
# PHISHING WITH FEAR



Cloudflare, Inc. acquired Area 1 Security in 2022

CLOUDFLARE
AREA 1 SECURITY

## PHISHING WITH FEAR

The mission of Area 1 Security is to eliminate phishing.

Every day, we hear directly from victims of phishing attacks. They will never be the subject of news headlines or criminal investigations. They reach out from the largest corporations in the world, startups and small businesses. Some are high-net worth individuals and public figures; many are family members and friends.

Phishing campaigns succeed because cyber actors find out how to turn emotion into action. Victims never succumb due to malice or stupidity.

Our innate curiosity, our desire to trust, and our child-like interest in a good story all make us susceptible to phishing, and cyber actors know this. We humans can't be taught to be less human. If we could, then training people to recognize and report the infinite number of ways they can be phished would have already prevented more breaches. Fortunately, our ability to think anew and act anew allows us to build technology that does what we on our own cannot[1].

Cyber actors "phishing with fear" find success amidst the current dogmas of cybersecurity:

1. Without any sophistication or cutting-edge computer science, cyber actors are able to use phishing successfully in 9 of 10 cybersecurity incidents.

2. While mega breaches fill reports and news headlines, cyber actors continue to use phishing to earn millions of dollars without recourse or repercussions.

3. Using their imagination, cyber actors evade cybersecurity aesthetes who respond to complexity.

The real challenge in cybersecurity today isn't technology. The technology to preempt cyberattacks already exists. The challenge is organizational inertia and industry focus.

[1] Why Cybersecurity Isn't So Complicated http://fortune.com/2016/02/09/cybersecurity-challenges/

