WatchGuard

RAISE THE BAR 2020

Navigating the 2020 Cyber Threat Landscape

Corey Nachreiner, CTO WatchGuard

Meet the Presenter

Corey Nachreiner

Chief Technology Officer (CTO)

WatchGuard Technologies, Inc.

- Young hacker *(Modems, phreaking, 2600, BBS, etc)*
- CompSci @ WWU
- Ex-Network & Malware Analyst / Pen-tester
- Ex-Dir. of Security Strategy & Research
- Tech geek (3D printing, VR, drones & robotics)

Agenda

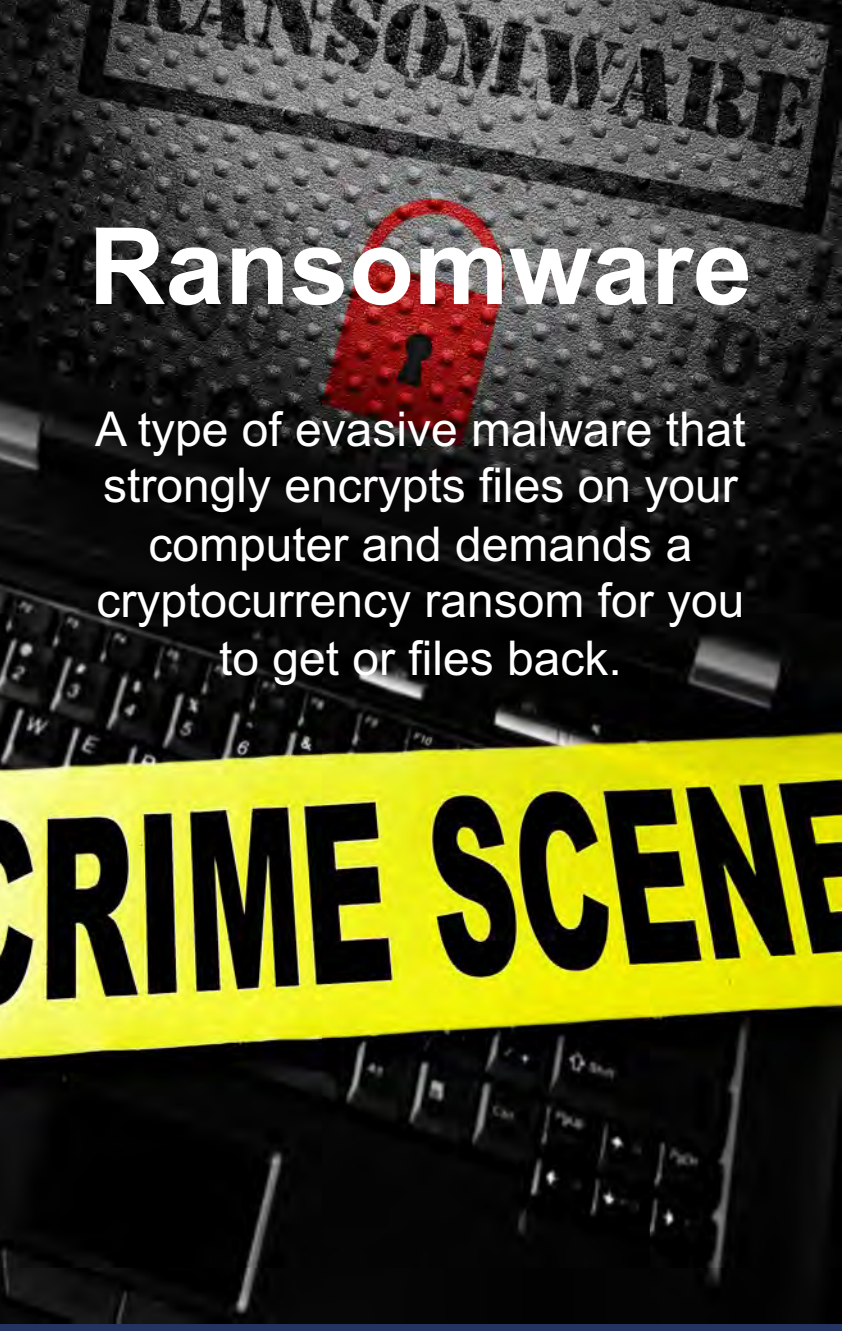
Five 2020 security threats & trends that affect everyone

Six work from home security tips for a pandemic

Summary:

Network and endpoint security for the win

Five Security Trends Affecting Us All



Ransomware

A type of evasive malware that strongly encrypts files on your computer and demands a cryptocurrency ransom for you to get or files back.

Quick History

- Spammed, shotgun ransomware
  - Cryptolocker, Cryptowall
- Vertical, targeted ransomware
  - WannaCry
- MSP Ransomware
  - Sodinokibi

Latest Evolutions

- Latest antimalware evasions
- Ransomware as a Service (RaaS)
- Target backups (NAS)
- Kills hundreds of security processes

Targets, Tactics, and Trends

- Healthcare
- Local and state government
- Industrial Control and Manufacturing
- MSPs, CSPs, and SPs
- … What's next?

RAISE THE BAR 2020

2020 Prediction - Ransomware Targets the Cloud

Ransomware Defenses

- Advanced Network Malware Detection *(APT & IAV)*
- Good Firebox Policy
- AuthPoint
- Threat Detection and Response
- DNSWatch

Spear Phishing

A very well designed and targeted email masquerading as legitimate correspondence. It tries to socially engineer you into doing something you shouldn't.

Quick History

- Phishing around since the 90s
- Notable *spear* phishing started 2010
- RSA's hack started w/spear phishing *(2011)*
- Anthem breach was a spear phish *(2015)*
- DNC Hack *(2016),* etc...

Latest Evolutions

- Automated social network recon
- Org partner mapping
- Brand impersonation
- Whaling & targeted smishing/vishing

Targets, Tactics, and Trends

- 90-95% of breaches start with spear phish
- 94% of spear phish use files not links
- Leading cause of account takeover
- 28% of phishing is targeted
- 30% open spear phish; ~14% click
- Lowest volume, but highest impact cost

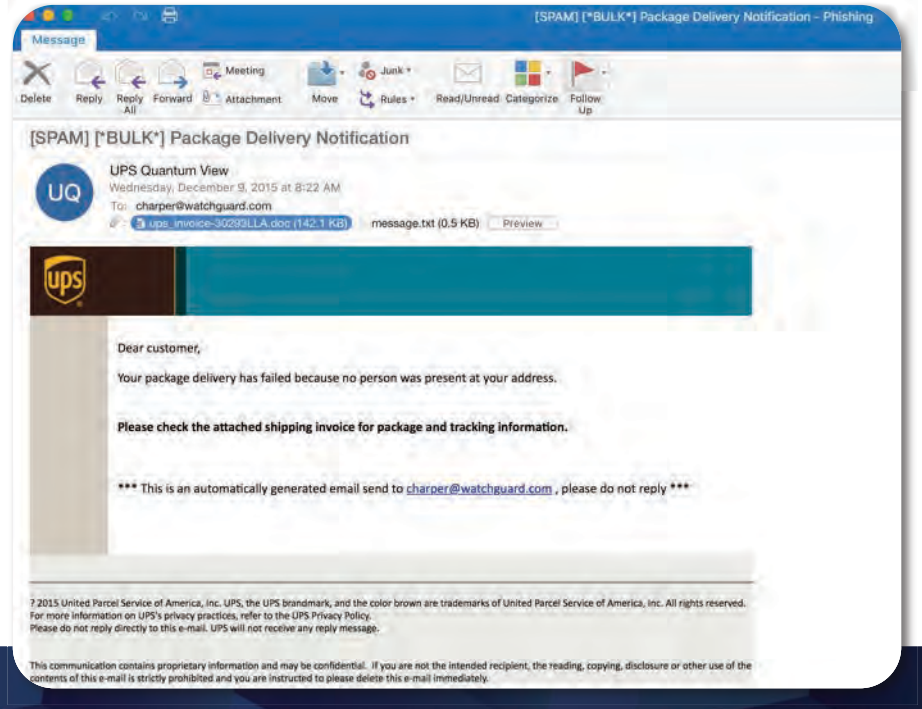
RAISE THE BAR 2020

Flavors of Phishing

Phishing – luring a victim into giving up credentials or doing something via a legitimate seeming email

Spear-phishing – A more customized phishing email that targets a specific individual or group

Whaling – spear-phishing that targets C-levels



Old phishing example:

