SECURITY MANAGEMENT PARTNERS

PASSWORD RESET (YOUR WAY OF THINKING)

JUNE 2019

YOUR SPEAKER

Matt Repicky, CISSP, CISA

Principal Security Consultant, SMP

Based in Waltham, MA, Security Management Partners is a full-service Information Security and IT assurance consulting firm. Since 2001, we've conducted thousands of client engagements, including audits, assessments, incident response and forensics services.

OVERVIEW

- How did we get here?
- Security guidelines for 2019 and beyond
- Hacking passwords
- Countermeasures
- Limited Trust

DATA BREACH HISTORY

- AOL (2005) – 92 Million
- T.J. Maxx (2007) – 94 Million
- Target (2013) – 70 Million
- Home Depot (2014) – 56 Million
- Anthem (2015) – 80 Million
- Yahoo (2013-2017) – 3 Billion

2019 LIST

- Facebook
- First American
- Quest Diagnostics / LabCorp
- Fortnite
- Dunkin' Donuts
- Oregon Department of Human Services
- FEMA
- Verifications.io
- Georgia Tech
- Baystate Health
- Houzz
- Instagram
- WhatsApp

FOLLOW ALONG

- Identity Force (https://www.identityforce.com/blog/2019-data-breaches)
- IT Governance Blog (https://www.itgovernance.co.uk/blog)
- Fraud.org (https://www.fraud.org/latest_breaches)
- Wikipedia (https://en.wikipedia.org/wiki/List_of_data_breaches)
- Brian Krebs (https://krebsonsecurity.com/)
- ID Theft Resource Center (https://www.idtheftcenter.org/data-breaches/)
- HaveIBeenPwned (https://haveibeenpwned.com/)
- Data Breach & Security Reports (Verizon, IBM, Varonis, Trustwave, Cisco, …)

WHAT DO THE REPORTS SAY?

- Breaches cost $$$ (average $148/record, $3.86m / breach)
- 1-in-4 breaches caused by human error
- Ransomware attacks down
- Bitcoin mining attacks up

REPORTS (CONT'D)

- Quicker containment saves $$$
- Avg time to identify breach – 197 days
- Avg time to contain breach – 69 days
- 445.6m records exposed : 1,244 breaches (2018)

WHY PASSWORDS?

- Passwords are the keys to the kingdom
- Common attack vectors
- Easily exploitable

UNCOVER PASSWORDS

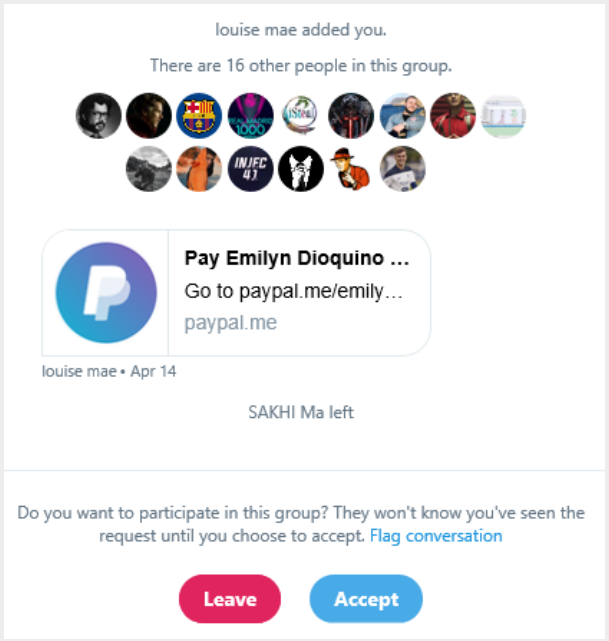
- Passwords are EVERYWHERE
  - 3rd party compromises
  - AWS s3 buckets, other cloud containers
  - Email
  - Post-its
  - Registry, LSASS, INI files, Config files, Excel files
  - Wikis
  - Chat logs
  - Google searches