OREN J. FALKOWITZ | CO-FOUNDER & CEO

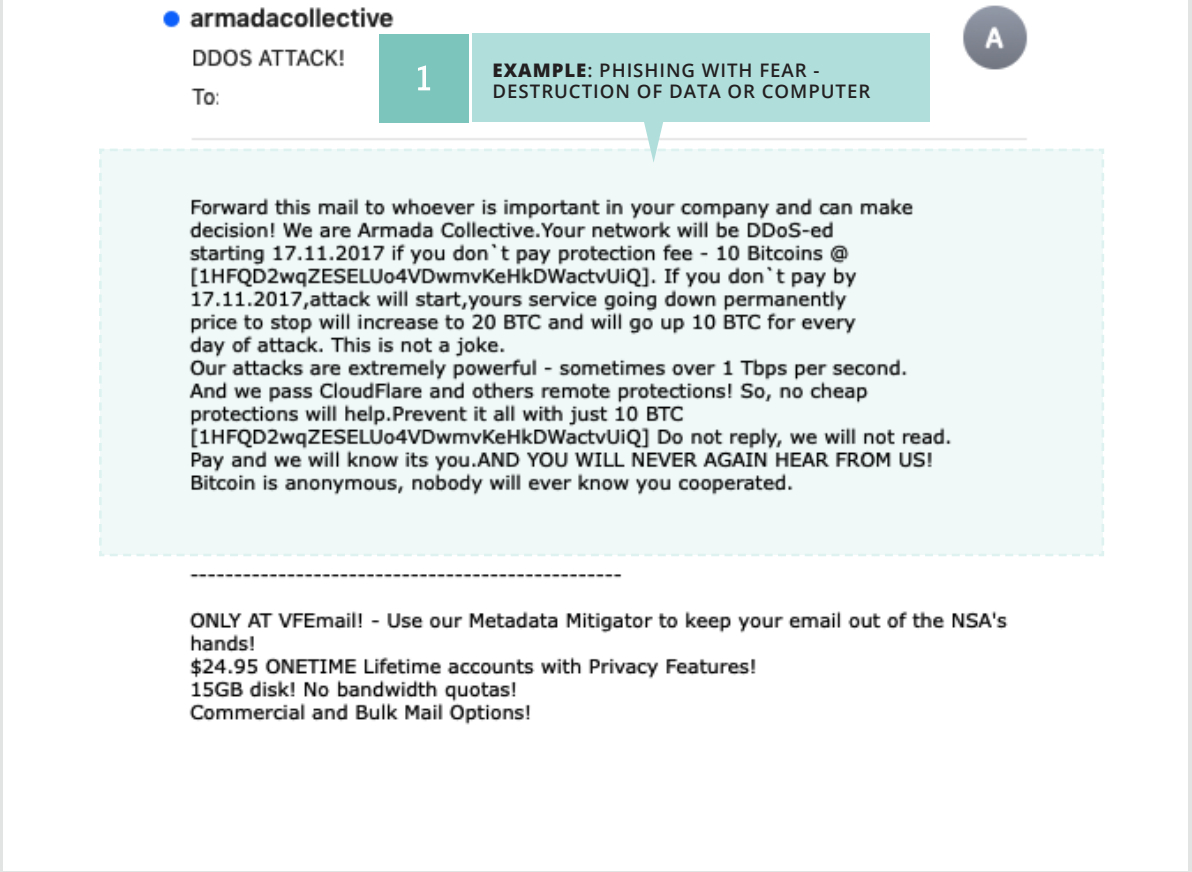
BLAKE DARCHE | CO-FOUNDER & CSO

# Campaign Details

An ongoing phishing campaign is earning millions of dollars for cyber actors with nothing more than empty threats.

*"Hey! I compromised your account..."* is enough fear to coerce thousands of individuals into paying extortion that includes leaking compromising pictures or videos, threats of physical violence including bombings, computer destruction, and data deletion.

---



[redacted] April 4, 2019 at 9:07 AM

[redacted] joker112

To: [redacted]

Reply-To: [redacted]

I

2 **EXAMPLE:** PHISHING WITH FEAR - COMPROMISING PHOTOS OR VIDEOS

I am aware joker112 is one of your pass words. Lets get directly to point. No one has paid me to investigate about you. You don't know me and you're most likely thinking why you're getting this email?

Let me tell you, i actually installed a software on the adult vids (pornography) web site and you know what, you visited this site to have fun (you know what i mean). While you were watching videos, your internet browser began working as a Remote Desktop that has a keylogger which provided me with accessibility to your display screen as well as web cam. Right after that, my software program obtained your complete contacts from your Messenger, FB, and emailaccount. Next i created a video. First part shows the video you were viewing (you've got a fine taste hehe), and second part shows the recording of your webcam, & its you.

You got not one but two options. Lets understand each one of these solutions in particulars:

First choice is to just ignore this message. as a consequence, i will send your videotape to every one of your personal contacts and you can easily imagine concerning the disgrace you will get. Furthermore if you happen to be in an intimate relationship, exactly how it can affect?

Latter choice is to compensate me USD 989. Lets name it as a donation. in this instance, i most certainly will without delay eliminate your videotape. You can carry on your daily routine like this never happened and you will not hear back again from me.

You'll make the payment through Bitcoin (if you do not know this, search for 'how to buy bitcoin' in Google search engine).

BTC address: 1PGXeJqk5A9KsTPSbwYiRBSiturESBmf1y

Elisabeth Harris

Your building is under my control

To: [redacted]

EH

3 **EXAMPLE:** PHISHING WITH FEAR - PHYSICAL VIOLENCE

Good day. My mercenary has hidden the bomb (tronitrotoluene) in the building where your business is located. My mercenary constructed an explosive device according to my guide. It is compact and it is hidden very carefully, it can not damage the structure of the building, but you will get many victims in case of its explosion.
My recruited person keeps the building under the control. If any unusual behavioror policeman is noticed the device will be exploded.
I can call off my mercenary if you make a transfer. You send me 20.000 dollars in Bitcoin and explosive will not detonate, but don't try to cheat -I ensure you that I have to call off my mercenary solely after 3 confirmations in blockchain network.

Here is my Bitcoin address : 1Dnw2qJxGFCZdE3PzCaVioBB9zERc7SzRB

You must send money by the end of the working day. If you are late with the payment the bomb will explode.
This is just a business, if I do not receive the bitcoin and a bomb explodes, other commercial enterprises will pay me more money, because it isnt an isolated incident.
To stay anonimous I will not log into this email. I check my wallet every thirty min and after seeing the bitcoins I will give the command to my man to get away.

If an explosion occurred and the authorities notice this email!
We arent terrorists and dont take liability for acts of terrorism in other buildings.

