Cisco Small Business IT Webinars

cisco.com/go/smb

Fishing for Phishers

AGENDA

1. Introduction
2. Solution Overview – *Cloud Email Security, AMP, Umbrella, Duo & TALOS*
3. Case Studies
4. Demo – *Email Security, Umbrella, AMP Integration*
5. Q&A
6. Conclusion

Solution Overview:

Cloud Email Security, AMP, Umbrella, Duo & TALOS

Our Speaker...

Wesley Wong
Cybersecurity Specialist

Why fight phishing?

Email is the #1 attack vector.

[Account-Deactivation]

MF

Microsoft Fix <mx-59545445435@protection.office-365.com>

Tuesday, August 21, 2018 at 1:18 AM

Show Details

Office-365

Hi **Sales**

Your account of **com** will be disconnected from sending or receiving mails from other users. because you failed to resolve errors on your mail.

You need to resolve the errors or your account will be disconnected from **com**.
Follow the instruction below to resolve now.

RESOLVE ISSUE NOW

Regards,
Microsft Security Team

This notification was sent to .com of Microsoft.com.

USPS <shipping@usps-service.com>

Shipping information for parcel 031760612

Retention Policy Junk Email (30 days) Expires Never

Our courrier was not able to deliver your parcel because nobody was present at your address.

Someone must always be present on the delivery day, to sign for receiving the parcel.

Shipping type: USPS Next Day
Box size: Large Box (2-5kg)
Date : Feb 6th 2017

You can reschedule the delivery over the phone, but you will have to confirm the information on the delivery invoice.
Another delivery can be arranged, by calling the number on the delivery invoice we left at your address and confirming the shipping information, including the address and tracking number.

A scanned copy of the delivery invoice can also be downloaded by visiting the USPS website:
https://tools.usps.com/web/pages/view.invoice?id=031760612&a mp;dest=

In the exceptional case that a new delivery is not rescheduled in 24 hours, the shipment will be cancelled and the package will be returned to the sender.

Thanks for shipping with USPS

HJ

Henry Jonnes <henry.jones@hr-communication.com>

Wesley Wong (weswong)

Wednesday, July 17, 2019 at 11:14 AM

Show Details

Hello,

You are receiving this message because you have unnused PTO hours that are set to expire at the end of the pay period.
According to new policies, we are unable to transfer these hours. More information about the new PTO policcy is available here.

Please review your balance in the Employee Portal and reach out to me directly with questions.

Thank you,
Henri Jones
Human Resources Coordinator

Save Yourself <SaveYourself47@1883.com>
To: [redacted]

Jul 8 at 3:30 AM

Hi, I know one of your passwords is: [redacted] - but not only that!

Your computer was infected with my private malware, because your browser wasn't updated / patched, in such case it's enough to just visit some website where my iframe is placed to get automatically infected, if you want to find out more - Google: "Drive-by exploit".

My malware gave me full access to all your accounts (see password above), full control over your computer and it also was possible to spy on you over your webcam!

I collected all your private data and I RECORDED YOU (through your webcam) SATISFYING YOURSELF!

After that I removed my malware to not leave any traces and this email was sent from some hacked server.

I can publish the video of you and all your private data on the whole web, social networks, over email of all your contacts and everywhere else.

But you can stop me and only I can help you out in this situation.

The only way to stop me, is to pay exactly 900$ in bitcoin (BTC).

It's a very good offer, compared to all that HORRIBLE SHIT that will happen if you don't pay!

You can easily buy bitcoin here: www.paxful.com , www.coinbase.com , or check for bitcoin ATM near you, or Google for other exchanger.
You can send the bitcoin directly to my wallet, or create your own wallet first here: www.login.blockchain.com/en/#/signup/ , then receive and send to mine.

My bitcoin wallet is: 1GLJa8dMq9XBaiMhXNJSQjVoNzh2xRanzD

Copy and paste my wallet, it's (cAsE-sEnSEtiVE)

I give you 3 days time to pay.

As I got access to this email account, I will know if this email has already been read.
If you get this email multiple times, it's to make sure that you read it, my mailer script is configured like this and after payment you can ignore it.
After receiving the payment, I remove all your data and you can life your live in peace like before.

Next time update your browser before browsing the web!

Myth: *We're too small.*

Reality: Being small could make you a more attractive target.

Myth: *We train our employees.*

Reality: Humans make mistakes.

Myth: *We have a Firewall.*

Reality: Threats will get past your firewall.

Defense in Depth

Layering a Phishing Solution

1. Stop phishing emails from reaching your user's inbox.
2. Determine the safety of email attachments.
3. Block users from reaching malicious websites.
4. Use multi-factor authentication.
5. Leverage a threat intelligence you can trust.

Cloud Email Security (CES)

Stop phishing emails from reaching your user's inbox.

AMP

Determine the safety of email attachments.

Table 1 Malicious attachment types.

