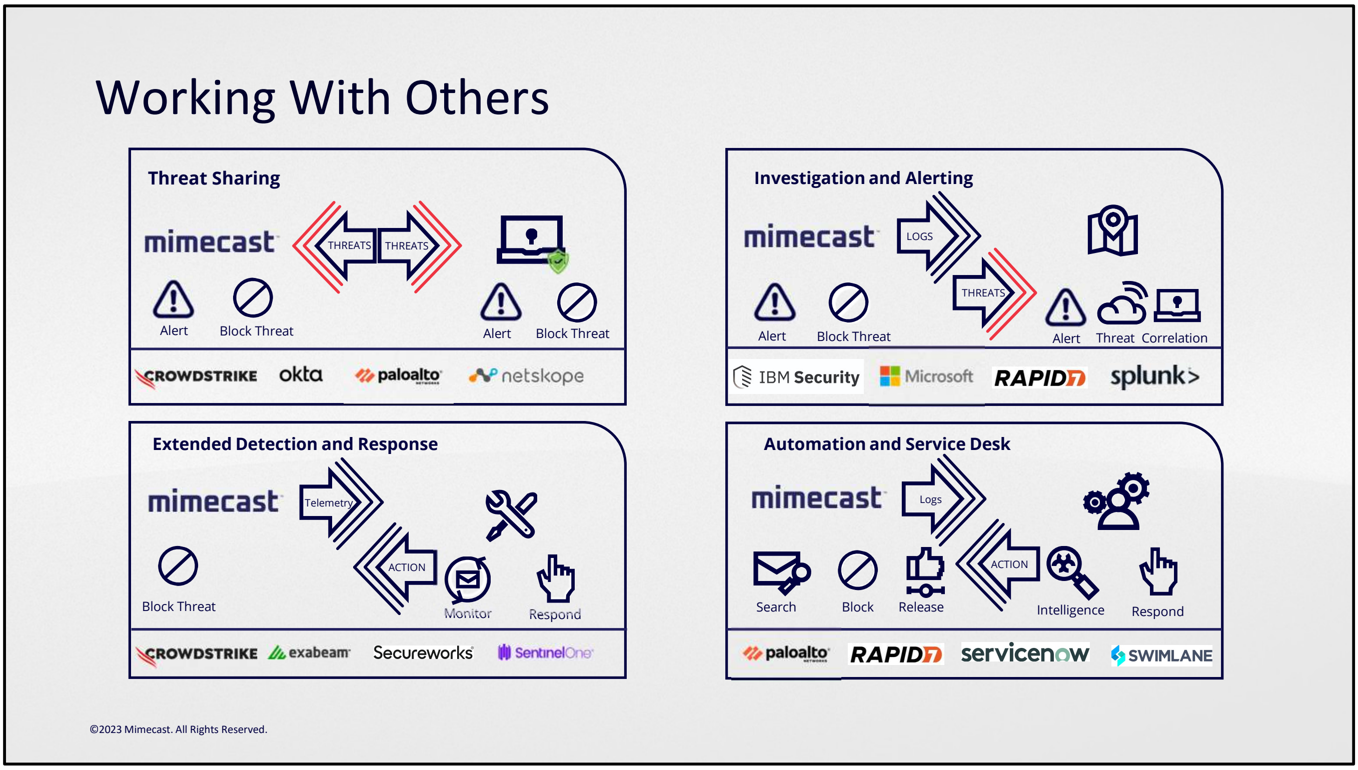
SIEM

DLP

ITSM

and more

We need to take everything into account to build a pattern for your organization and then work with AI/AL to really hone in on the anomalies. Every org is different, every user is different, so why should each user be treated the same when it comes to risk? We provide the ability to expose the risks, and mitigate the risks through personalized training, dynamically changing protection in line with user risk profiles and proactive controls to make sure we spot breaches before they happen.



