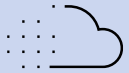
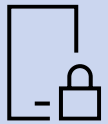
Microsoft Security

Enhancing Cyber Security

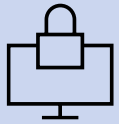
Agenda



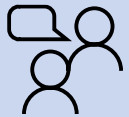
Growing Digital Landscape



Cyber Attack Trends

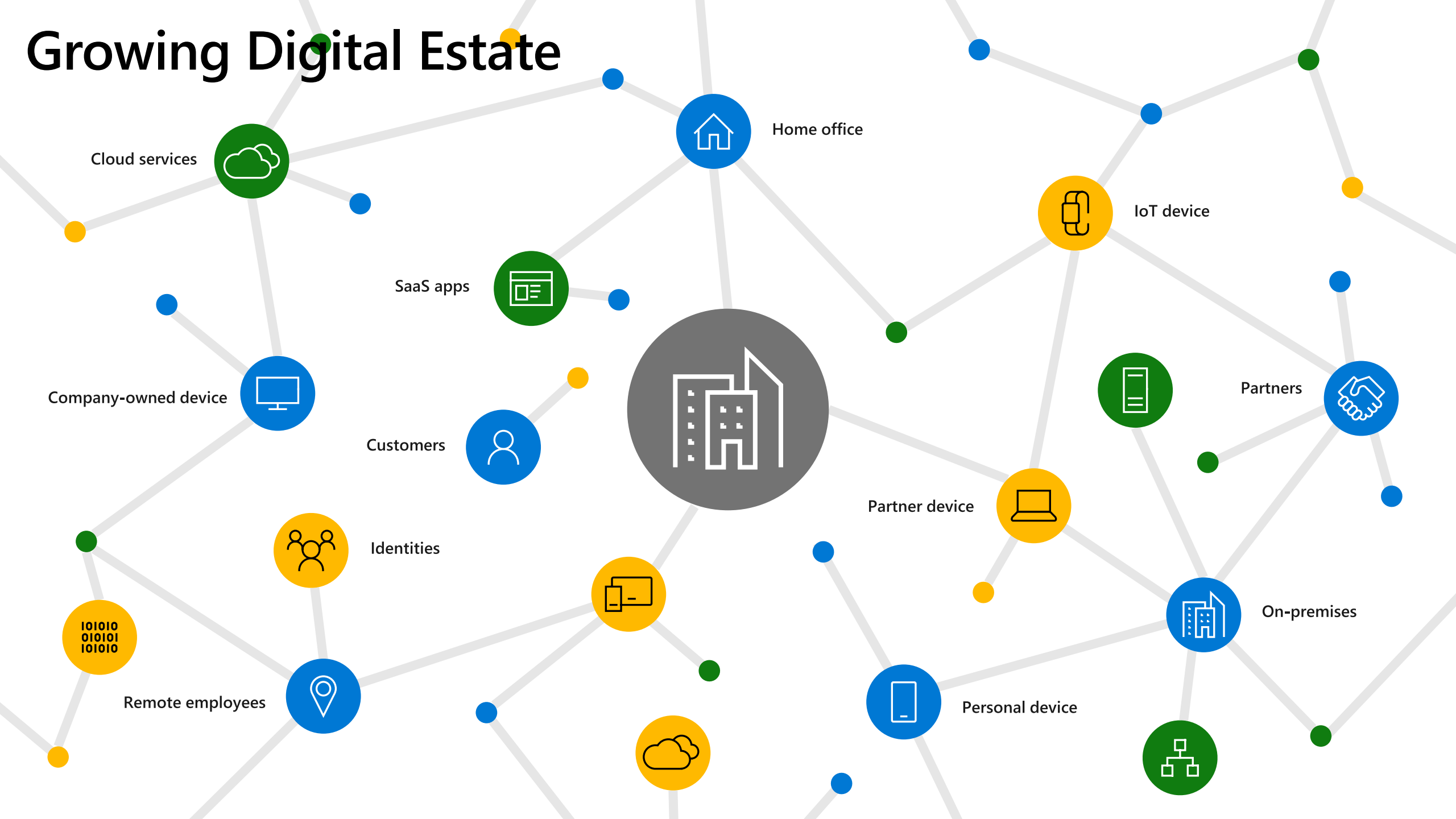


Zero Trust Approach to Security



