

ENDSIGHT.NET

Cybersecurity Office Hours

Stephen Hicks, Security Practice Manager

Q4 2025



endsight



Stephen Hicks
**Security Practice
Manager**
CISSP, CCSP, CISM

Phone Number: (510) 280-2036

Email: shicks@end sight.net



MBA from St. Mary's University.



Over 25 years in IT (over a decade in
Cybersecurity).

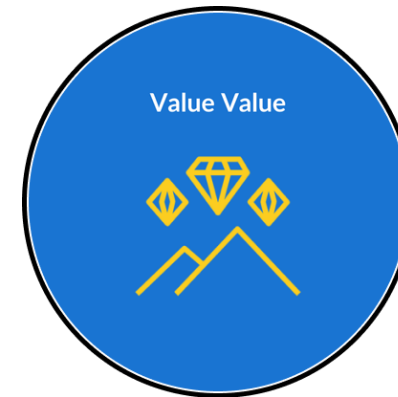
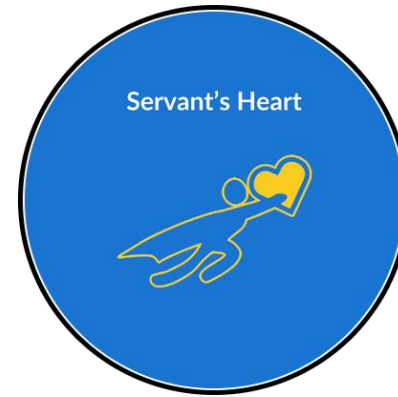
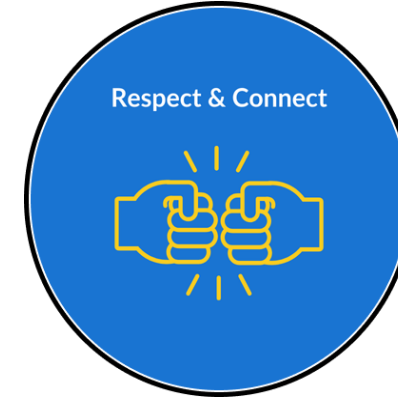
Majority of career working with SMBs.



Over a dozen technical certificates.

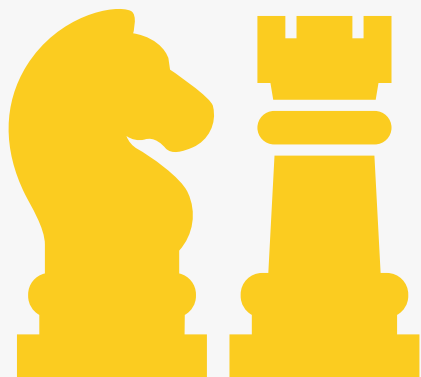
**We live in the darkness, ”
so you don't have to.**

ABOUT



WHAT THIS IS INTENDED TO BE

High level,
strategic discussion



Suitable for
C-Suite



Not tactical,
not user focused



Agenda

01 Security and IoT

02 Fake Astronauts (and scams)

03 SonicWALL

04 VPNs vs ZTNA

The “S” in IoT

- What is IoT?
 - The Internet of Things



- Typically not incredibly secure
- Wait, they're serving ads now?
 - Samsung Smart Fridge Ads
 - <https://www.theverge.com/news/780757/samsung-brings-ads-to-us-fridges>
- A story about casinos and fish (not Phish)
 - <https://www.securityweek.com/hacked-smart-fish-tank-exfiltrated-data-rare-external-destination/>

The “S” in IoT stands for “Security”

- Important to be careful what we connect to the Internet
 - *Yes, this is in fundamentals training too*
- Home devices were the cause of two major hacks at Lastpass
 - *Both were Plex*
- Corporate devices have similar vulnerabilities.
 - **Reminder** – don’t connect anything to the Internet you don’t need connected to the Internet

Fake Astronauts (and scams)



- Seriously. Fake Astronauts.
 - <https://www.cbsnews.com/news/woman-romance-scam-fake-astronaut-distress-japan/>
 - A woman in Japan was convinced to send money to 'buy oxygen' because the astronaut was 'under attack'.
- This is unfortunate (and silly) but it does lead to an important point –
 - Scams are the major form of all compromises today.
 - Users need training; people fall for obvious scams commonly
- Endsight has several clients send us emails regularly with obvious scams and phishing asking if they are accurate.
 - This includes leadership. Training is paramount.
 - For further interesting reading: <https://www.reddit.com/r/scams> has a modern repository of concerns and current scams people fall for.