- Not individualized
- Bulk recipients
- Uses real assets
- Malicious document

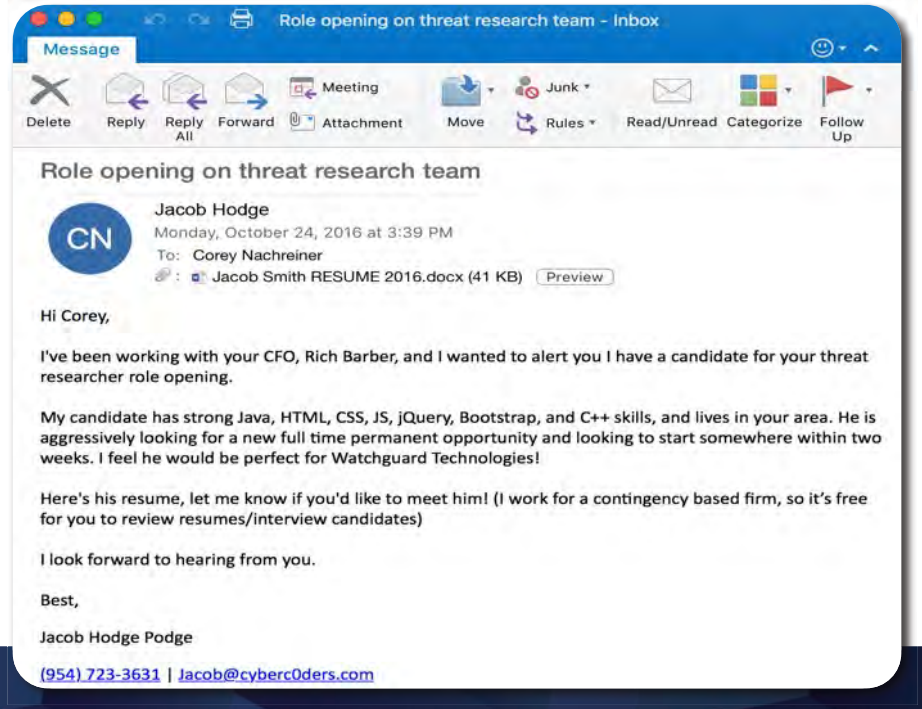
RAISE THE BAR 2020

Flavors of Phishing

Phishing – luring a victim into giving up credentials or doing something via a legitimate seeming email

Spear-phishing – A more customized phishing email that targets a specific individual or group

Whaling – spear-phishing that targets C-levels



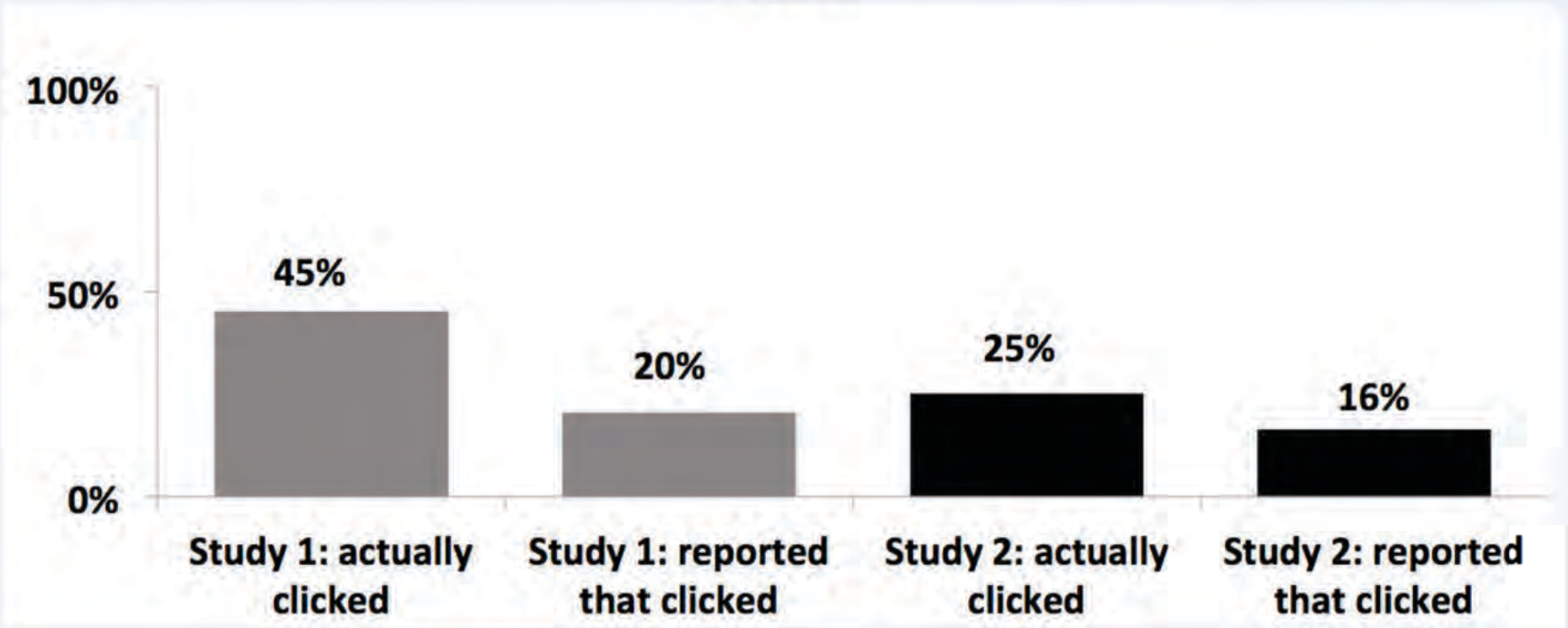
Spear-phishing example:

- Personalized to me
- Fits my job role
- Understands business relationships
- Sender makes sense in context
- Malicious attachment fits context

RAISE THE BAR 2020

Users Still Click Phishing Emails

78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway.



Friedrich-Alexander University (FAU)

Users Still Click Phishing Emails

78% c … . And yet they click

From: john.smith@turner.com
To: zinaida.benenson@fau.de
Subject: CNN request -- about your upcoming Black Hat talk

Zinaida,

John at CNN here. I'm the news network's cybersecurity reporter. Here's a link to my work, in case you're not familiar with it.

I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!

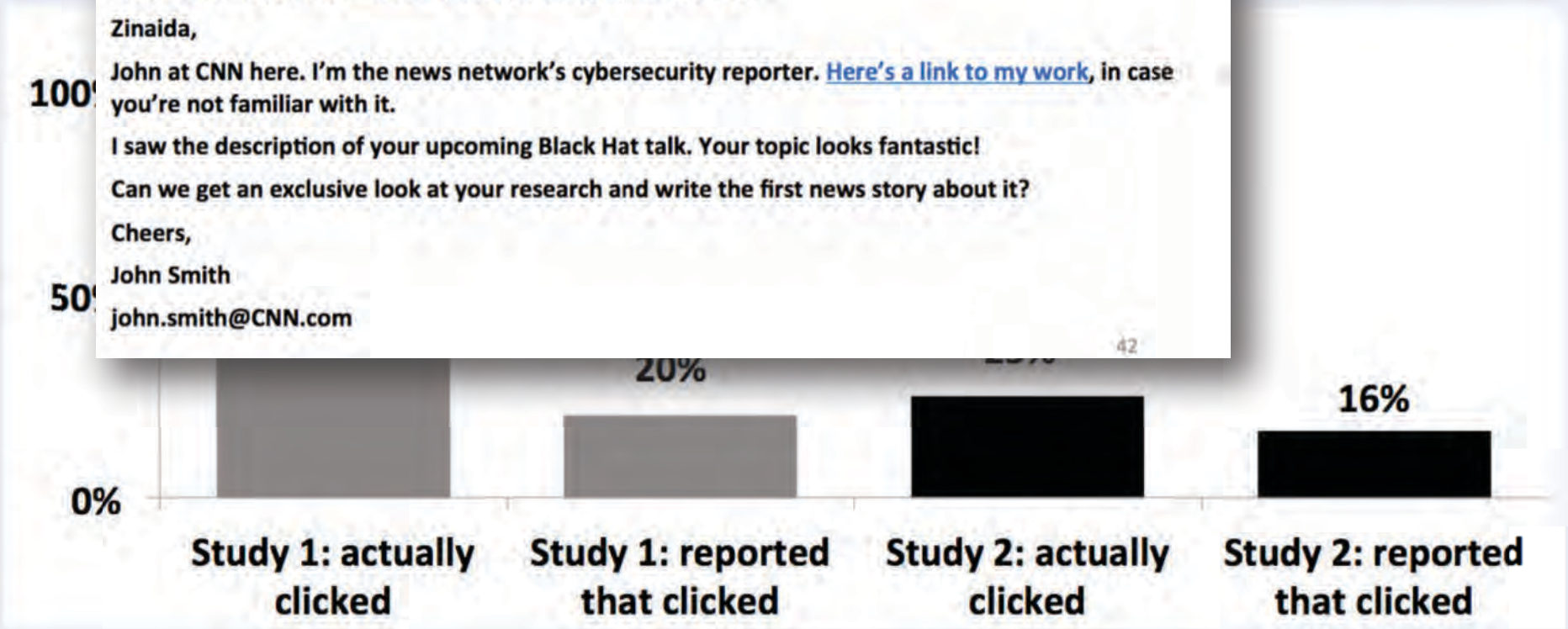
Can we get an exclusive look at your research and write the first news story about it?