Working With Others

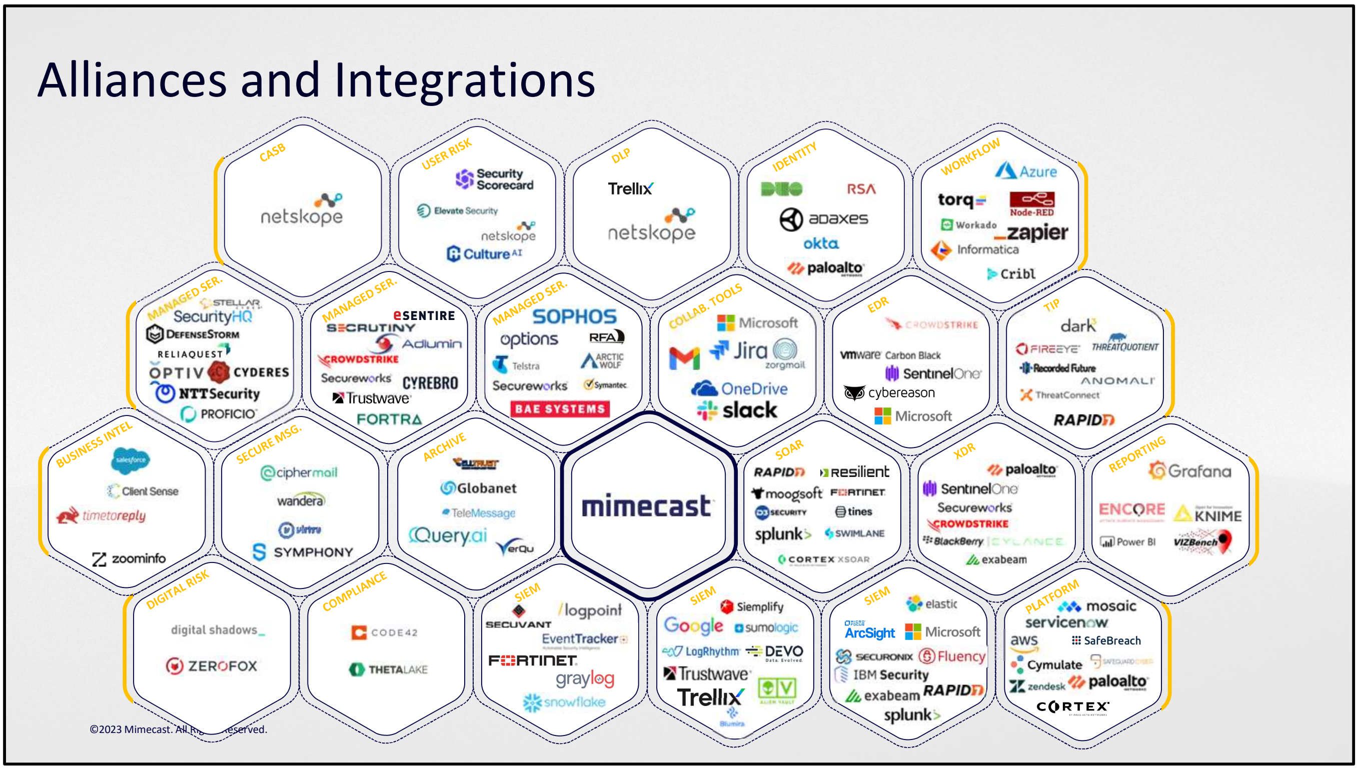
Threat Sharing

Investigation and Alerting

Extended Detection and Response

Automation and Service Desk

We spoke about external risks, BEC attacks, insider threats, and of course the user education but one thing that takes it to the next level, you guessed it, even more data! wE HAVE A TREASURE TROVE OF RISK DATA BUT SO DO OTHER TOOLS. Sharing our data with other tools you have and vice versa compounds the value you get from multiple tools you are using.



Alliances and Integrations

We have over 100 prebuilt integrations ready to go in 5 minutes. This is where we take the human risk to the next level. The measuring of simulated vs actual risk, the incorporation of data from your HR platforms, your endpoint solutions giving us a rich details of what users are doing outside email and collaboration tools and the ability to mitigate the now exposed risk through well defined workflows means exposing, preventing and containing threats is now so much easier and can be done all under one roof and that's why Mimecast is a leader.. NEXT SLIDE.. in the Human risk management space.

mimecast®

The Connected Human Risk Management Platform

Thank you everyone for being a great audience, any questions please feel free to reach out to be as myself and my team Alex and Catherine will be here after the sessions today.