SonicWALL



It's been a **bad year** for SonicWALL

- At least one SSLVPN breach, possibly two.
- Two attacks on cloud backups.



This isn't the **only vendor**, however:

- Cisco had a flaw on 10/15/25
- Ivanti had one in Dec 2024
- Fortinet had one in January
- Since we spoke last, Endsight has had *seven (7)* SSL VPN related breaches, and we're doing something about it.

VPNs and ZTNA



Endsight is actively following SonicWALL guidance (and you should have received our communications so far), but...



... SSLVPN is just no longer safe.

Why? – The design



A primer on SSLVPN Design (and a video to share)

<https://www.endsight.net/security-shorts/vpn-breach-warning> (Link will be on the recording page)



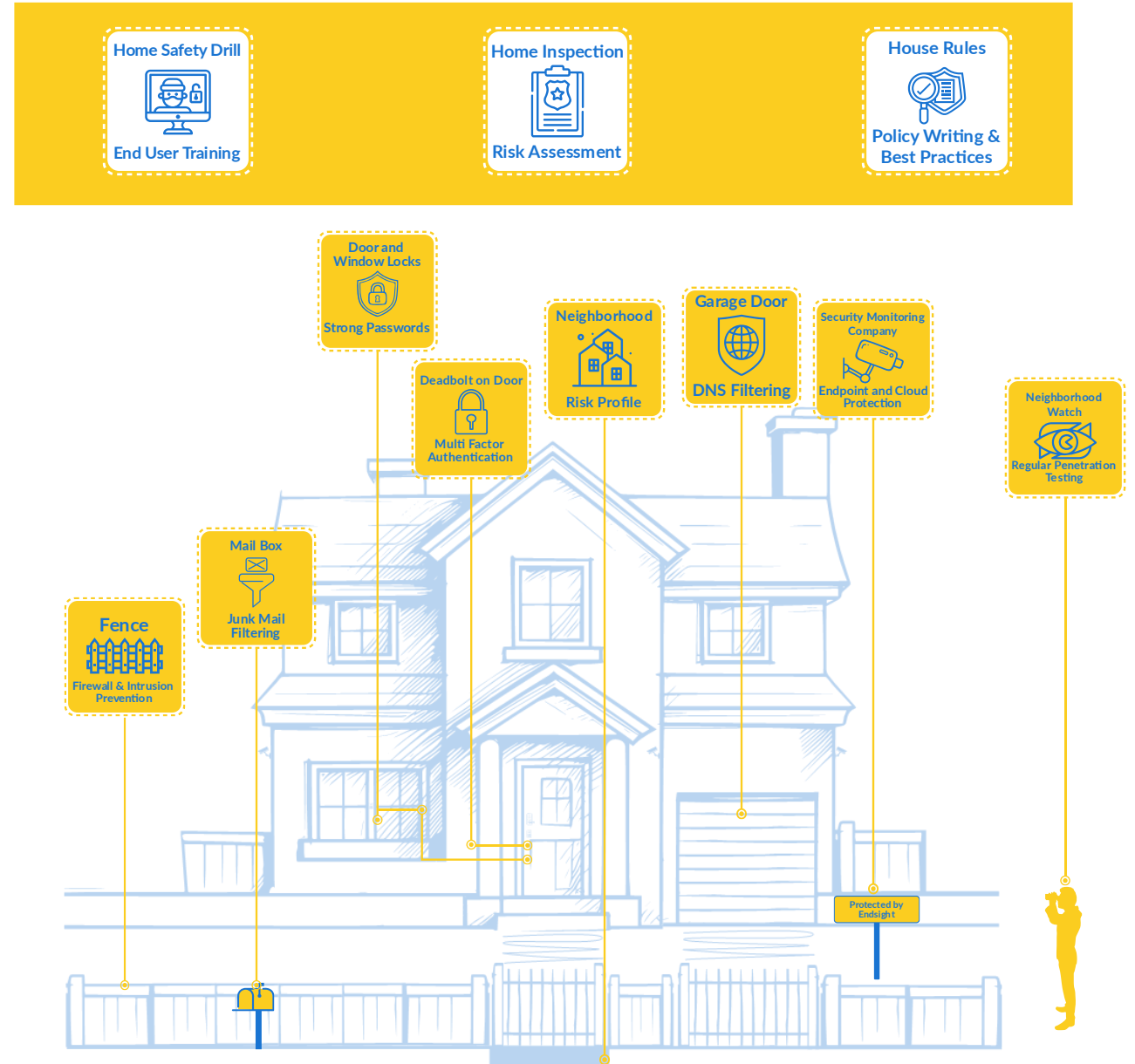
The **risk** is inherent in SSL VPN design, not a specific **product** or **manufacturer**.