Summary & Discussions

Growing Digital Estate

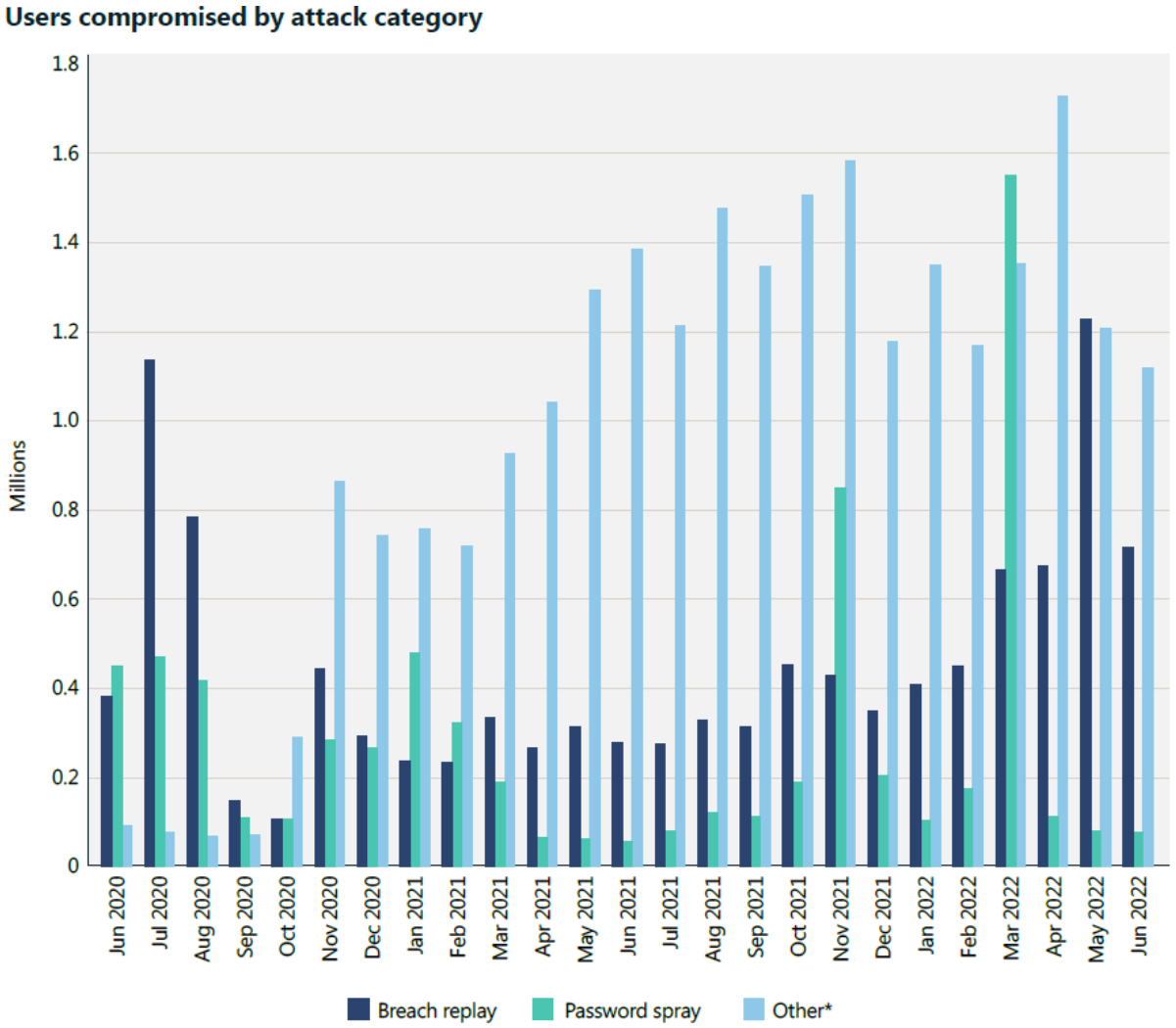


Identity compromise #1 reason for most breaches

1,287 password attacks every second

73% of passwords used are duplicates

98% impacted organizations had too many admin accounts

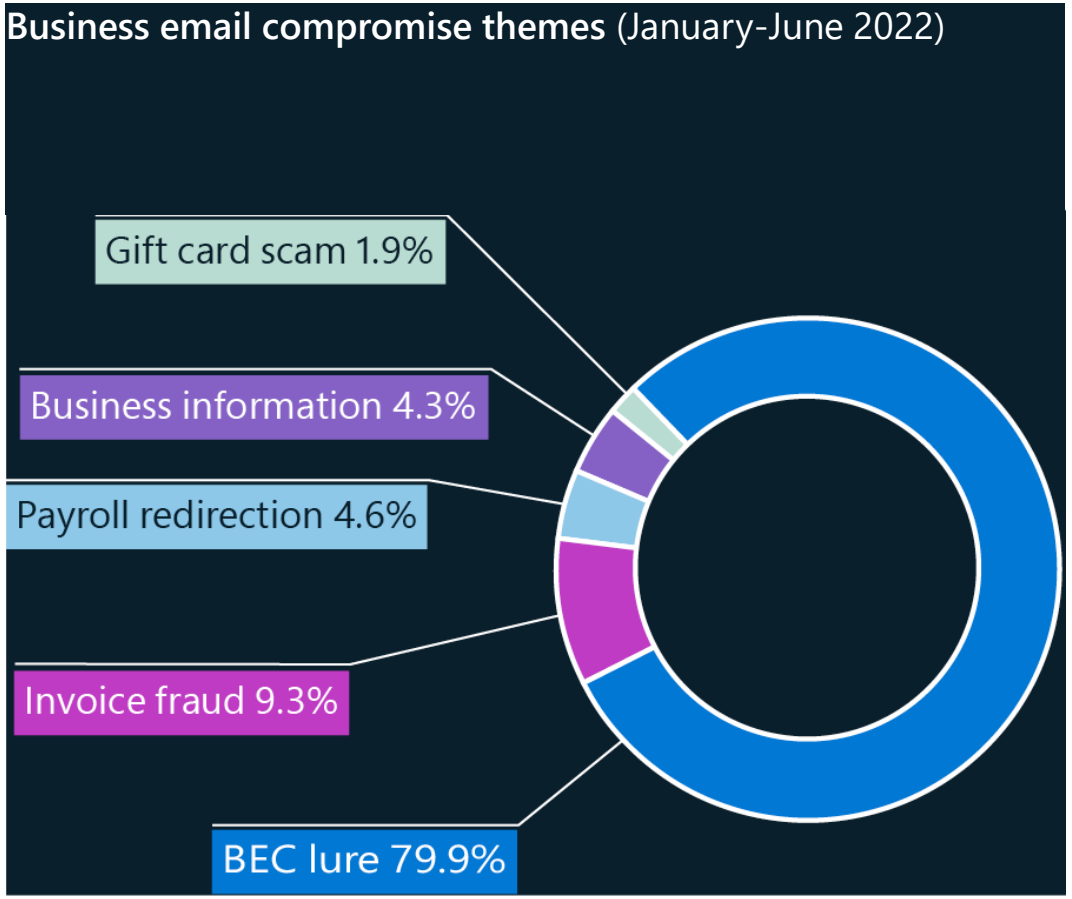