# Game of Numbers

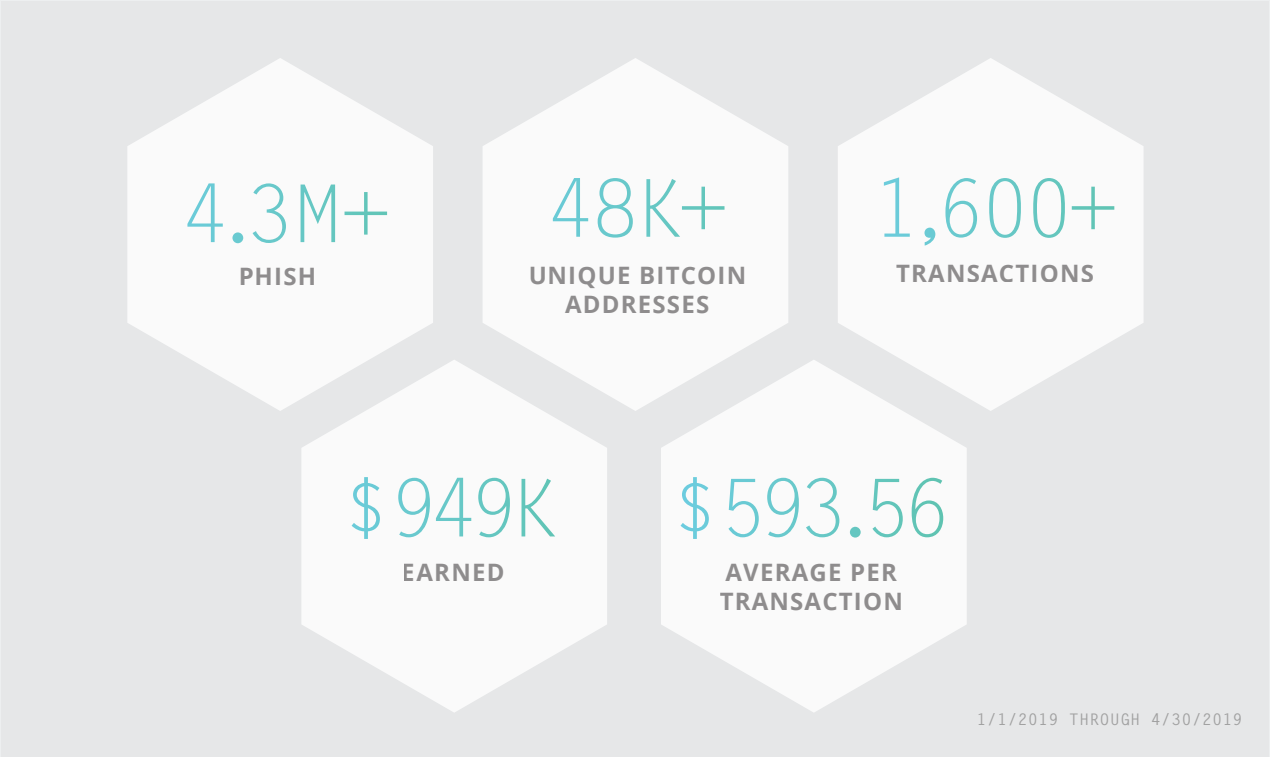
Cybersecurity experts immediately recognize -- as empty threats -- these phishing lures, but those not steeped in phishing, or filled with the paranoia of cybersecurity professionals, are falling victim at an alarming rate.

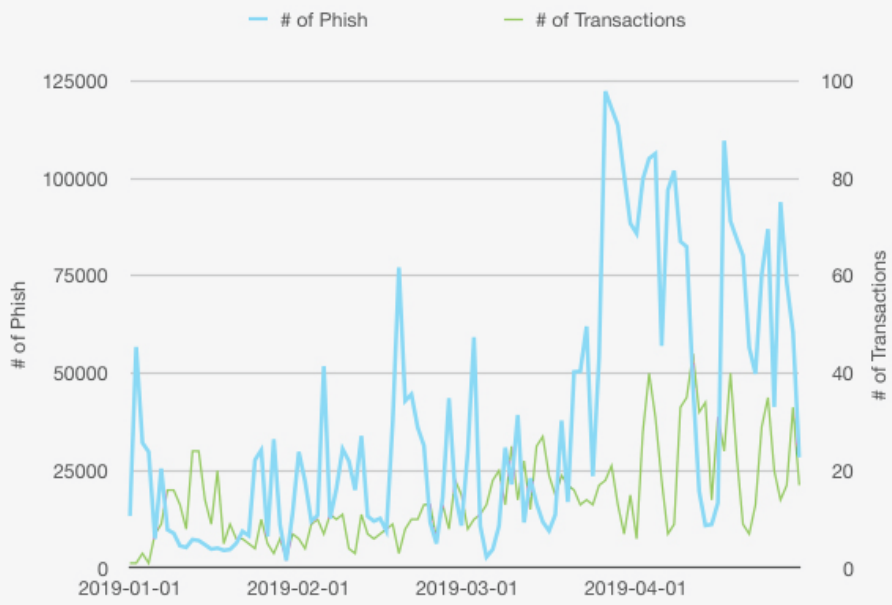
An analysis of over 4.3 million "phishing with fear" emails detected by Area 1 Security offers insight into the nature of the campaign messages, revealing an ability to bypass SEGs and Cloud provider anti-spam solutions; and leading to significant financial gain for cyber criminals.

