ZERO-TRUST SECURITY

Presentation by Srimoyee Dutta
Third Year Computer Engineering

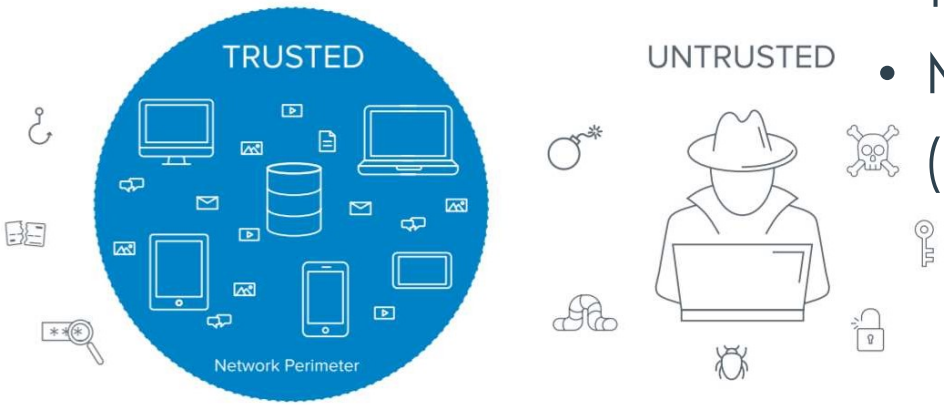
Today's Presentation

DISCUSSION POINTS

- Traditional Security and its drawbacks
- Zero trust architecture
- Why Zero trust is necessary
- Benefits of Zero trust
- Disadvantages of Zero trust
- Implementing Zero trust model

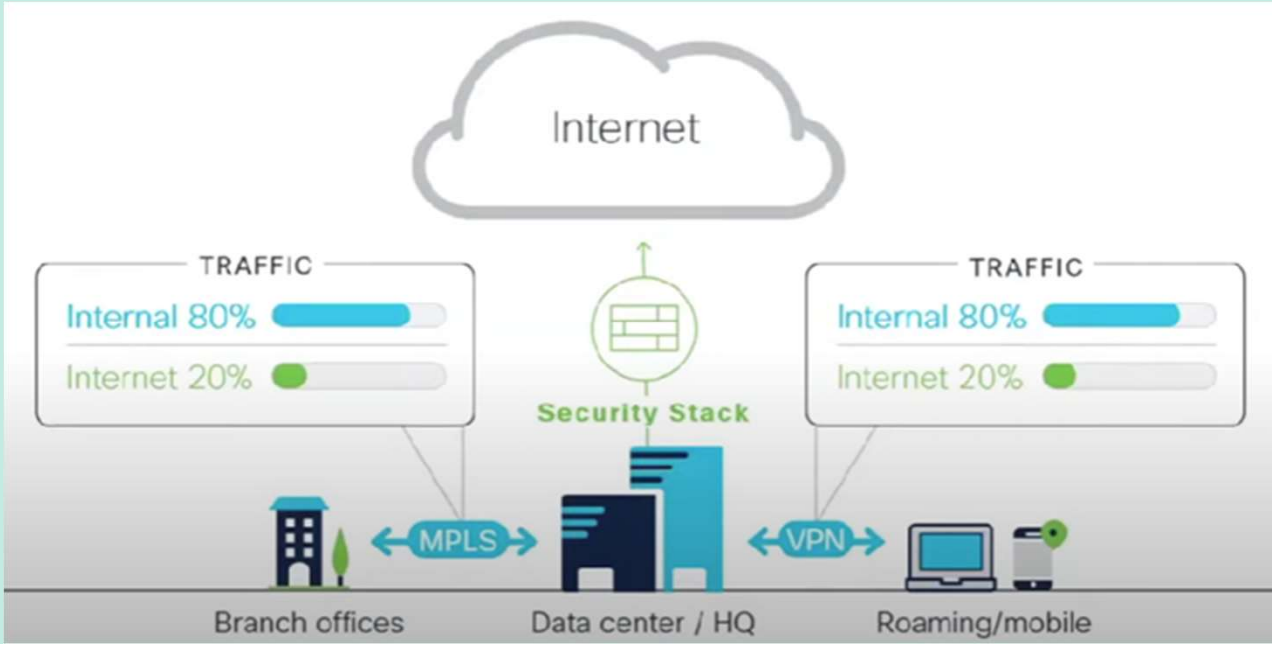
Traditional (Castle-Moat) Security

- Perimeter based Networks
- Assumes all systems and users inside the perimeter can be trusted
- Attacker can compromise single endpoint within trusted boundary and quickly expand their foothold through the entire network
- Not able to accommodate modern work styles (such as BYOD, work-from-home, etc.)