Cheers,

John Smith

john.smith@CNN.com

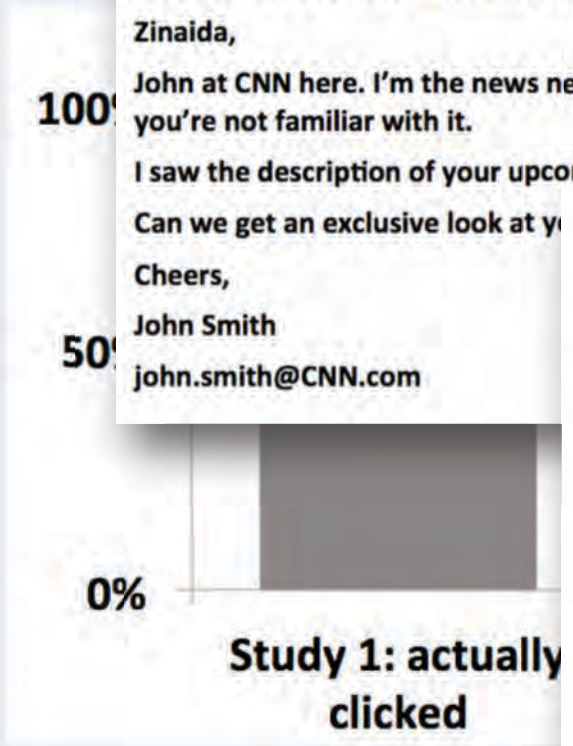
42



Friedrich-Alexander University (FAU)

Users Still Click Phishing Emails

78% c … . And yet they click



From: john.smith@turner.com
To: zinaida.benenson@fau.de
Subject: CNN request -- about your upcoming Black Hat talk

Zinaida,

John at CNN here. I'm the news network's cybersecurity reporter. Here's a link to my work, in case you're not familiar with it.

I saw the description of your upcoming Black Hat talk. Your topic looks fantastic!

Can we get an exclusive look at y

Cheers,

John Smith

john.smith@CNN.com

From: Journal of Experiments (EXPE) exp@editorial-expe.com
To: zinaida.benenson@fau.de
Subject: Invitation to Peer Review EXPE-M-35-00737

Dear Dr. Benenson, In view of your expertise […]

[…]

If you would like to review this paper, please click this link:
http://expe.editorial-expe.com/l.asp?i=35189&l=GKXKMQK

If you do not wish to review this paper, please click this link:
http://expe.editorial-expe.com/l.asp?i=87665&l=6HN7KK

Best regards,

Editor

<name I've never heard of>

Covid-19 Related Phishing

Watch out for:

- Fake CDC info
- Unemployement scams
- Fake video conference links (Zoom)
- Fake stimulus emails

From: CDC <envhealthmedia@cdchealth.org>
Sent on: Tuesday, March 3, 2020 7:22:13 PM
To: [redacted]
Subject: COVID19: Community spread now up by 70% [EXTERNAL]

Warning: Level 3, Community Spread!
Alert - Level 2, Practice Enhanced Precautions

The Centers for Disease Control and Prevention (CDC) and public health officials have reported a total of 60 confirmed cases who have tested positive for the virus that causes COVID-19, including six patient who have died.

For full Transcript of the CDC Telebriefing Update on COVID-19 and cases that might be around your community, see below;

CDC Newsroom Releases

CDC works 24/7 protecting America's health, safety and security. Whether disease start at home or abroad, are curable or preventable, chronic or acute, or from human activity or deliberate attack, CDC responds to America's most pressing health threats. CDC is headquartered in Atlanta and has experts located throughout the United States and the world.

Spear Phishing Defenses

- DNSWatch
- WebBlocker
- Advanced Malware Detection
- AuthPoint

Fileless Malware

A sophisticated and evasive type of malware that avoids writing files to your computer storage, making it harder for endpoint solutions to detect.

Quick History

- Memory resident viruses of the 80s
- Fileless network worms of the 00s
  - *CodeRed, SQL Slammer*
- "**Living off the Land**" attacks today
  - Powersploit, Powerware

Latest Evolutions

- DLL and memory injection
- Use of legitimate Windows tools
  - PowerShell, Netsh, etc
- Attached to zero day exploits

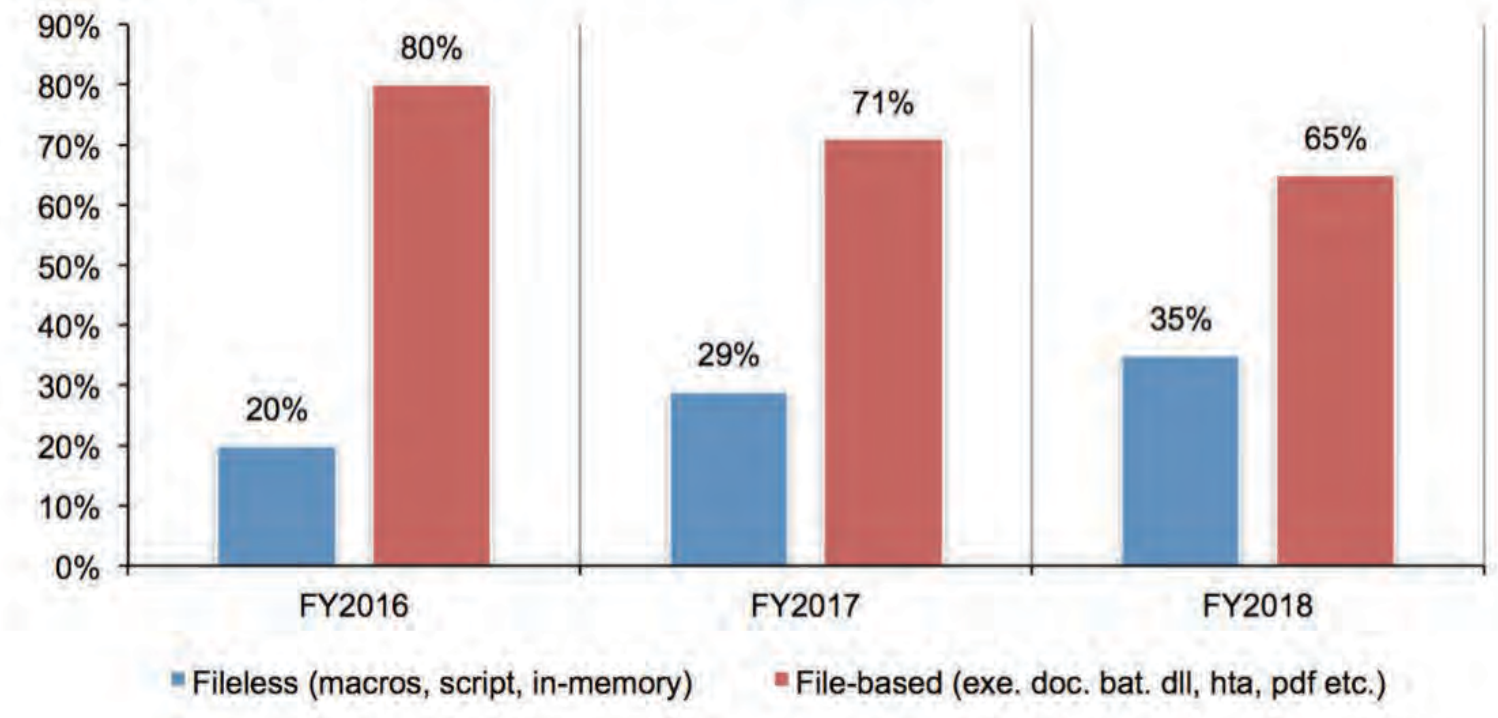
Targets, Tactics, and Trends

- Really picked up around 2016
- Not always completely fileless
- Often starts with Office documents
- PowerShell threats increased 460% in 2019

