Protecting Customer from Themselves
Cyber Crimes are on the Rise!

- **$3.92 M**: Average cost of a Data Breach
- **650%**: Increase in Trojan-based malware threats
- **90%**: Breaches caused by Phishing

Sources: Ponemon Institute | HIPAA Journal | Retruster
The Impact of Security Breaches

- Ransom
- Lost revenue
- Brand damage
- Regulatory fines
- Investigation costs
- Lawsuits

Data Breaches are a global problem

Source: Bleeping Computer
The Menace of Ransomware
Internal Threat Actors aren’t always aware of the damage they’re causing
What is an Internal Threat Actor?

Any User within the Trusted Internal Network who has legitimate access to resources

1. Has conscious intent to cause harm
   - Malicious insider or An imposter who technically is an outsider
2. Has no conscious intention of causing harm
   - Careless or negligent insider
Example – Malicious Insider

• Anthem’s Data Breach - Employee Data Exfiltration

• Employee had been stealing and misusing Medicaid member data for almost a year
  – Emailed files containing Anthem member data to personal email account
  – Included information like Medicare ID, SSN, Health Plan ID, names, dates of enrollment etc.

Source: Observit
Example – Negligent Insider

• Lake City, Florida Ransomware Attack
  – City employee downloaded infected file via email
  – Multi-staged attack which included:
    • Emotet Trojan which started the attack & downloaded,
    • TrickBot Trojan which downloaded and installed,
    • Ryuk Ransomware which encrypted critical files
  – City paid a ransom of 42 bitcoins ($500,000)

Example – Phishing Attacks

• RSA’s Breach
• Employees fell for a targeted phishing attack
• Multiple hacker groups involved
  – Pretended to be trusted co-workers and contacts
• Led to a successful Advanced Persistent Threat (APT) attack
  – 40 million employee records were compromised

Source: Observit
Example – Ransomware Attacks

• Riviera Beach, Florida Ransomware Attack
  – Employee of Police Department opened an infected email
  – Infected computers across the city’s network
  – City government held a vote and paid a hefty ransom of 65 bitcoins ($600,000)

Attackers are Challenging and Outsmartering Traditional Security Practices
Zero Trust Solves These Security Issues

• Conceptual model driving architectural changes
  – The concept has been around for long
  – Vendors and customers finally implementing the model
  – Demands major architectural changes

• Visibility is key
  – Visibility into users, data, workflows etc.
Zero Trust Solves These Security Issues

• “Trust Nobody”
  – Microsegment network perimeters
  – Limit excessive user privileges
  – Enable compliance
  – Avoid solutions that don’t support diverse integrations
  – Improve security detection and response with centralized visibility & control
  – Avoid solutions that are too complex to deploy and use
Zero Trust Implementation Will Take Time

Meanwhile, We Need a Solution for the Problems of Today
Encryption Introduces New Challenges
>80% of Internet Traffic is Encrypted
Encryption gives you **Privacy**

But it hurts your **Security**
You Cannot Defend Against Threats You Cannot See
Encryption Makes Defenses Ineffective

**Infiltration**
- Intrusion Prevention System (IPS)
- Firewall
- Secure Web Gateway (SWG)
- Anti Virus System

**Command and Control**
- Advanced Threat Protection (ATP)
- Anti Malware System
- Sandbox

**Exfiltration**
- Data Loss Prevention System (DLP)
- Forensics

---

*The Cyber Attack Continuum*
The Zero Trust Model Will Fail Without Decryption Because Visibility is Key
Decryption is operationally challenging
And Expensive
The “DNS over HTTPS” Problem

- DNS used to be unencrypted
- Security via DNS Filtering was effective
- DNS inspection Created privacy concerns
  - Companies tracking/selling user data
- DNS over HTTPS (DoH) enables DNS traffic encryption
  - Users now susceptible to encrypted attacks hiding in DoH traffic
  - Security enforcement via DNS is no longer an option
Emerging TLS-1.3 Standard

• New Encryption Standard
• Aims to enhance efficiency, user privacy & user data security
• Requires costly upgrades to implement
• TLS 1.3 decryption may see a slow adoption rate
How do we solve the problems of **today**

While enabling the Zero Trust model for a more secure **tomorrow**?
Dedicated and Centralized Decryption
Dedicated and Centralized Decryption

- Simplified Operations
- Provides full visibility to the entire security infrastructure
- Enhances efficiency and efficacy of existing security infrastructure
- Enables the entire security infrastructure with the “Decrypt once, inspect many times” model
- Centralizes decryption, policy control, key management
Dedicated and Centralized Decryption

- Is vendor agnostic and provides flexible deployment options
- Is easy operationalize and to use
- Provides centralized visibility and analytics
- Provides centralized management capabilities
The “Secure Decrypt Zone”

Enhanced performance due to
Decryption/Re-encryption offload

Improved user experience due to
reduced latency

Centralized decryption, policy control and
key management

Encrypted Internet Traffic
Decrypted Internet Traffic
A Dedicated and Centralized Decryption Solution

Sits at the core of the Zero Trust Model
Even Better Security with Multi-Layered Security Services

- Application Firewall
- Threat Intelligence
- URL & Web Filtering
- Traffic Steering
- Threat Investigator
- User ID Based Traffic Filtering
Thank You