FORRESTER®

Endpoint Security For Remote Scenarios

Chris Sherman

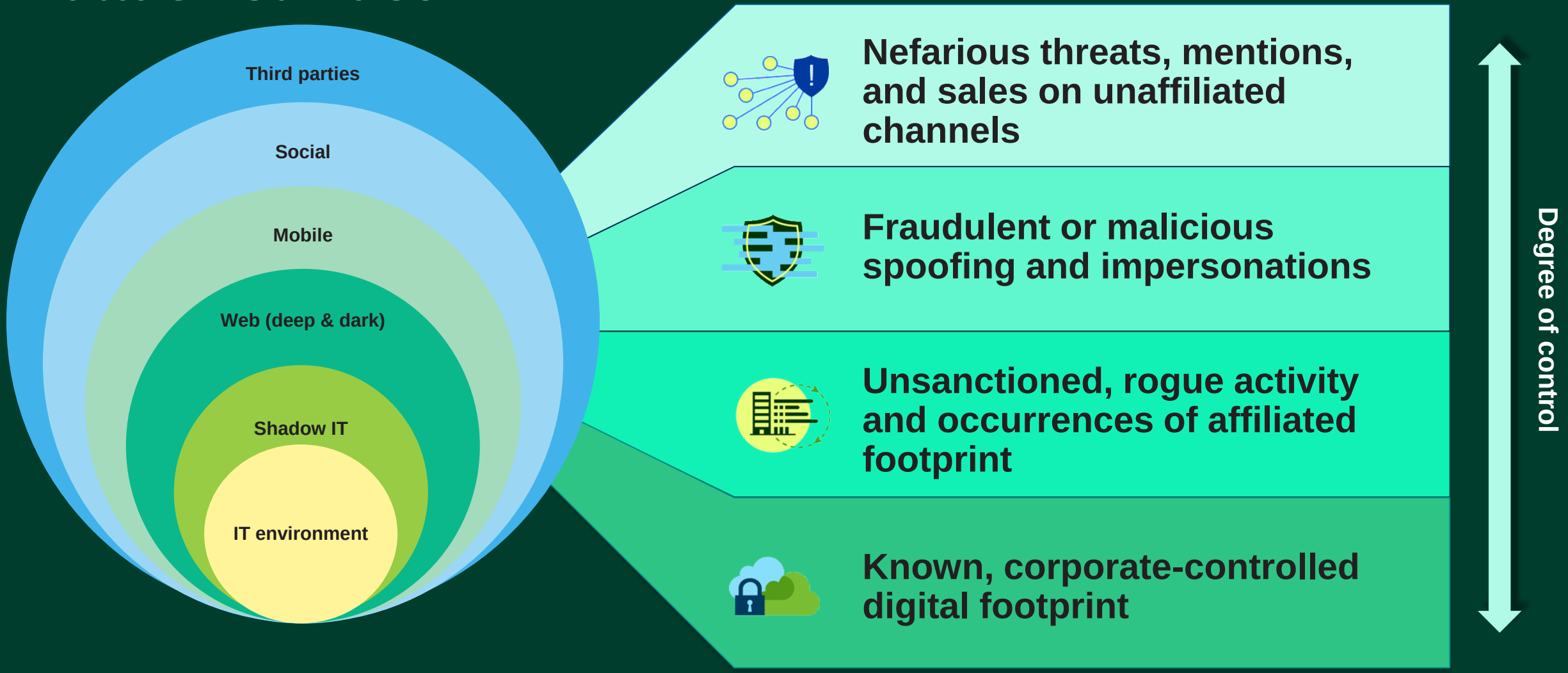
Senior Analyst

May 28th, 2020

Cyberattacks are a board-level concern

- Security is shifting from a director/VP/CISO problem to a CEO problem
- Data protection is a key concern
- The attack surface is expanding
  - Mobile and IoT are presenting new challenges
  - BYOD/user-owned devices are here to stay

You are dealing with a rapidly expanding attack surface



Data breaches are commonplace

- 56% of enterprise respondents say they suffered at least one breach last year
- 23% of breaches are due to insiders
  - 44% were malicious in their intent

Base: 217-784 Security decision-makers with network, data center, app security, or security ops responsibilities

Source: Business Technographics Global Security Survey, 2019

Why don’t “perimeter only” models work anymore?

- Networks are broadly laid out – easy to find blind spots
- Data is mobile – perimeters are nonexistent
- Remote work increases chance of theft and/or loss
- Trust occurs, but verify is not followed up on
- Malicious insiders pose additional challenges

Agent proliferation adds to the complexity and expense

The average enterprise has more than six agents per endpoint.