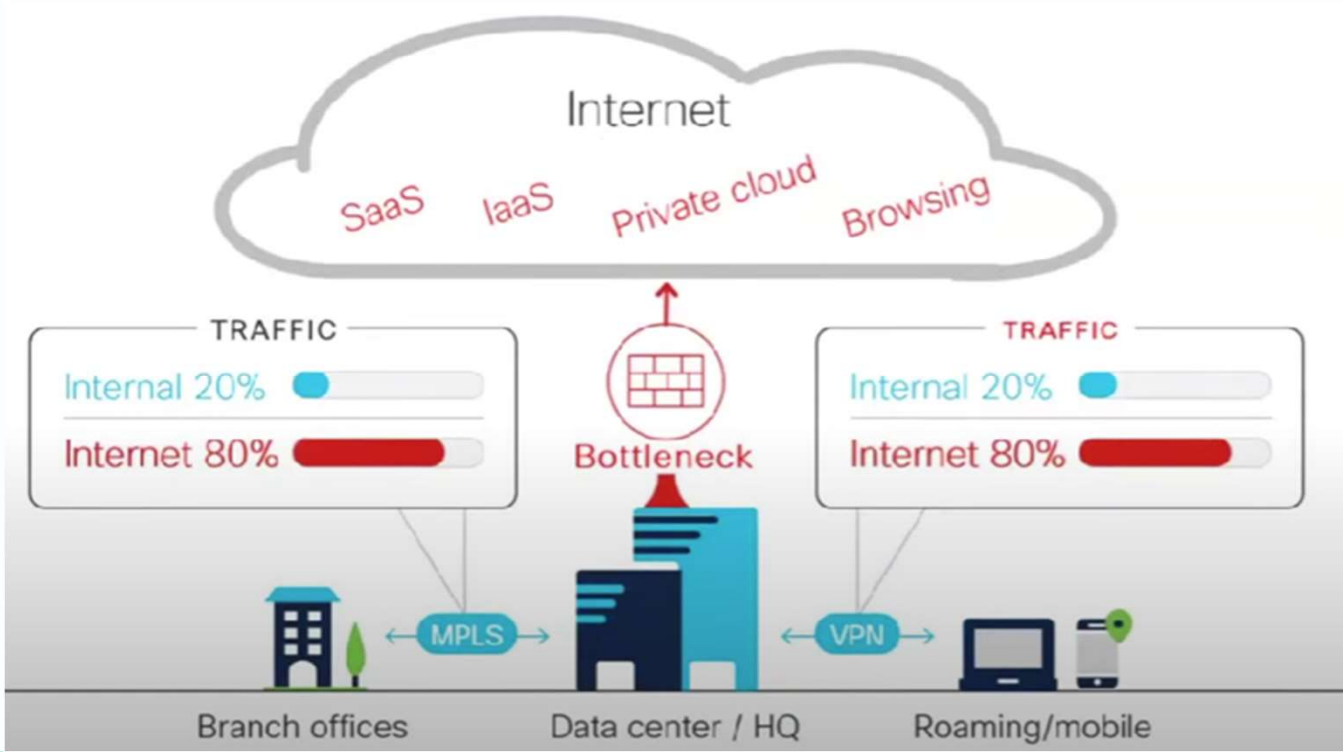
Centralized Security

- Most traffic was internal
- Internet was used for browsing/light traffic
- Most of the work was done at office, inside the defined trusted network perimeter.