RAISE THE BAR 2020

Fileless Malware Growing

Figure 2. The growth of fileless and file-based attacks



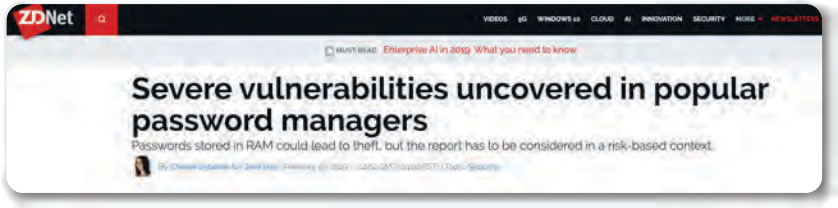
- 77% of attacks that successfully compromised organizations in 2017 utilized fileless techniques - *Ponemon Institute*
- Fileless malware attacks accounted for 52% of all attacks in 2017 - *Carbon Black*

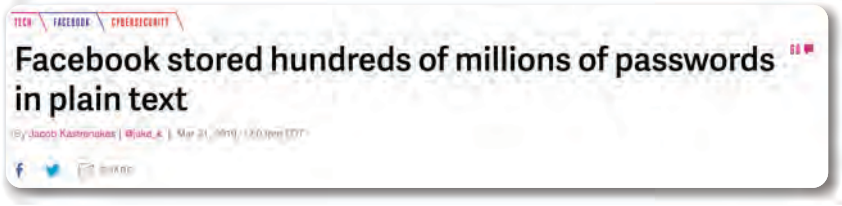
** Ponemon Institute's "The 2017 State of Endpoint Security Risk Report"*

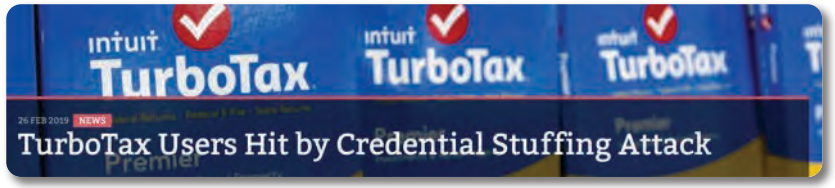
Fileless Malware Defenses

- Intrusion Prevention System
- Advanced Malware Detection
- Threat Detection and Response

Huge Target on Authentication







Account Takeover

An attack where the invader successfully logs into an org impersonating a trusted employee. Often involves lost or stolen credentials.

Quick History

- 2002: First mandatory breach disclosure law
- 2004: Gates, ”passwords are dead”
- 2011: Sony PSN lost 77m passwords
- 2013: Google exec, “passwords are dead”
- 2013 Yahoo lost 1b passwords
- 2019: Collection 1-5 leak, 2.2b passwords

Latest Evolutions

- Password Spraying (common passwords)
- Credential Stuffing (leaked passwords)
- Mimikatz & WCE
- SMS 2FA bypass
- SIM swapping

Targets, Tactics, and Trends

- Reddit (2FA bypass)
- Cred Stuffing:
  - Citrix
  - HSBC
  - State Farm
  - Retail vertical
- Passwords still top factor in 2020