While mega-breaches at Marriott, Equifax, and Facebook fill the headlines, the economics of being a bad guy on the internet remains a highly lucrative business today. It's been clear for some time that we're moving on a trajectory from data theft to data and network ransom, to data manipulation and physical destruction. That you can send a phishing campaign without even rudimentary knowledge of how to code malware or manipulate Windows internals, yet earn a million dollars, means that the equilibrium in the cybersecurity marketplace is shifting dramatically in favor of attackers.

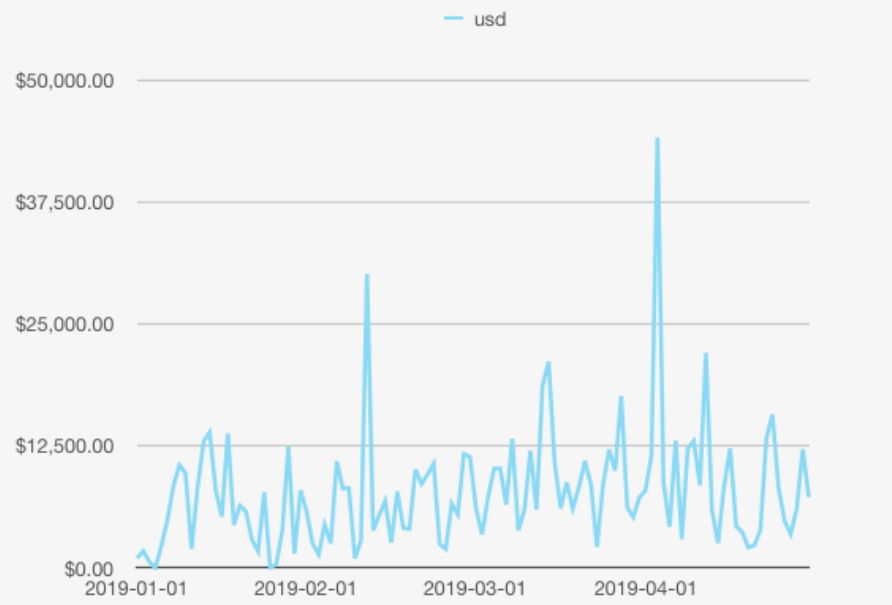
Within the 4.3 million phish, we identified 48,000 unique Bitcoin addresses used by cyber actors to receive funds. Our analysis of the wallets shows over 1,600 transactions totaling 174.042 Bitcoins[1] valued at $949,703.45 -- nearly $600 per transaction.

[1] 1 Bitcoin == $5,321.15 on 5/1/2019






Cyber actors manage to steal tens of thousands of dollars on a daily basis, if not more, using nothing more than fear



# Why Attackers are Getting Away with It

We've identified at least three specific techniques that cyber actors phishing with fear use to evade detection of Secure Email Gateways (SEGs) and cloud inbox provider spam engines in this campaign.

1. New and "clean" sending addresses fail to be detected by SEGs and spam filters that rely on reputation-based analytics. It's never been easier to register a new email account with Google or Microsoft that has a perfect reputation and passes all of the sender authentication checks such as DKIM, DMARC, and SPF.

2. We all know that training is not effective at stopping phishing. The use of evolving themes ensures individual users will be unable to pattern recognize these campaigns before their emotions of fear take over.