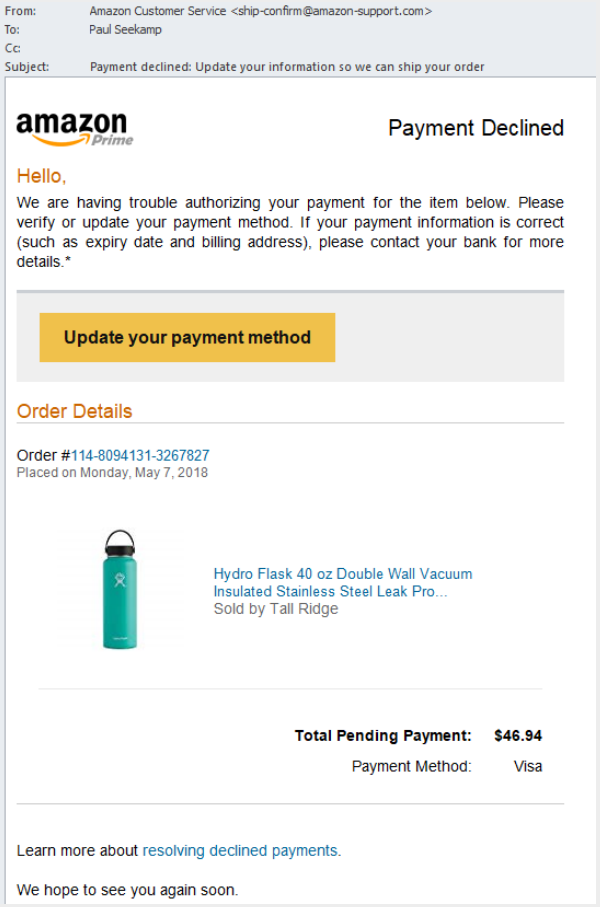
MORE PASSWORDS

- Guessing Attacks
  - Online or Offline
- Sniffing Attacks
  - Starbucks Wireless
  - Airport Wireless
  - Rogue Wireless
- Man In The Middle

THE CATCH ALL

- End-user Vulnerabilities
- Phishing
- Smishing
- Vishing





WE ARE COMPLIANT!

- Passwords are:
  - stored and transmitted securely
  - changed every x days
  - meeting regulatory standards
- We don’t use wireless
- SSL Certificates on all services
- Users are trained to identify Phishing and Vishing attacks

WHAT IS A COMPLIANT PASSWORD?

- Length
  - NIST - 8 Characters
  - PCI - 7 Characters
  - HIPAA - 8 Characters
  - MSFT - 8 Characters
- Complexity
  - uppercase characters
  - lowercase characters
  - non-alphanumeric characters

COMPLIANCE VS SECURITY

- A 2010 study by Weir et al. found that users will simply capitalize the first letter of their password and add a “1” or “!” to the end, making the password no harder to crack.
- When required to use numbers in their passwords, 70% of users on added numbers before or after their password.

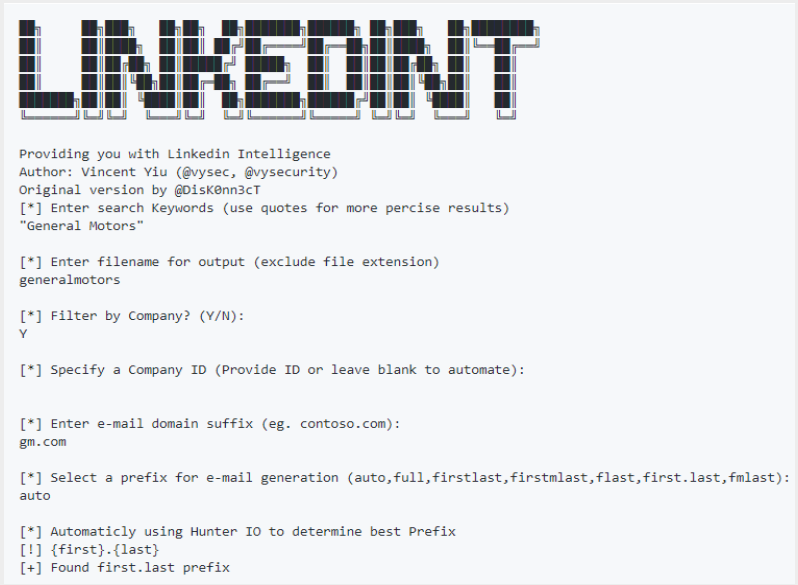
*statistic source: https://auth0.com/blog/dont-pass-on-the-new-nist-password-guidelines/