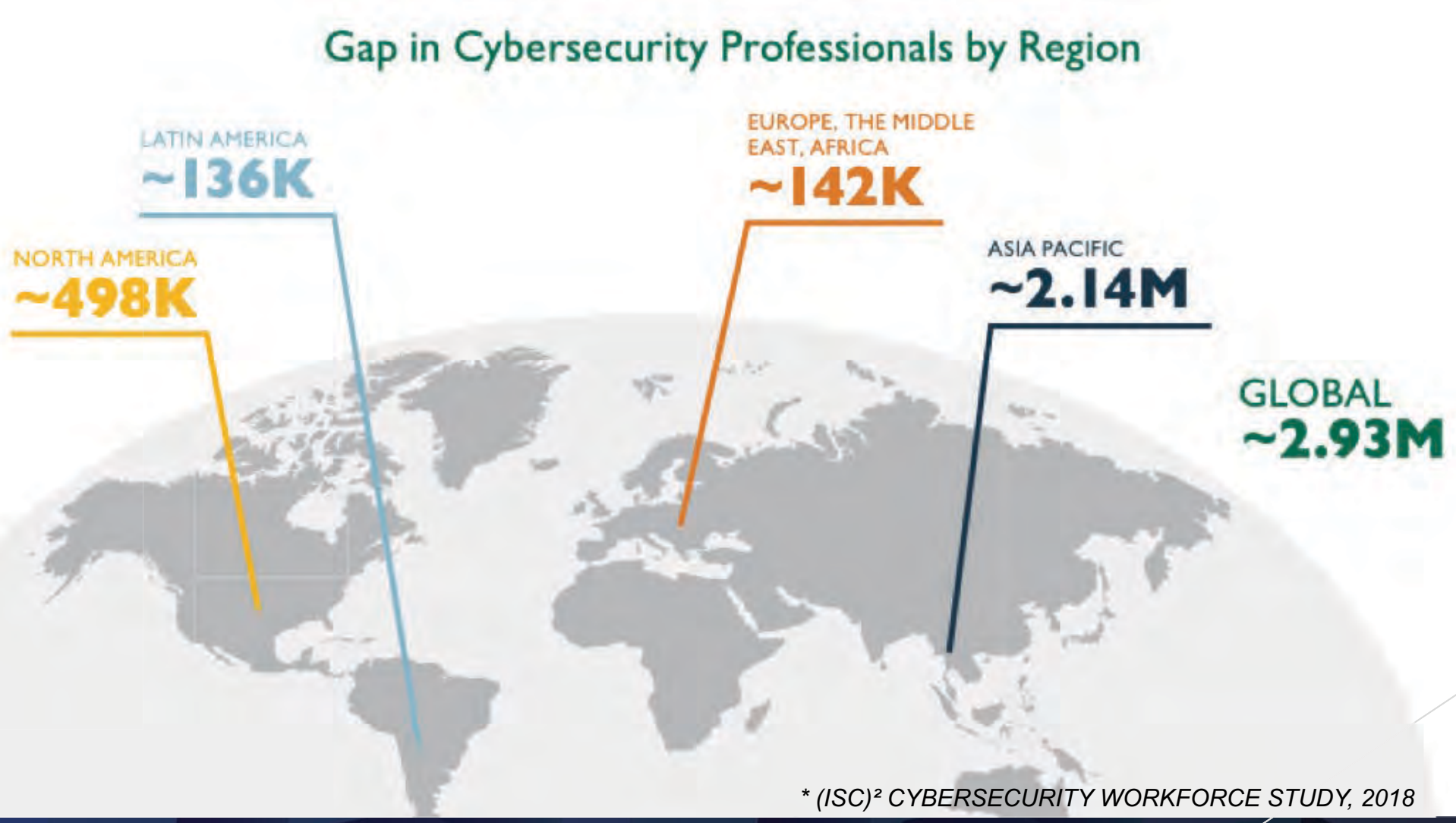
RAISE THE BAR 2020

Account Takeover Defenses

- DNSWatch
- WebBlocker
- AuthPoint
- Advanced Malware Detection

2020 Prediction:
The Cybersecurity Skills Gap Widens

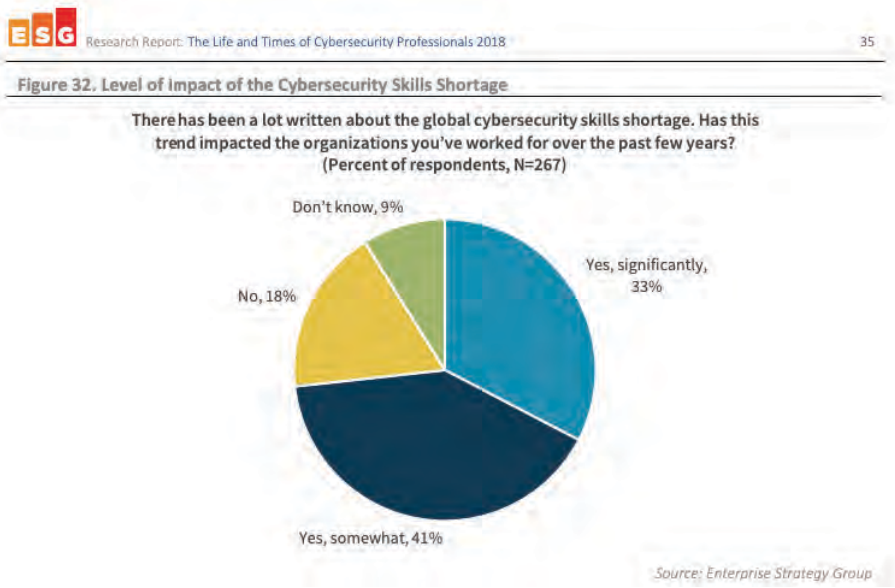
Cybersecurity Skill Gap 2018

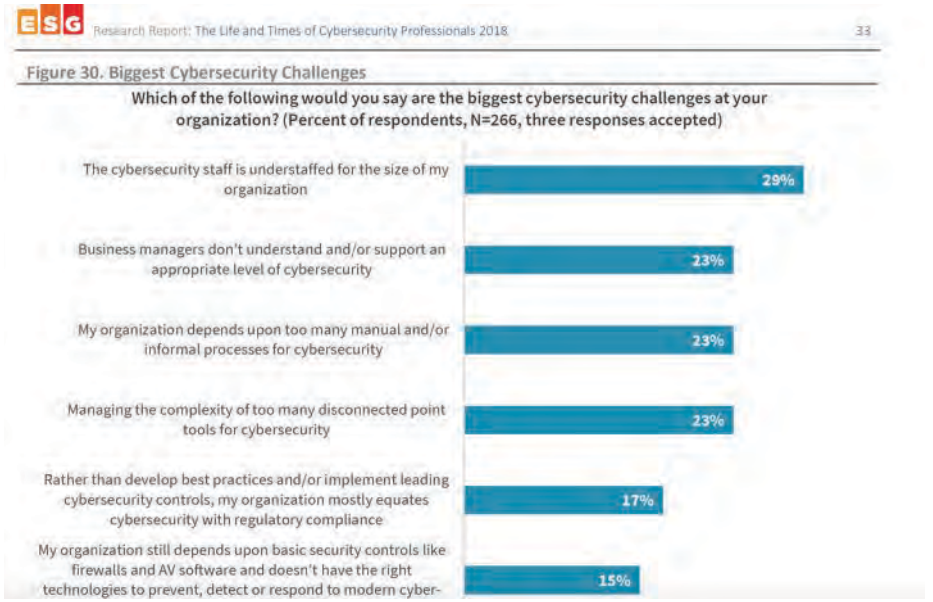


** (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018*

2021 Projected Cybersecurity Skill Gap

- 74% of companies claim the shortage lessens their security
- 29% claim it's their top cybersecurity challenge
- Cybersecurity Ventures' predicts **3.5m unfilled jobs in 2021**





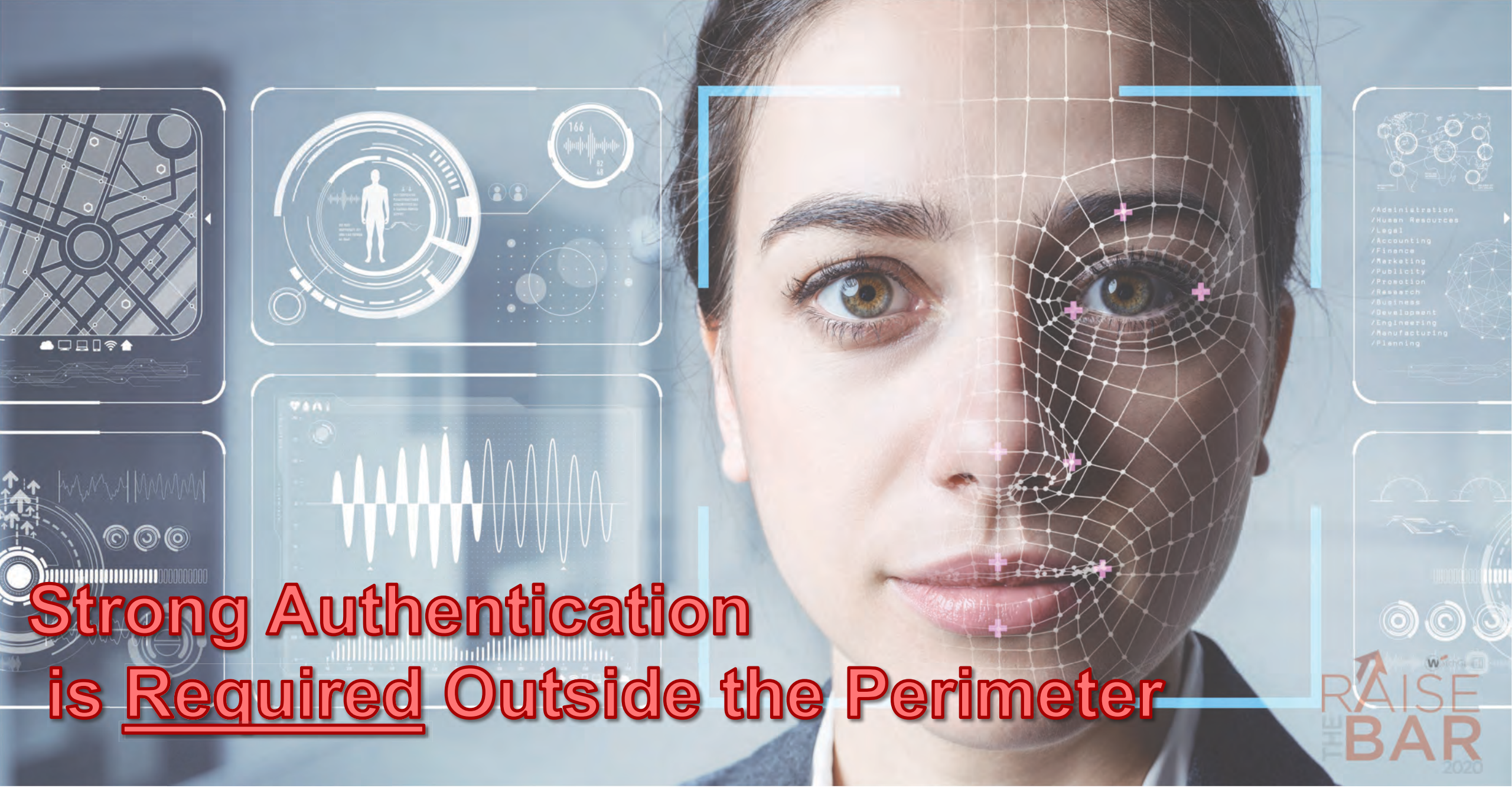
Your Partners Can Help (MSPs)