3. Text evasion and white spacing including the use of images in the body of the email to present text, rather than typing the text itself. In so doing, the attacker could evade detections that search for keywords commonly found in malicious emails. Another technique, intended to evade the same type of detection, involved inserting HTML tags or zero width unicode characters to break up words in the body of the email. With this technique, the content of the email remains human readable but the additional tags or whitespace render keyword search ineffective. In the last technique, the attacker spoofed the sender email address to make it appear as if it was sent from the target's own email account.

4. Lexical scramblers / obfuscation involves the use of legitimate text within a message body usually hidden below the normal campaign message. Typically this text can involve the use of literary passages or garbled text with no meaning. These are used to defeat legacy techniques that focus on simple heuristics such as message length or number of characters in the message; and / or message intent. To an untrained model the use of Jane Austen's or Lord Byron's works within a Bitcoin Phish message can look like a legitimate correspondence and is intentionally used to evade detection.


Yesterday at 4:02 PM
JC
To:
Reply-To:
4
EXAMPLE: BITCOIN FEAR PHISH
Well, I believe, $2900 is a reasonable price tag for our little secret. You will make the payment through Bitcoin (if you don't know this, search "how to buy bitcoin" in Google).
BTC Address: 1BsbsB92VLVQgNCQaLo7Z6LvS31CANJKpd
(It is cAsE sensitive, so copy and paste it)
Note:
You have one day to make the payment. (I've a unique pixel within this email message, and now I know that you have read this e-mail). If I don't get the BitCoins, I will send out your video to all of your contacts including relatives, co-workers, and many others. However, if I receive the payment, I'll destroy the video immidiately. If y really want evidence, reply with "Yes!" and I definitely will send your video recording to your 14 friends. It is a no negotiable offer, thus don't waste my time and yours by replying to this e mail.
5
SEPARATED BY A LARGE AMOUNT OF WHITESPACE APPEARING BELOW THE READER'S EYE LINE
6
FOLLOWED BY LEXICAL OBFUSCATION USING UNRELATED PROVERBS
With money you would not know yourself, without money nobody would know you. - Spanish Proverb
A cur's tail grows fast. - Italian Proverb
Find something you love to do and you'll never have to work a day in your life. -Harvey Mackay
He who lives on hope, dies of hunger. - German Proverb
Jane Austen~ In every power of which taste is the foundation excellence is pretty fairly divided between the sexes
Cats pose a danger to pregnant women and immunosuppressed inividuals, since their feces can transmit
7
JANE AUSTEN – "IN EVERY POWER OF WHICH TASTE IS THE FOUNDATION OF EXCELLENCE..."
e the last.
's the fly's day off.
ton Mather
Frank A. Clark~ Real generosity is doing something nice for someone who will never find it out.
A noisy noise annoys an oyster.
He who controls others may be powerful, but he who has mastered himself is mightier still. -Tao Te Ching
Cats are independent, by which I mean smart. - D. Barry

```
My Bit<span>&#8203;</span>co&#8203;in wal<span>&#8203;</span>let Addre&#8203;ss:<br><span aelizu="aelizu" style="padding:0
;margin: 0;" ><div  id="eioedoderadluynesvymy" style="padding:0;margin: 0;" ></div><div ecsh="ecsh" id="oaojeaicajqihiaayy
s" style="padding:0;margin: 0;" ></div><span xpr="xpr" style=" margin: 0;padding:0;" ><div ywzbye="ywzbye" style=" margin:
 0;padding:0;" ></div><span  style="padding:0;margin: 0;" ></span><span ujwiao="ujwiao" style="padding:0;margin: 0;" ><div
  class="ejooyciimofinwawi" style="padding:0;margin:0;"></div><span bpvh="bpvh" style="padding:0;margin: 0;" ></span><div
 id="ovdoabmloiarjeyuiztaa" style="padding:0;margin: 0;" ></div><span qsi="qsi" style=" margin: 0;padding:0;" ></span></sp
an><span owez="owez" style=" margin: 0;padding:0;" ></span><span  class="pkiyyoicyxqaopemiikp" style="padding:0;margin:0;"
></span><span rjnqyc="rjnqyc" style=" margin: 0;padding:0;" ></span></span><div ttcota="ttcota" style="padding:0;margin:0;
"><span  class="kaefdafywtuosiojgga" style="padding:0;margin:0;"></span><div ymjlfd="ymjlfd" style="padding:0;margin: 0;"
></div><div fgniab="fgniab" style=" margin: 0;padding:0;" ></div><div  id="uxeeeiipyoaayfiefkyxyzbk" style="padding:0;marg
in: 0;" ></div></div><span  style="padding:0;margin:0;"></span><span zyoy="zyoy" style=" margin: 0;padding:0;" ><span piye
g="piyeg" id="asaeeeaaaledyilvaheghxb" style="padding:0;margin: 0;" ><span  style="padding:0;margin: 0;" ></span><span  sty
le="padding:0;margin: 0;" ></span><span  style="padding:0;margin:0;"></span><span xtiyk="xtiyk" style="padding:0;margin:0;
"><b>1Kth<img alt="" width="0" src="https://img.crarsmoog.org/shuvfloct/mipjuw" height="0">UFkKjDVgP5GU<img alt="" width="
0" src="https://images.hafsmiss.net/fulpreft/glashwiv" height="0">fUkdbhzVTGe1jH<img alt="" width="0" src="https://www.yof
tsmast.org/smaptbref/kegbriss" height="0">bm43</b></span><div wiaiaf="wiaiaf" id="riyeaqjlawearvyisco" style="padding:0;ma
rgin: 0;" ></div></span><span  style="padding:0;margin: 0;" ><span  id="xpdynjylixdebaaqaebaykde" style="padding:0;margin:
 0;" ></span><span  class="ibepiyayedofvqyjakw" style="padding:0;margin:0;"></span><span  id="rktroqbaicokwlyoxl" style="p
adding:0;margin: 0;" ></span><div otwn="otwn" style=" margin: 0;padding:0;" ></div><div  style="padding:0;margin: 0;" ></d
iv><span  style="padding:0;margin: 0;" ></span></span><span kyo="kyo" class="vbyoeiyavaayhefaafal" style="padding:0;margin
:0;"><div  id="ejokiiedoyobagg" style="padding:0;margin: 0;" ></div><div  style=" margin: 0;padding:0;" ></div><span lfvuk
="lfvuk" style="padding:0;margin: 0;" ></span><span  style="padding:0;margin:0;"></span><div eecloh="eecloh" class="oqoive
ieennrelijej" style="padding:0;margin:0;"></div><span  style="padding:0;margin: 0;" ></span></span><span ooe="ooe" id="emy
enijtrdnoytq" style="padding:0;margin: 0;" ></span></span><div  class="miibzozlqacyseikyjaocs" style="padding:0;margin:0;"
></div></span><span  style=" margin: 0;padding:0;" ></span><span  id="msluieucvfxfaeoziolyo" style="padding:0;margin: 0;"
></span><div eibtag="eibtag" style=" margin: 0;padding:0;" ></div><br>
<br>
```

