Going Dark Analysis and Preparations
Analysis and Preparation

Kathleen M Moriarty
Chief Technology Officer, Center for Internet Security

March 3, 2022

Fundamental Shifts in Management

Network Protocol Stack Evolution, Pervasive Encryption, and Zero Trust

- **Encrypted HTTP traffic 30% in 2013 - > 80% in 2022**
  - All Mozilla users, Let's Encrypt Statistics
- **Increased use of QUIC, where the performance gain has a significant impact**
  - HTTP traffic, DNS core infrastructure
  - Leaves only the spin bit visible for performance monitoring
- **Zero Trust Architecture**
  - Pervasive use of encryption within applications, not just the network
  - Dynamic authentication of identities and components limit survivability of attackers on systems and networks
  - Dynamic verification of software, workloads, and hardware are as expected (i.e. allow lists)
  - Log everything!

RFC8404: Effects of Pervasive Encryption on Operators

- **Internet Service Provider Level**
  - Network operators rely primarily on TCP and IP headers
  - Minimal impact by use of TLSv1.3 on Internet level traffic
  - Performance metrics use dedicated packets at service provider level
  - Content Delivery Networks shift to End-to-end only
  - Lawful Intercept or Exceptional Access capabilities limited
- **Organization Level**
  - Intrusion detection and prevention moves to the endpoint
  - Zero Trust shifts endpoint protection to allow-list approaches in time
  - Use and value of indicators of compromise or known bad information declines in value

Transforming Information Security

Optimizing Five Concurrent Trends to Reduce Resource Drain

Validated and Trusted Assurance with Architectural Patterns that Scale

What Changes?

Shift Requires Assessment and Planning to Support Expected Service Levels

Service	Impact
Network Monitoring	IPv6 and Overlay protocols for Organizations, specialized measurement protocols for service providers
Intrusion Prevention	Based on allow lists at endpoint
Internet Core Service, e.g. DNS, SMTP, XMMP/MLS	Resolvers become the sole point of exposure, unless end-to-end is encryption applied
Content Delivery Services	End-to-end, caching capability eliminated

Thank You