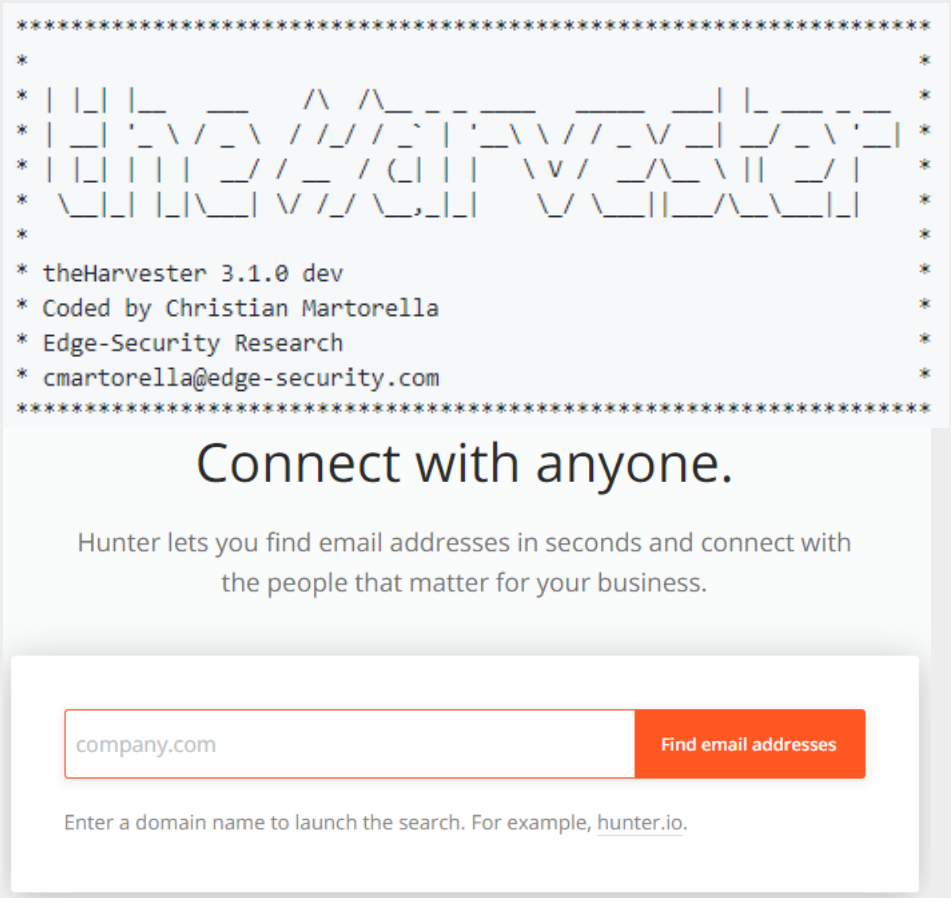
HOW CAN WE LEVERAGE "COMPLIANCE"?

- Make a list of common passwords:
  - {Season}{year}
  - {Month}{year}
  - {Company}{123}
  - {Company}{!}
  - {Sports team}{123}
  - {Town}{123}
  - {Keyboard walk} (qwerty, 1qazxsw2)
  - {Company Lingo}{123} (Taxi = PickUpper)

NOW WHAT?

- Scrape the Internet!





REVERSE BRUTEFORCE

- Log all the users in at once, using one password at a time.

MULTIFACTOR FTW?

- Call/text the target – ask for code
  - http://bluffmycall.com/
  - https://www.spooftel.com/freecall/
  - http://www.spoofmytext.com/
  - http://textopirate.com/en
- Log into other systems
  - Web or Mobile Applications
  - VPN
- Plan a physical attack
  - Drop a USB
  - Plug a drop box in reception area
  - Radius Wireless