Summary

- IoT has little security baked in
- Astronauts and scams
- SonicWALL and changes
- VPN/ZTNA

Defense in Depth

(People, Process, Technology)



Is Your House in Order?

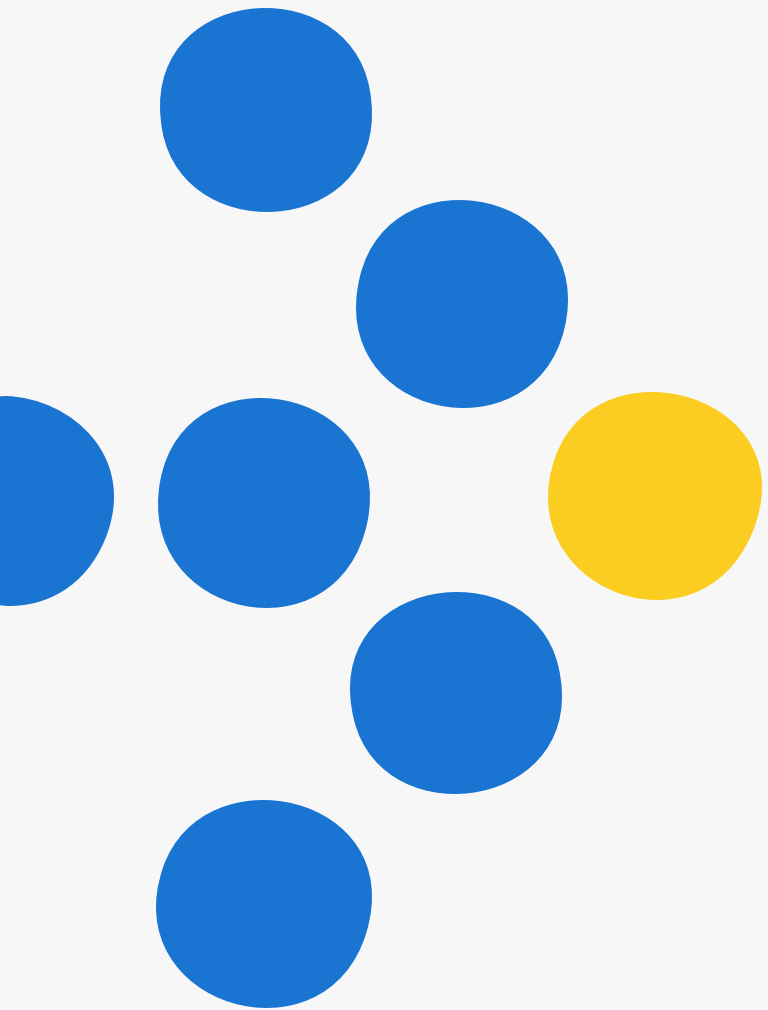


Next Session

- January 29th @ 1 PM
- Topic: I have absolutely no idea. (But I bet it'll be interesting) – Stay tuned.
- To register:
 - Scan the barcode
- Go to: <https://get.endsight.net/cybersecurity/office/hours>
 - Email akreps@endsight.net to register
 - Answer "Yes" in the poll.
 - We can also auto register you for the remaining 2025 sessions
-

AI Office Hours

- December 11th @ 1 PM PST.
- Similar format to Security Office Hours, but with some training.
- To register:
 - Scan the barcode
 - Go to: <https://www.endsight.net/development/webinar>
 - Email akreps@endsight.net to register
 - Answer "Yes" in the poll.



Q&A

Q&A

- I received a call from my bank's fraud department. While on the phone with them I looked up the phone number and it was their Fraud department. I was cut off and I recalled the no. It was their fraud department, but the lady I spoke with looked at my file and said they didn't call me. Good thing I was cut off. How do you protect yourself from something like this?
- How can we prevent credit card companies and other vendors from utilizing our voice for authentication? What are scammers doing to capture your voice to utilize as a part of a broader scam? I am seeing a huge uptick in scam calls.
- What is your first pet's name?



Stephen Hicks
CISSP, CCSP, CISM
Security Practice Manager @
Endsight

Thank you!