8 **EXAMPLE**: PHISHING WITH FEAR - HTML TAGS INVISIBLE TO THE READER

```
He&#8204;llo&#8204;
<br><br>
I'm a&#8204; ha&#8204;cke&#8204;r who&#8204; cra&#8204;cke&#8204;d yo&#8204;u&#8204;r e&#8204;ma&#8204;i&#8
04;l a&#8204;s we&#8204;ll a&#8204;s de&#8204;vi&#8204;ce&#8204; a&#8204; co&#8204;u&#8204;ple&#8204; o&#82
4;f mo&#8204;nths ba&#8204;ck.
<br><br>
```

9 **EXAMPLE**: PHISHING WITH FEAR - HTML UNICODE WHITESPACE OBFUSCATION

# How to Solve for This

Traditional approaches to fighting these attacks off are not working.

Buying insurance against the possibility of a breach is a misuse of resources. SEGs are not solving the problem. Trying to train people out of responding to these fear-provoking prompts is not enough. Remediation and autopsy are too little, too late, and too expensive. And because these attacks are so easy to mount, we can only expect that the problem will become more severe over time.

The rational and ***effective*** approach is to ***preempt*** e-mails that phish with fear. Preemption is the proven strategy for success, rather than cleaning up messes after malicious links have been clicked.

When security leaders broaden their focus to preemption, they will finally get something that up until now has been unavailable at any price: cybersecurity they can rely on to keep their organizations and their employees undistracted, safe and secure.