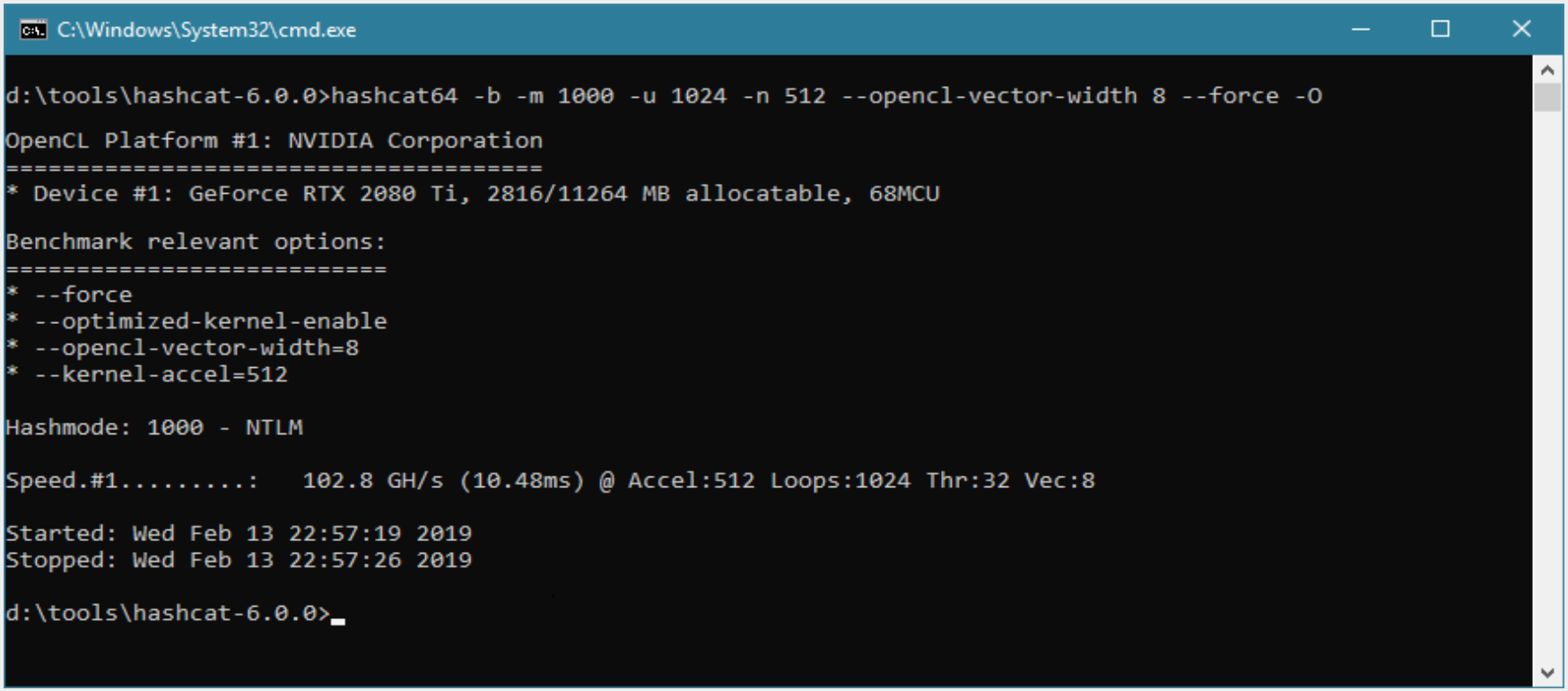
NICE TRY

- Our passwords are not that easy.
- We blacklist “weak” passwords.
- We bought a tool that limits repetition and consecutive characters.