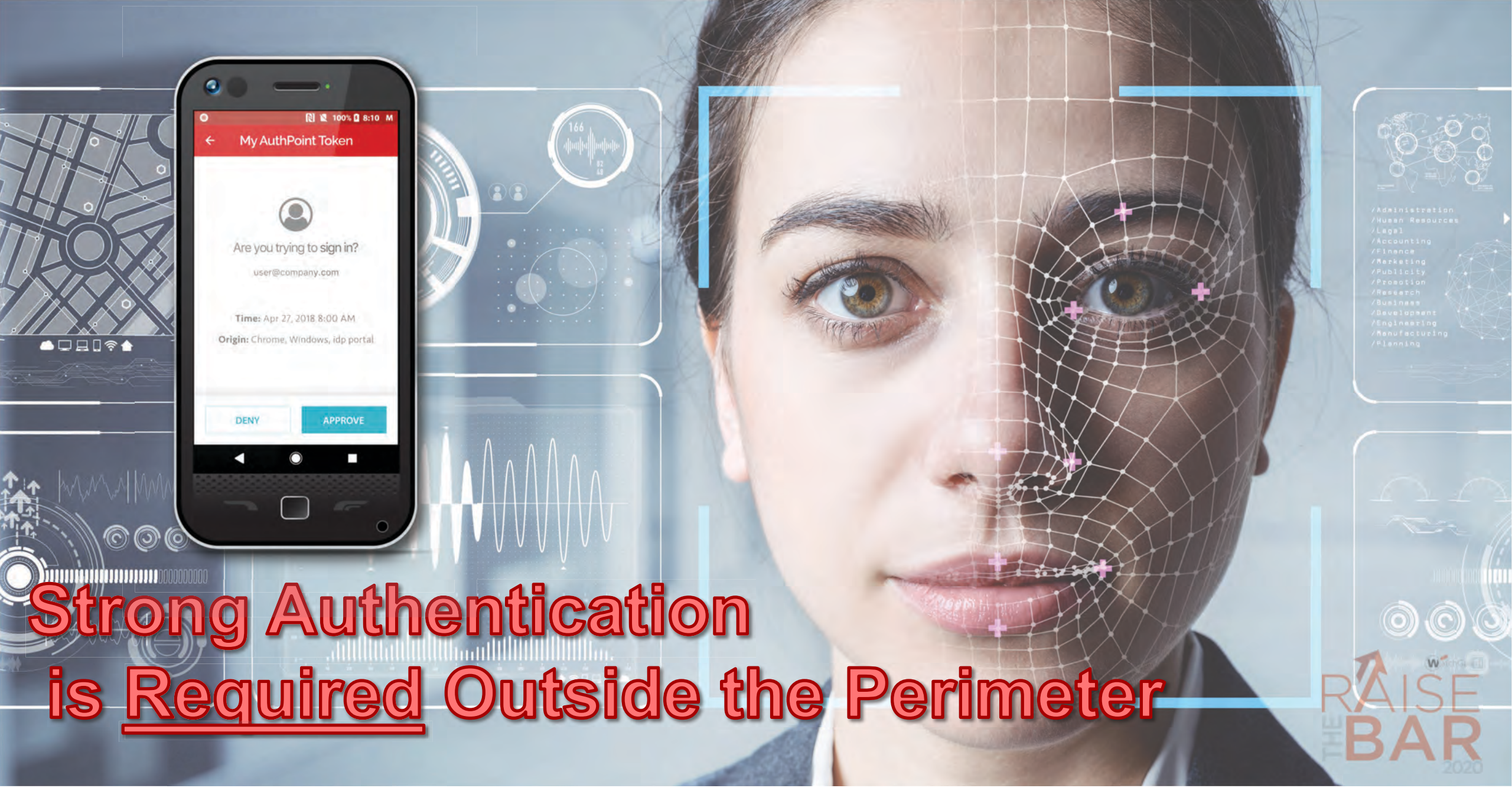
6 Work from Home Security Tips

For a Global Pandemic

WatchGuard

RAISE THE BAR 2020


Strong Authentication
is Required Outside the Perimeter
/Administration
/Human Resources
/Legal
/Accounting
/Finance
/Marketing
/Publicity
/Promotion
/Research
/Business
/Development
/Engineering
/Manufacturing
/Planning
THE RAISE BAR
2020

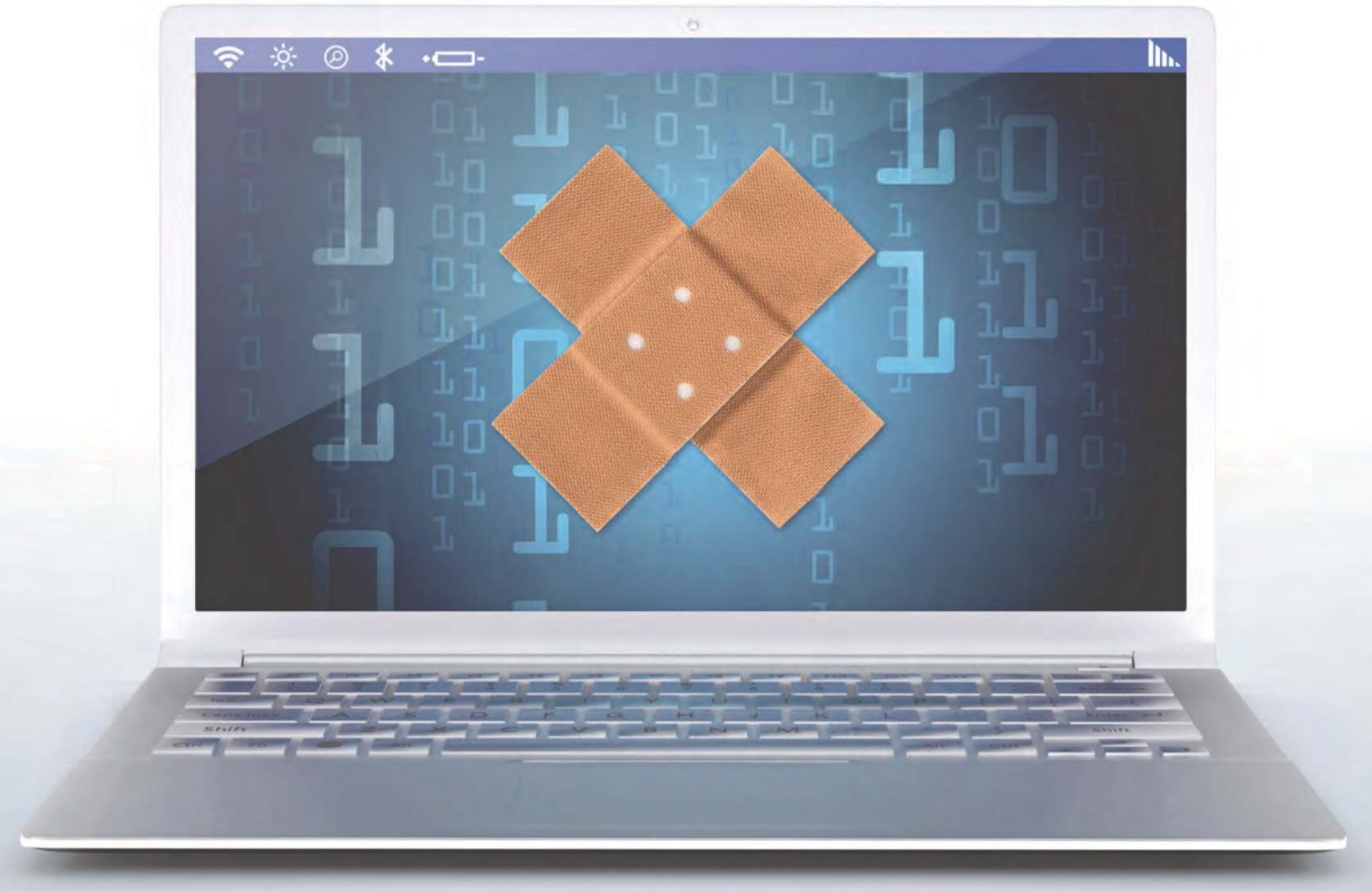

My AuthPoint Token
Are you trying to sign in?
user@company.com
Time: Apr 27, 2018 8:00 AM
Origin: Chrome, Windows, idp portal
DENY
APPROVE
Strong Authentication
is Required Outside the Perimeter
THE RAISE BAR
2020