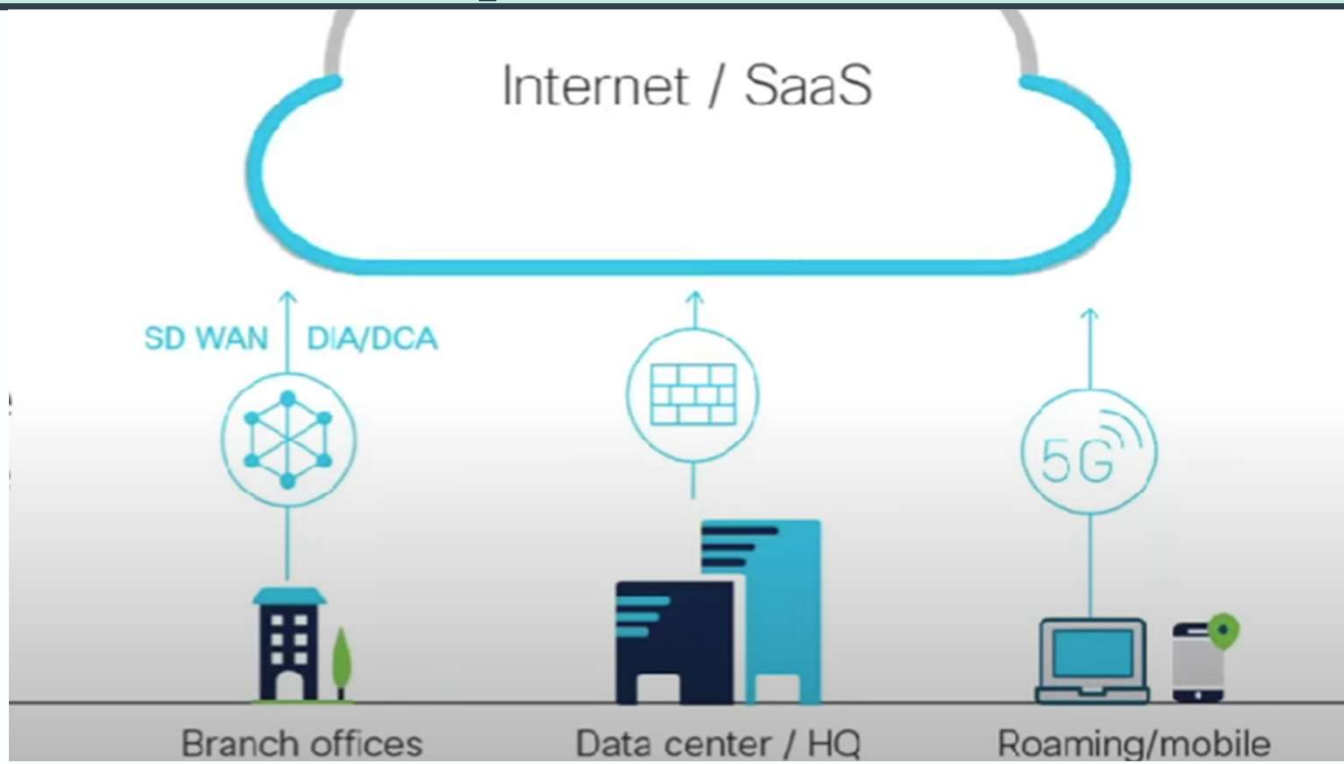


Drawbacks of Centralized System

- Costly
- Low Performance
- More No. of tools needed
- More Integrations
- High Maintenance