9 of 10 intrusions begin with email

710 million phishing attacks per week

72 minutes to access your private data if you fall victim to a phishing

Impersonation attacks using senior official names on the rise

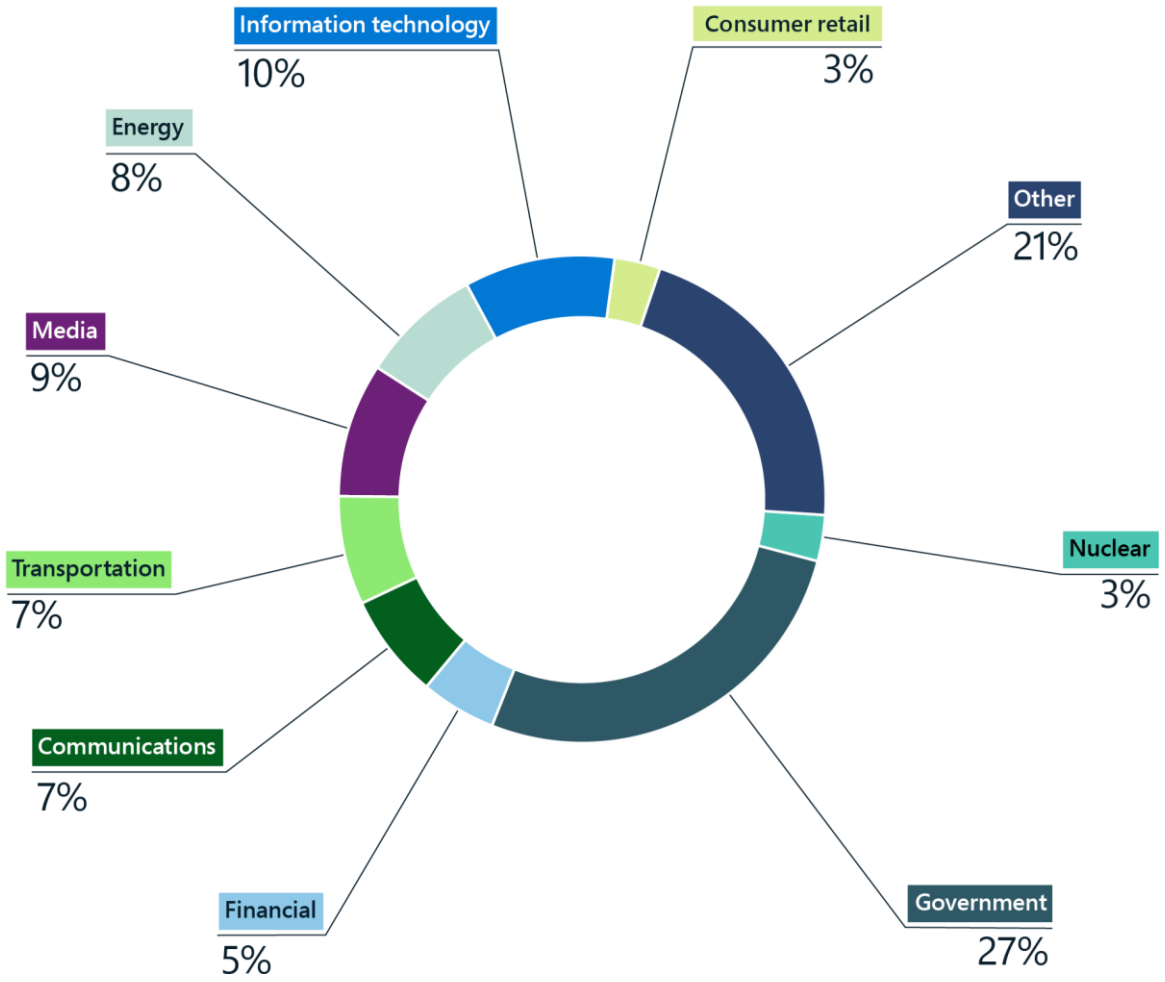


Endpoint is the new perimeter

99% of exploited vulnerabilities more than a year old