VPNs Help Keep You Safe Anywhere

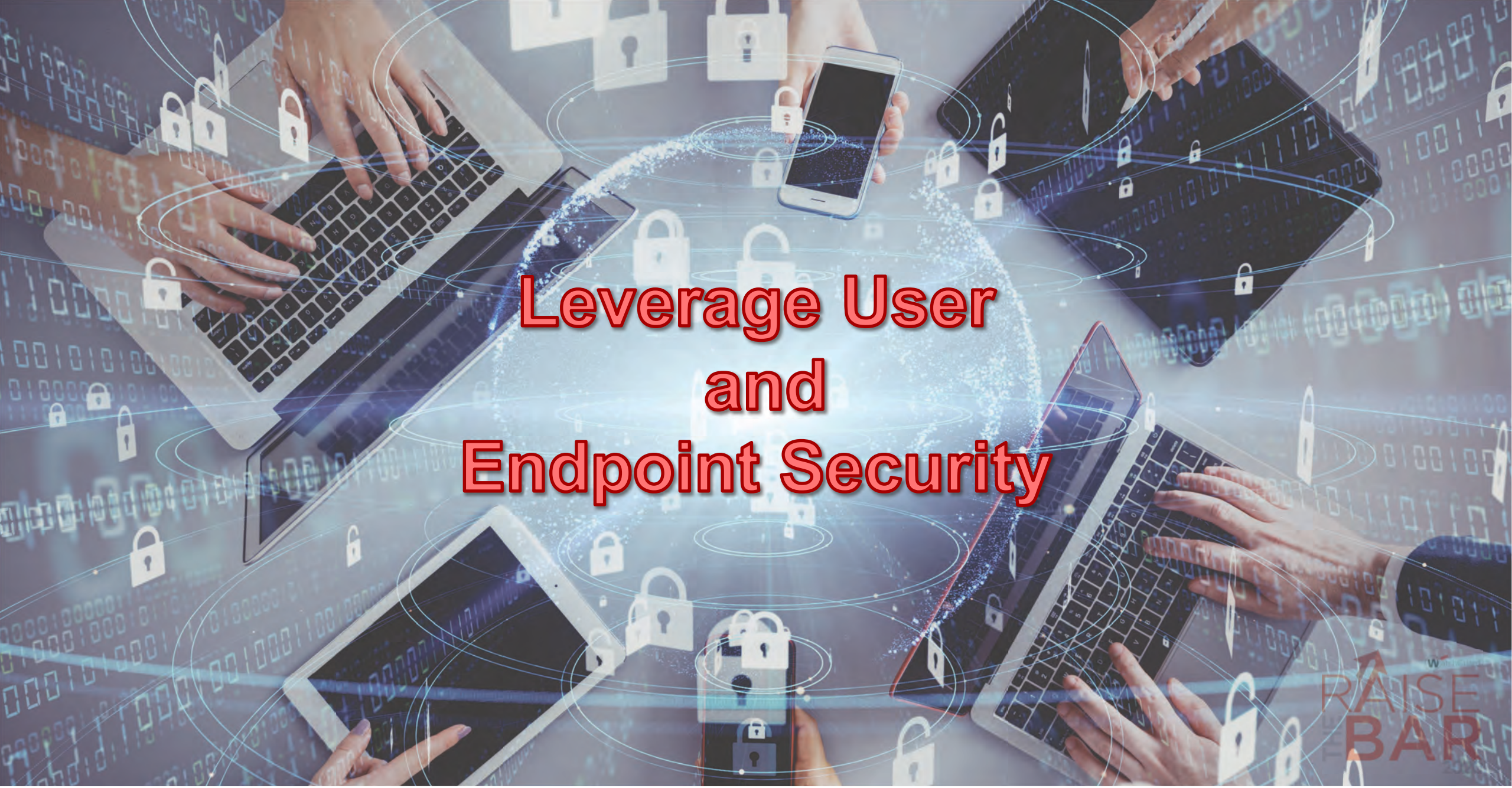
VPNs Help Keep You Safe Anywhere


New Tools, New Targets (Zoom, etc.)
RAISE THE BAR
2020

Updates Matter: A Culture of Patching



RAISE THE BAR 2020


Leverage User
and
Endpoint Security

WatchGuard Passport

Passport is an easy-to-buy bundle of user-focused security services.

Each service provides persistent, always-on protection that travels with your user.

WatchGuard

Two companies, ONE powerful security platform – from the network to the user

Beware Scams that Prey on Current Fears

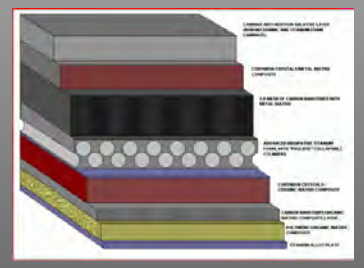
That’s too scary..... Puppy break!