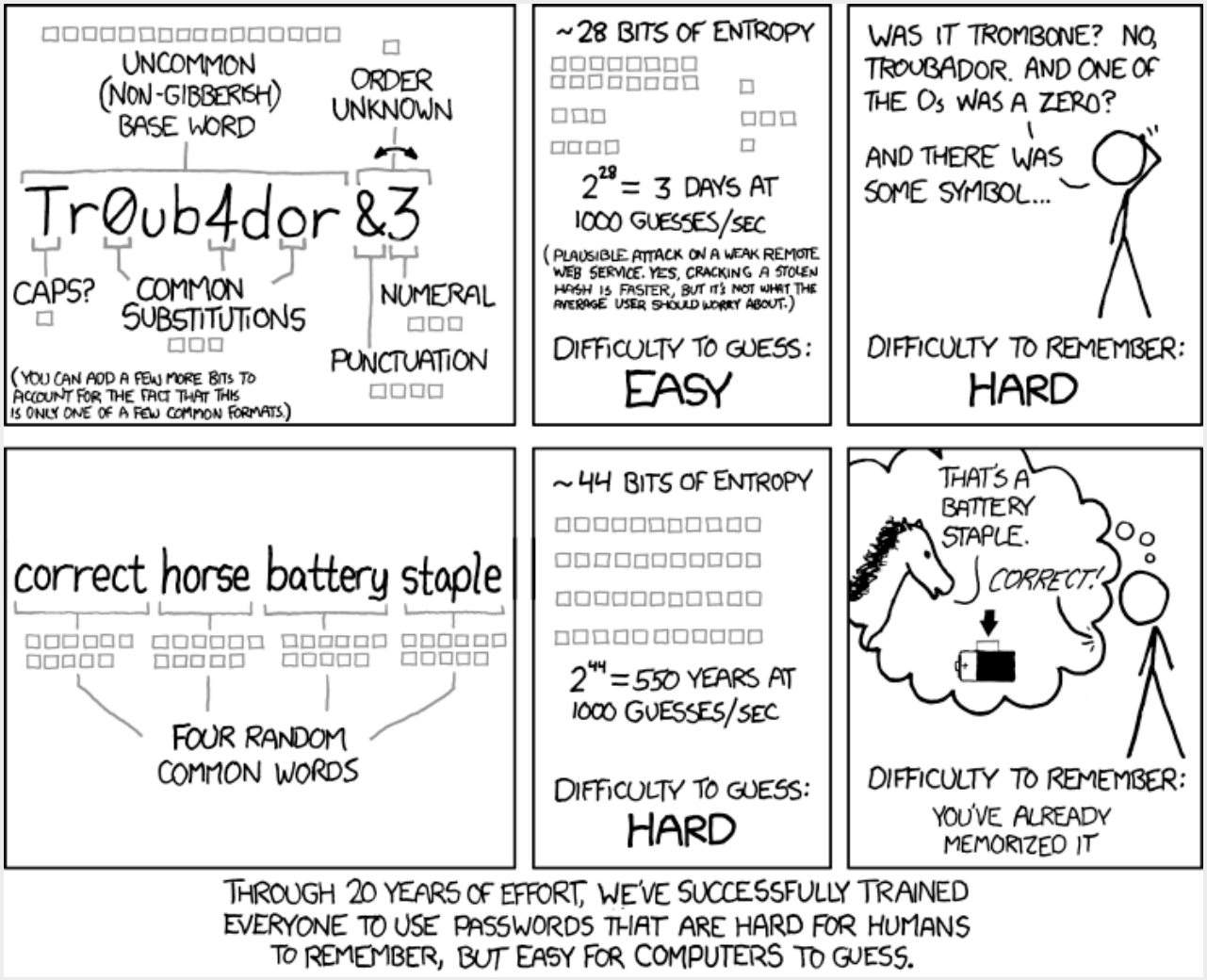
PASSWORD CRACKING

- Any 8 character password is cracked in 2.5 hours. (8x 2080Ti GPUs)
- Any 9 character password is cracked in 4 days. ($2k worth of AWS)

HASHCAT


C:\Windows\System32\cmd.exe
d:\tools\hashcat-6.0.0>hashcat64 -b -m 1000 -u 1024 -n 512 --opencl-vector-width 8 --force -O
OpenCL Platform #1: NVIDIA Corporation
* Device #1: GeForce RTX 2080 Ti, 2816/11264 MB allocatable, 68MCU
Benchmark relevant options:
* --force
* --optimized-kernel-enable
* --opencl-vector-width=8
* --kernel-accel=512
Hashmode: 1000 - NTLM
Speed.#1.....: 102.8 GH/s (10.48ms) @ Accel:512 Loops:1024 Thr:32 Vec:8
Started: Wed Feb 13 22:57:19 2019
Stopped: Wed Feb 13 22:57:26 2019
d:\tools\hashcat-6.0.0>

LENGTH vs COMPLEXITY


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

PICK YOUR PASSWORD

- Butterfly11
- Celtics’19
- Winter2019&
- Spring2019^
- P@tri0ts19
- Jenny0101
- Debbie08@@
- P4s$w0rd1
- 08Lexus++

- ho*mEr1un
- pac1kSe9nd
- Sn<owclo>ud
- Ren5talPro4perty
- 1Narragansett9
- O$ceanBree4ze
- $muhNEE$19
- Ih8myjob19
- 3HumpDaaay#

WHAT ZERO TRUST IS

- Security model from 2010
- Assumes EVERYONE is a threat
- Networking & System & Software combined
- Micro-segmentation & Access Controls
- Identity Access Management
- Privileged Identity Management
- Multi-Factor Authentication
- User & Device validation

WHAT ZERO TRUST ISN'T

- Different than Principle of Least Privilege
- A quickly implemented, one time deployment of Off-The-Shelf software/security solutions
- A replacement of current security controls
- A solution for just n critical systems
- A solution for your weakest link

WHY SO POPULAR NOW?

- It's catchy
- It's trendy
- Vendors like to say they have it
- Vendors like to say they are needed for it

- It's necessary

A GOOD PROGRAM IS BUILT ON…

- Governance
- Security Awareness
- Well-designed networks
- Well-designed systems
- Appropriately limited access
- Active monitoring
- Effective execution
- Culture & attitude
- Periodic review & evaluation

SOME QUICK "WINS"

Zero Trust micro-segmentation	Do you allow inbound connections to your LAN? Do you allow vendor systems on your network? Do you allow workstation to workstation connections?
Zero Trust IAM	Do you require MFA for all users? All the time? Do you have strong password policies? Do you have limited access rights to all data repositories?
Zero Trust PIM	Do your admins have separate accounts for I-net & email? Are your admin rights all DA or unique to need? Do you allow service accounts to be Domain Admins? What endpoints do your admins use their access from?
Zero Trust Device Validation	Do you allow BYOD? How do you register them? Do you provide conditional access for devices? How well do you perform de-provisioning of devices?

smp

SECURITY MANAGEMENT
PARTNERS

QUESTIONS?

sales@smpone.com