Source: Forrester's Proprietary Survey, 2017

Endpoint Security Suites And UEM Are Converging

What are your firm's plans to adopt the following PC and mobile technologies? Implementing/implemented + Expanding/upgrading implementation (4 5)

Base: 505 Infrastructure technology decision-makers (1,000+ employees)
Source: Forrester Business Technographics Global Infrastructure Survey, 2019

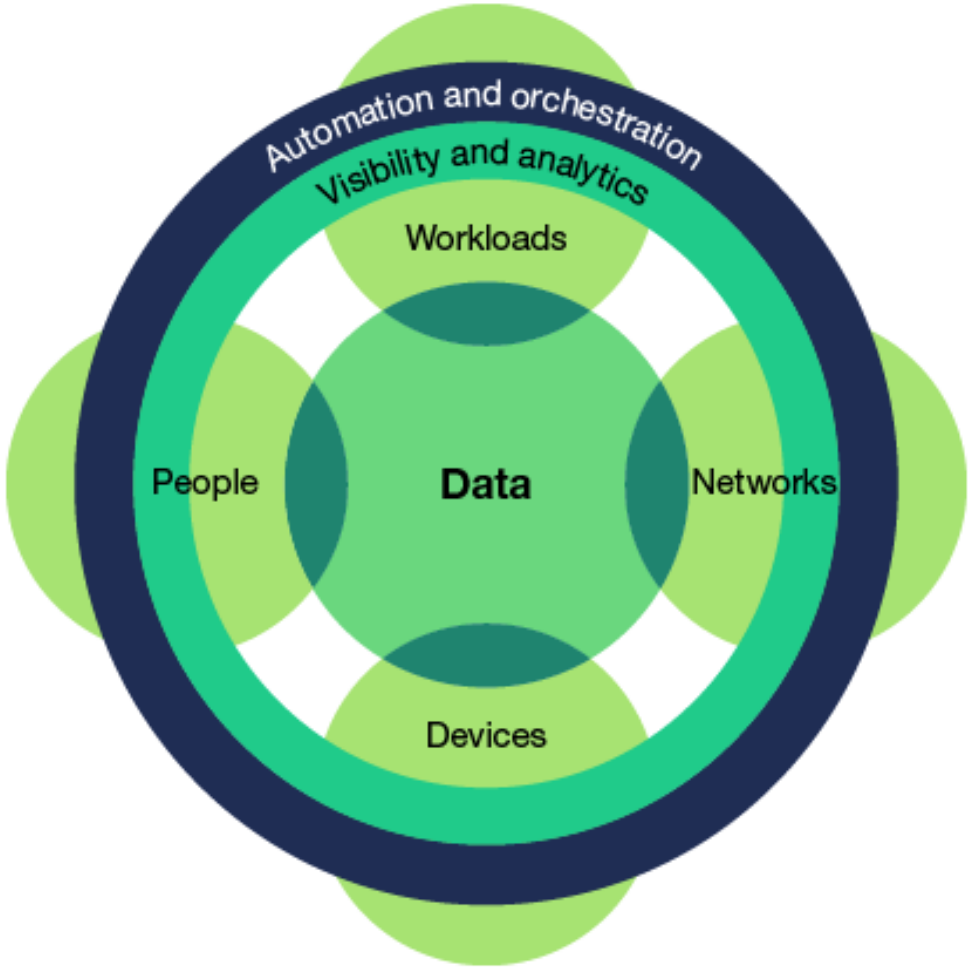
Why an integrated Security/IT approach is needed

- Reduces friction between the two teams
- Stops malware propagation
- Improves visibility throughout the network and reduces time to breach detection
- Increases data awareness
- Stops the exfiltration of toxic data into the hands of malicious actors
- Reduces both capital and operational expenditures on security
- Reduces security agent fatigue

Poll Question

“How would you rate the level of integration between your security and IT management tools?

Use Forrester's Zero Trust framework to guide your integration strategy



Technology requirements for the Zero Trust framework

- Must easily integrate with current security tooling
- Deploy quickly with little or no additional tech
- Work with any device, any browser, mobile or not
- Multiple isolation levels, aligned with device/network/user/data risk
- Preserve native user experience
- Stop phishing and web-based attacks
- Enable forensics

ZT use case #1: Enterprise data theft from personal device

ZT use case #2: Phishing

Recommendations

- Embrace the positive security model through on-device segmentation of sensitive data, apps, and hardware
- Identify and enforce isolation levels based on real-time risk
- Track risk levels associated with device configuration and mobile behavior
- Correlate data, network, and user behavior telemetry for context/improved risk identification and coordinated control

Thank You.

Chris Sherman
Senior Analyst

617.613.6082
csherman@forrester.com