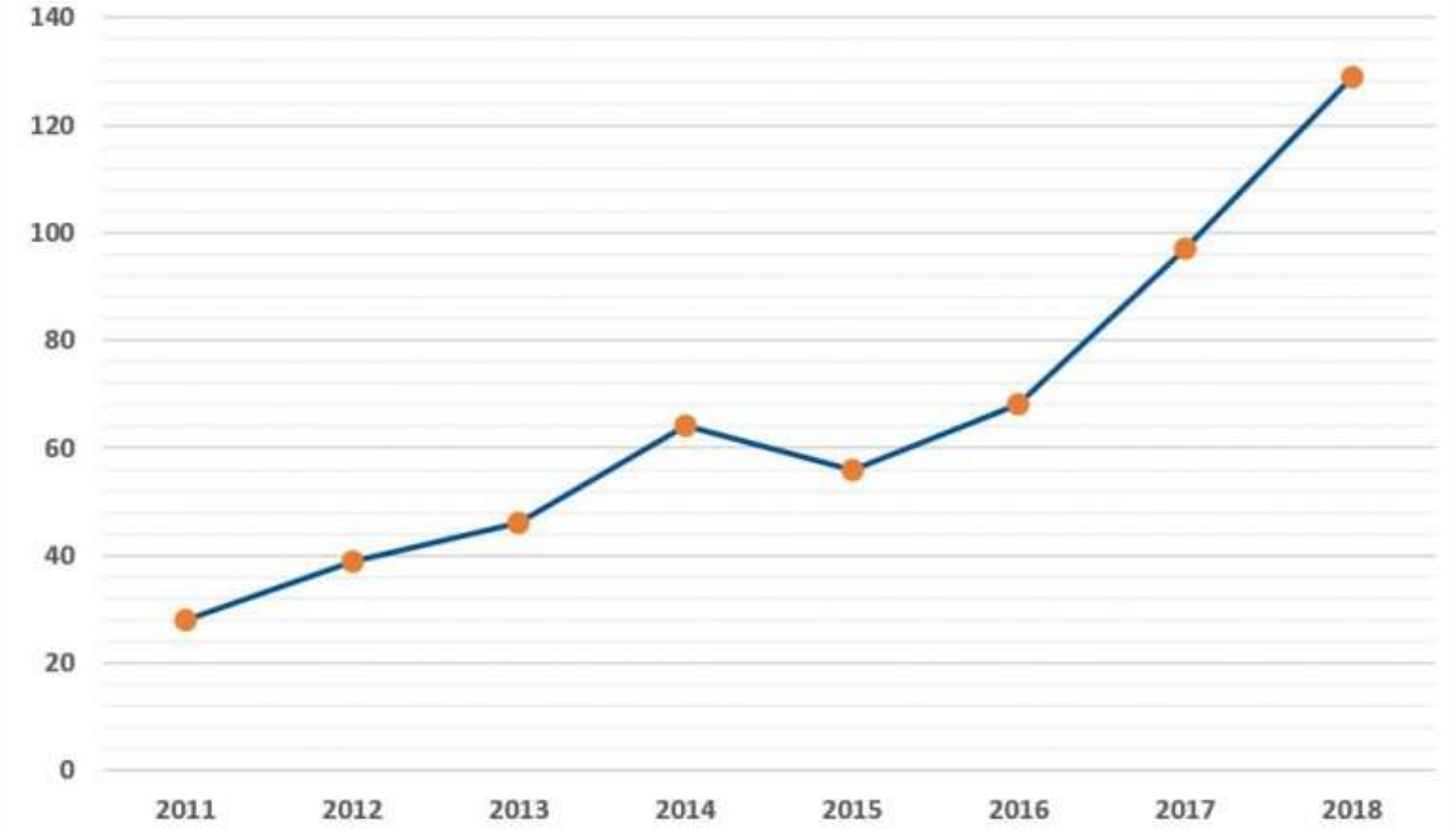


Decentralized System



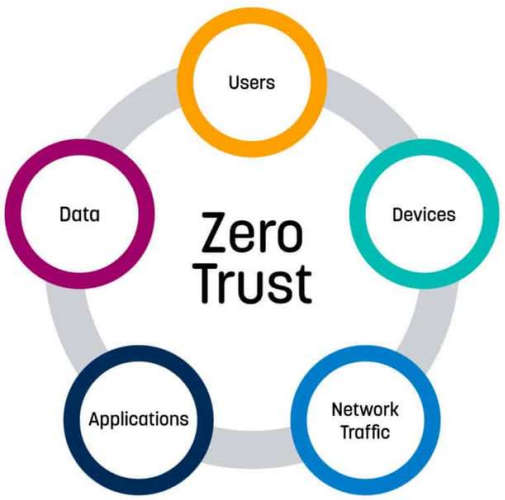
- Direct Internet Access
- Better Performance
- Not much Maintenance
- Less expensive compared to Centralized Security System

Number of Cybersecurity Breaches Disclosed per Year



WHAT IS ZERO TRUST?

It means that we do not blindly trust any device/user, unless they have proven they are trustworthy. The zero trust security model ensures data and resources are inaccessible by default.



- Assumes hostile environment
- Doesn't distinguish between internal and external
- Prevents/Restricts Lateral Movement