WatchGuard:
Full Protection, Inside & Out

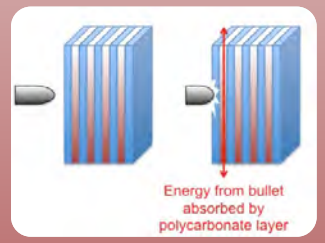
Layered Defense Still Wins…

Secure Facility

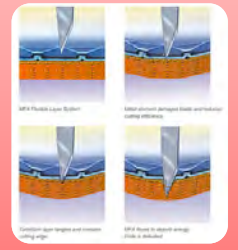
Tank Armor



Bulletproof glass



Bulletproof vest



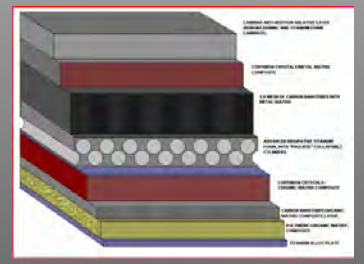
Chemical Safety

RAISE THE BAR 2020

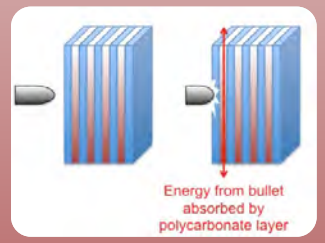
Layered Defense Still Wins…

Secure Facility

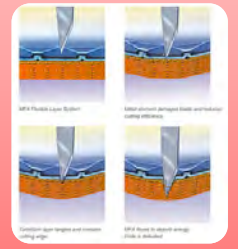
Tank Armor



Bulletproof glass



Bulletproof vest



Chemical Safety

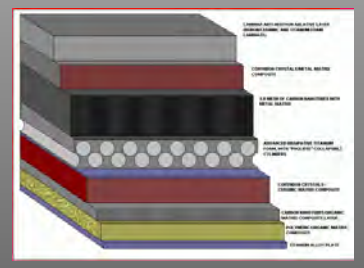
Cybersecurity

RAISE THE BAR 2020

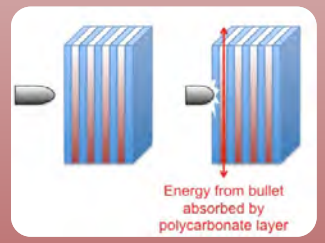
Layered Defense Still Wins…

Secure Facility

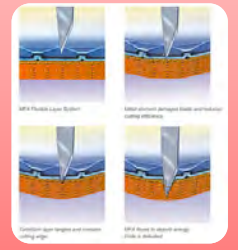
Tank Armor



Bulletproof glass



Bulletproof vest



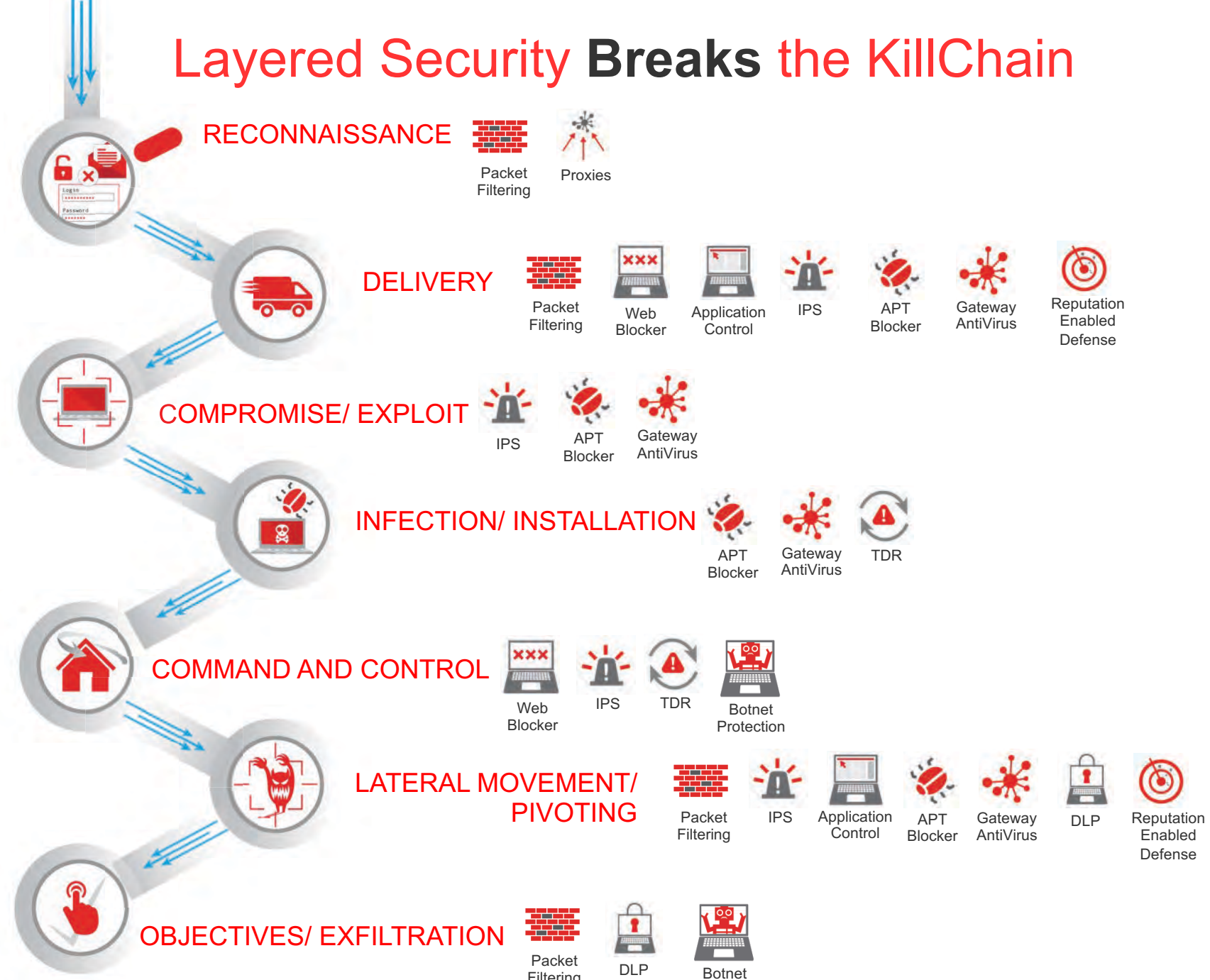
Chemical Safety

Cybersecurity

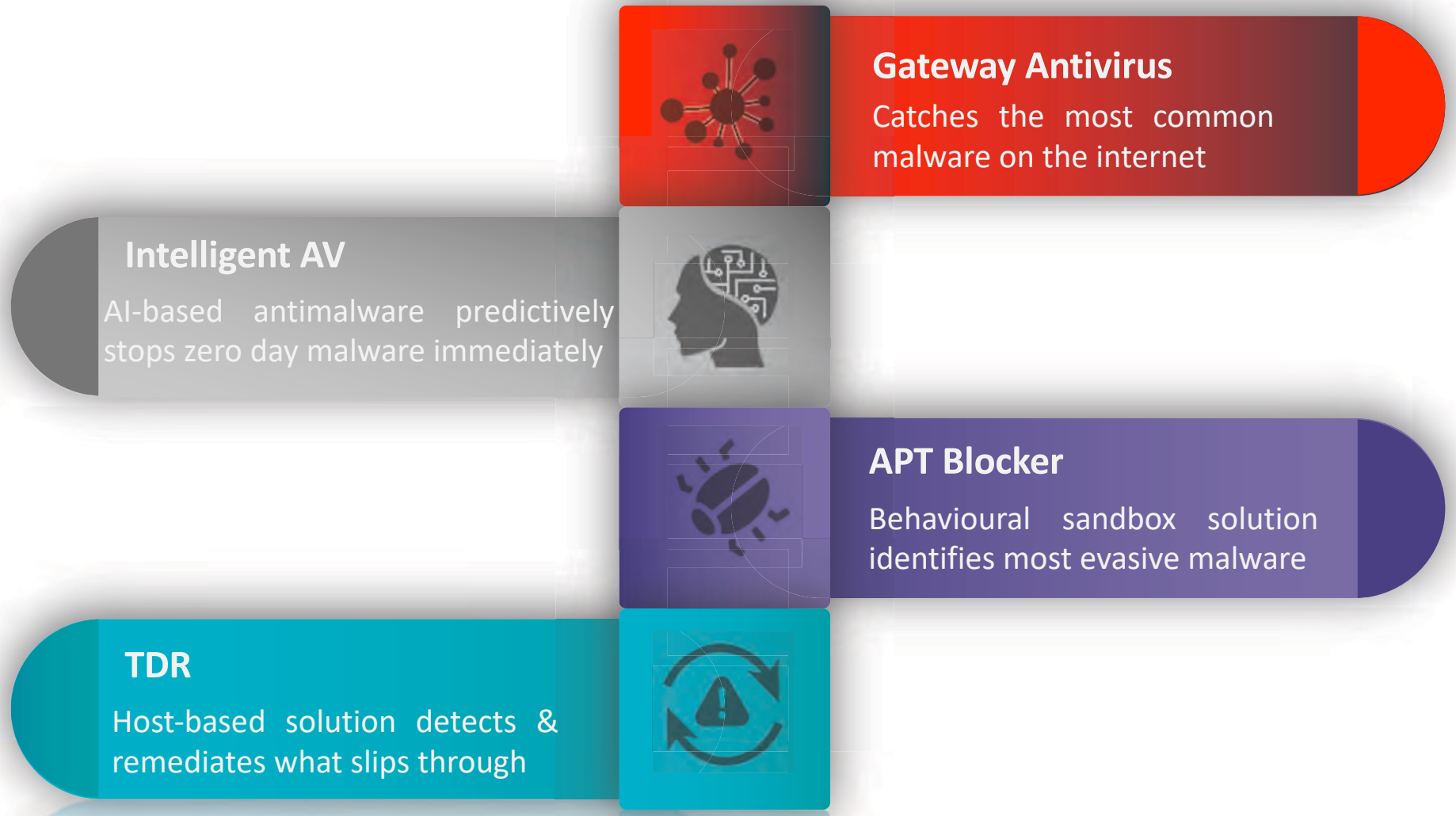
…but here's what to focus on in 2019

RAISE THE BAR 2020

Layered Security **Breaks** the KillChain



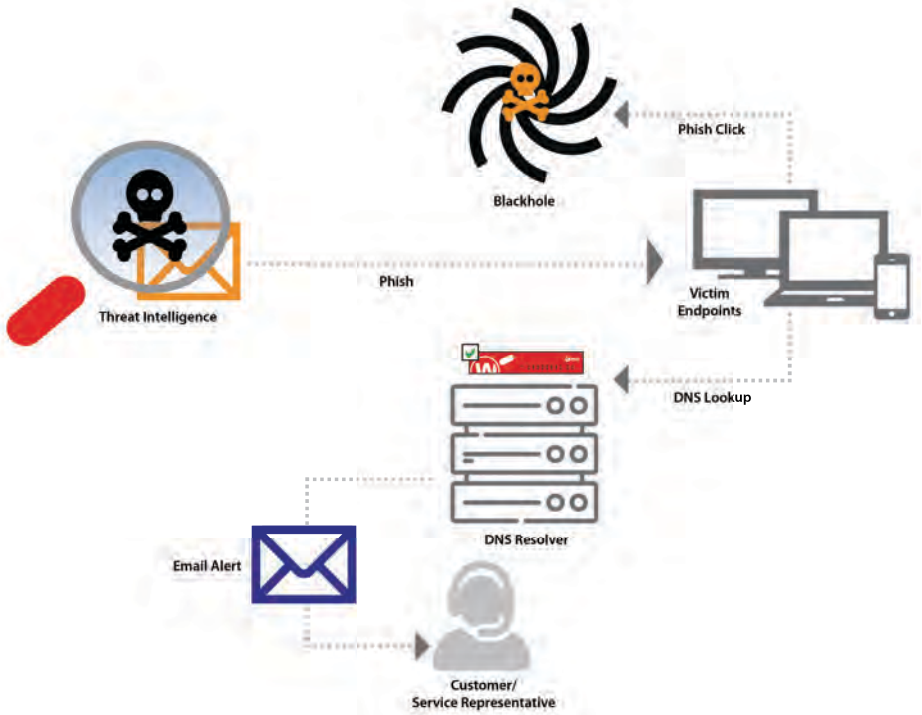
2020 Focus: Advanced Antimalware Pipeline



RAISE THE BAR 2020

2020 Focus: MFA with AuthPoint

2020 Focus: DNS Filtering



On-Prem

Off-Prem

RAISE THE BAR 2020

Learn more at... www.Secplicity.org

Daily Security Bytes

InfoSec Blog

The 443 Podcast

Google: 2019 Security Predictions Review – Hot Predictions
or https://www.youtube.com/watch?v=f-Y88U6iu9k

RAISE THE BAR 2020

THANK YOU

BTA's Building My Business Webinar Series

BTA's members-only webinar series is designed to improve your bottom line.

The June 4 webinar will be:

How to Operate & Manage a Remote Sales Team

4 p.m. Eastern, Thursday, June 4

Brandon Dawson
& Dave Robards
Cardone Enterprises

BTA COVID-19 Member Resources

Visit www.bta.org/COVID-19 for the following resources and more:

NEW DOCUMENTS:

- PPP Loan Forgiveness Application
- April 15 PPP Final Rule for Eligible Payroll Expenses

- Dealers Helping Dealers Q&A
- Bob Goldberg Q&A
- Webinars guiding dealers through the crisis
- COVID-19 Explanation of Laws
- Employee Rights Under the Family First Coronavirus Response Act Notice
- CARES Act information
- Paycheck Protection Program (PPP) information
- Essential Business Letter
- Short-Term Cash Flow Management During the COVID-19 Crisis
- CDC & OSHA Guidelines for Employers
- U.S. Chamber of Commerce Grant for small employers
- Bob Goldberg article on the use of face masks
- BTA COVID-19 LinkedIn Discussion Group link