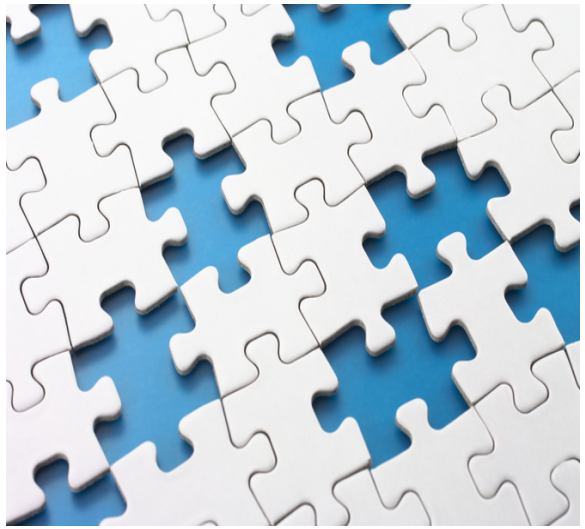
TLS 1.3 Impact to Enterprise Security

John Banghart
Center for Cybersecurity Policy and Law

CENTER FOR CYBERSECURITY
POLICY AND LAW

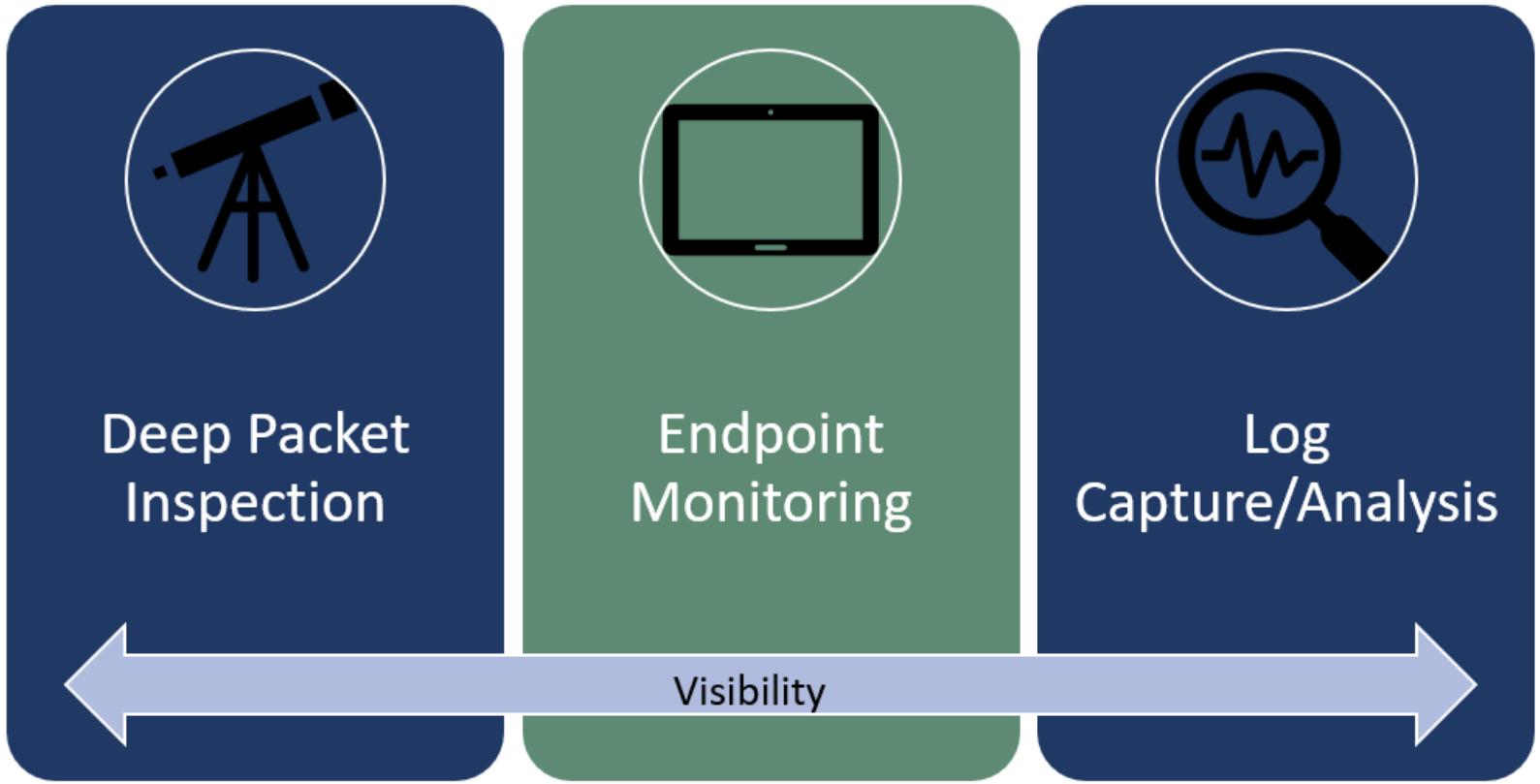
Just to be clear…



CENTER FOR CYBERSECURITY
POLICY AND LAW

What's the Problem

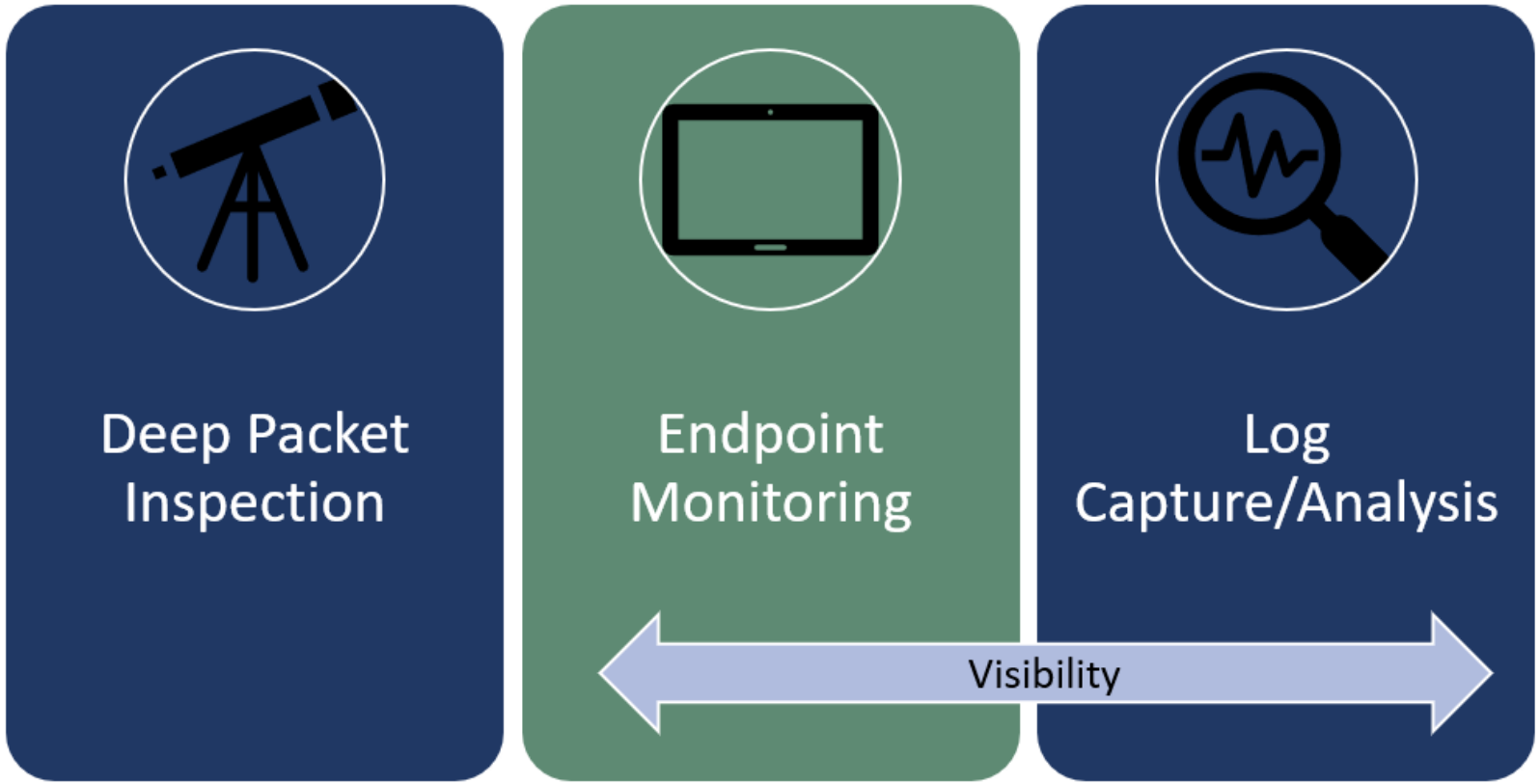
Enterprise security relies on visibility



CENTER FOR CYBERSECURITY POLICY AND LAW

TLS 1.3 Impacts Visibility

In simple terms:



Sure, but…

"TLS 1.3 isn't used everywhere, nor does it have to be."

- That's fair, but encryption of data in transit is a near universal requirement and older versions won't be supported forever.

"Endpoint monitoring combined with robust log capture and analysis seems like enough"

- Well, let's take a closer look at all three.

Endpoint Monitoring

Positive:

- Can provide direct insight into host activity
- Provides control capabilities for defenders and responders

Negative:

- Compromised platform can disguise its behavior
- Agent access can vary widely; many devices may not have agents at all (e.g. IoT, BYOD)

Log Capture/Analysis

Positive

- Lots of device support
- Tools for processing an analyzing are improving

Negative

- Volume and velocity increases rapidly with the proliferation of devices
- Still prone to human error
- Logs are frequently disabled at the start of an attack or modified/deleted at the end
- Logging is often not enabled (due to human error) or set at too low a level to save resources, because
- Log data takes space, space takes money; logs can be a significant business cost.

Deep Packet Inspection

Positive

- Identify/prevent malicious activity on the network, especially lateral movement
- Detect data breaches quickly

Negative

- DPI devices add to the attack surface
- Can’t see much of what goes inside the host

What I’m Saying Is

- None of these capabilities are perfect
- They all provide visibility in their own ways
- Removing one of them creates blind spots

Why This Matters

Loss of DPI creates a gap in the overall visibility picture negatively impacting:

- Detection of malicious actor movement/activity
- Detection of data exfiltration and command and control channels.

Which in turn negatively impacts:

- Preventative detection
- Incident response
- Forensic investigation

Finally

Security and privacy requirements differ between the public internet and enterprise environments.

Enterprises frequently have legal, regulatory, and contractual obligations to protect data in their care by all means possible.

Taking a capability out of the mix and hoping that other existing solutions can pick up the slack isn't realistic.

Enterprises need a solution that does not diminish their ability to protect the information in their care.

Thank You

John Banghart
Center for Cybersecurity Policy and Law

https://centerforcybersecuritypolicy.org/enterprise-data-center-transparency-and-security-initiative

CENTER FOR CYBERSECURITY
POLICY AND LAW