Type	Percentage
Office	42.8%
Archive	31.2%
Script	14.1%
PDF	9.9%
Binary	1.77%
Java	0.22%
Flash	0.0003%

Source: Talos Intelligence

Table 2 Top 10 malicious extensions in email.

Extension	Percentage
.doc	41.8%
.zip	26.3%
.js	14.0%
.pdf	9.9%
.rar	3.9%
.exe	1.7%
.docx	0.8%
.ace	0.5%
.gz	0.5%
.xlsx	0.2%

Source: Talos Intelligence

Umbrella

Block users from reaching malicious websites.

Duo

Use multi-factor authentication.

What is MFA?

Combining something only you should know with something only you should have.

Why Cisco?

Supreme threat intelligence and seamless security integration

TALOS

Leverage a threat intelligence you can trust.

Our Threat Intelligence Advantage

See More

Block more

Respond Faster

Talos Intel Background

THREAT INTEL

INTEL SHARING

300+
Full Time Threat Intel Researchers

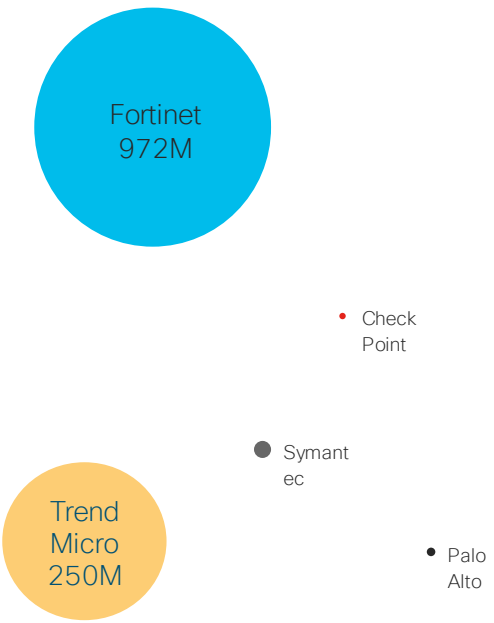
MILLIONS
Of Telemetry Agents

4
Global Data Centers

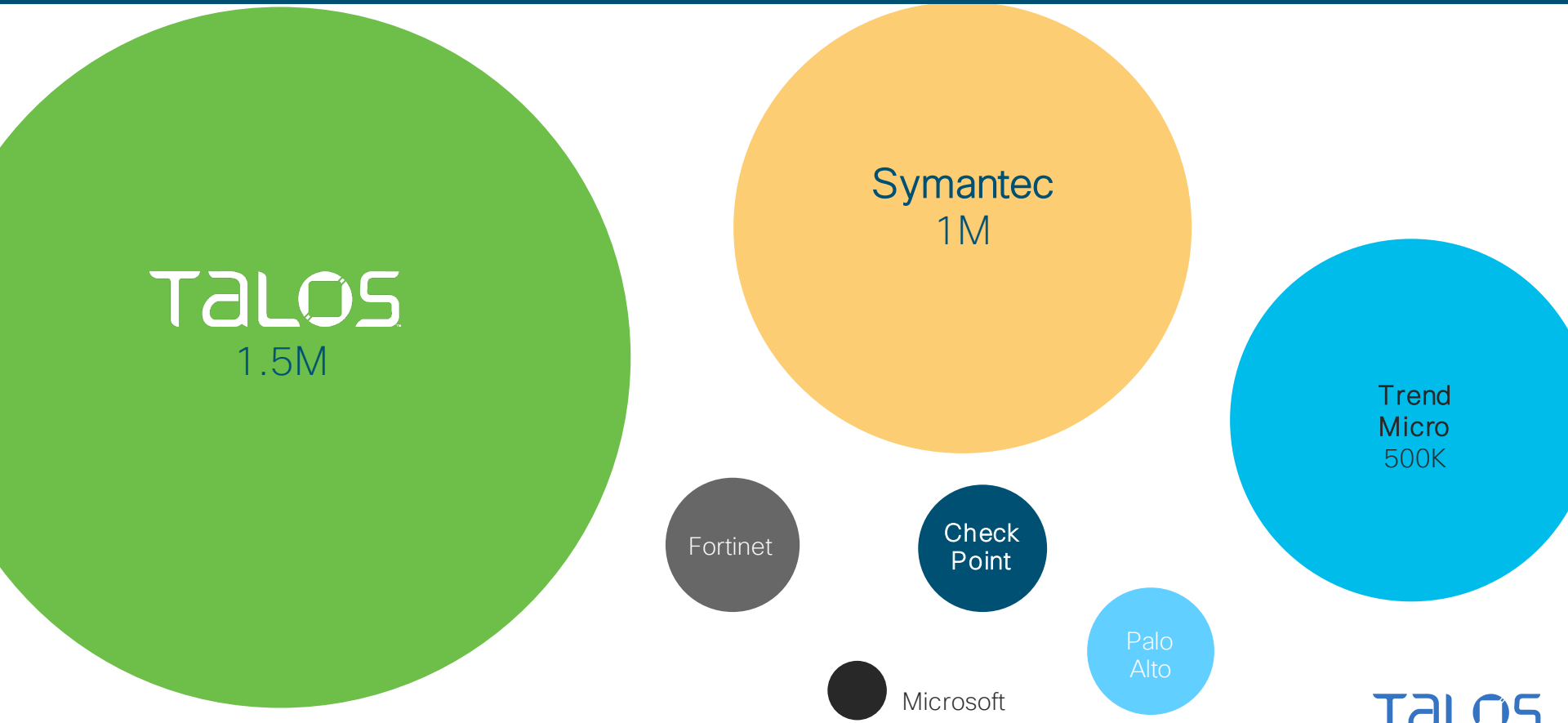
100+
Threat Intelligence Partners

1100+
Threat Traps

Threats Blocked (Daily)



Unique Malware Samples (Daily)



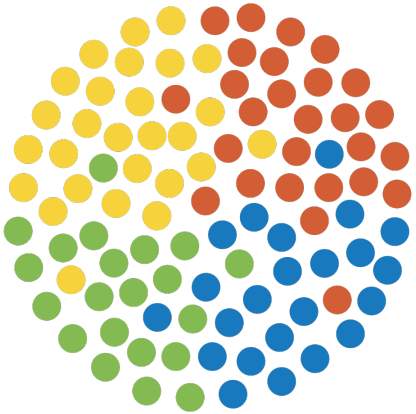
Seamless integration

Engineering solutions that work together and talk to each other

"By adopting a set of security platforms and tools that all work together versus disparate pieces that may actually conflict with each other, you get an amplification of security effectiveness, as well as simplification of management."

Ben M. Johnson
CEO of Liberty Technologies

Case Studies



Indra

"A certain individual who is interested in carrying out a targeted attack will look into employees' personal information. Email addresses are easy to retrieve and use, and offer a direct door to sensitive data and the possibility of moving within our network from there."