Zero Trust

UNTRUSTED TRAFFIC

IDENTITY BASED SEGMENTATION

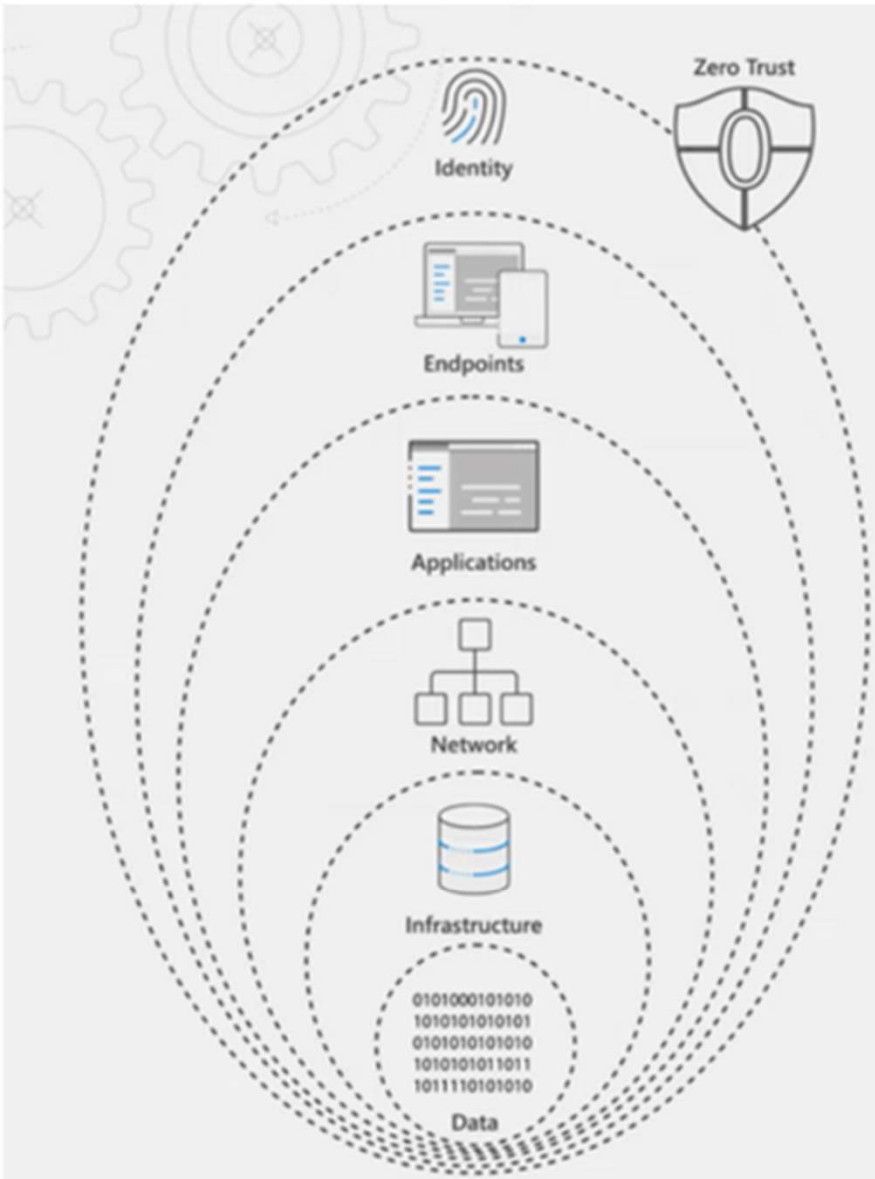
MICRO-SEGMENTATION

LEAST PRIVILEGE ACCESS

ASSESS TRUST DYNAMICALLY

ASSESS TRUST THE SAME WAY

Principles of Zero-Trust



Verify explicitly

Apply least privileged access

Assume breach

Why Zero Trust?

- Perimeter-Based Security is Ineffective in the Evolving Enterprise
- Cloud Data Centers Require Shared Security Responsibility
- Third-Party SaaS and PaaS Applications Can't Be Trusted Blindly
- The Internet Network is an Unsecured Network
- Everyone in the Expanding Workforce Shouldn't Have All-Access
- You Cannot Verify the Security Status of All WFH Environments
- BYOD is Not as Secure as Work Devices
- Cyberattacks Are Increasing
- Advanced Persistent Threats (APTs) Are Becoming More Sophisticated
- The Security Stakes Are Higher

Benefits of Zero Trust

1. GAIN GREATER VISIBILITY
2. PREVENTS DATA BREACHES
3. OPTIMIZING SECURITY STAFF
4. SECURE REMOTE WORKFORCE

Drawbacks of Zero Trust

TAKES TIME AND EFFORT TO SET UP

1. DIFFERENT WAYS TO STORE AND ACCESS DATA

2.MORE DEVICES TO MANAGE

3.INCREASED MANAGEMENT OF VARIED USERS

4.MORE COMPLICATED APPLICATION MANAGEMENT

Ways to Implement Zero Trust

- Visualize the environment
- Define zero trust zones
- Create policies
- Observe traffic between zero trust zones
- Enforce the security policies
- Monitor and refine the zero trust zones and policies

THANK YOU