Juan Gámez Torres, Senior Security Consultant

Indra's CES with AMP Implementation

Challenges

- Protect tens of thousands of endpoints from malicious emails
- Prone to advanced, targeted attacks via email

Results

- Forty percent of incoming emails blocked due to suspicious characteristics
- Ability to tightly control outbound messages
- Expanded security visibility and awareness

"Cisco Email Security helps us separate what is good from what is bad, what is spam from what is legitimate, and so on. The number of suspicious emails that make it to our mailboxes is very low."

Juan Gámez Torres, Senior Security Consultant

centrexIT

“We knew that antivirus and firewalls weren’t enough to protect our clients.”

Eric Rockwell, CIO

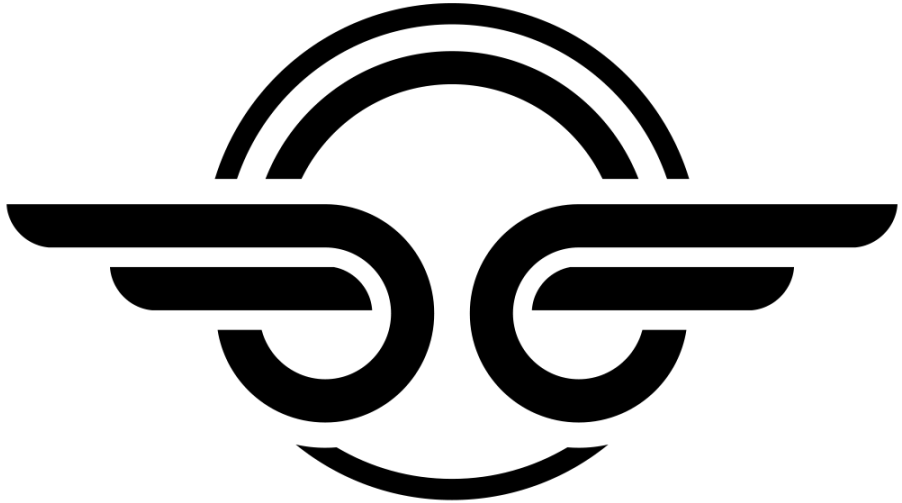
CentrexIT's Umbrella Integration

Challenge

- Provide strong security in industries that are subject to rigorous regulatory scrutiny.

Impact

- 70% fewer malware related tickets
- Avoided tens of thousands of dollars in ransom costs
- Saved thousands of hours of cleaning and troubleshooting
- Created auditable security trails for compliance



BIRD

Bird's Duo Integration

Challenge

- Protect sensitive information, such as customer data, intellectual property, business plans and more

Result

- Mitigated the risk of compromised passwords and phishing attacks in the organization

Demo – *Umbrella*

Q&A

Before we go...

Click the link in the chat for a free trial of Cisco Umbrella!

We Appreciate Your Feedback!

Please take a moment to let us know if this session met your needs and expectations.

The confidential evaluation survey will open once the event window is closed.


CISCO