Old versions of unsupported applications still in use on millions of devices

Ransomware as a Service (RaaS)

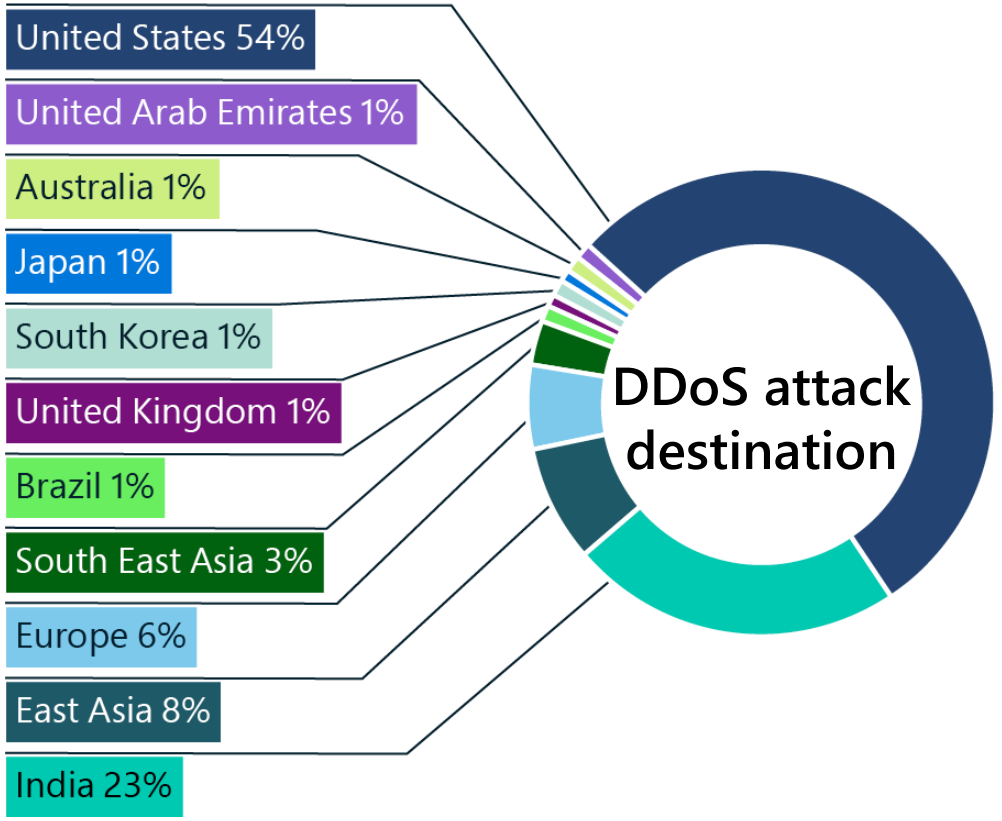


Network related attacks expected to rise

2,000 DDoS attacks per day

Substantial increase in nation state attacks

150M network intrusions (network exploits & malware)

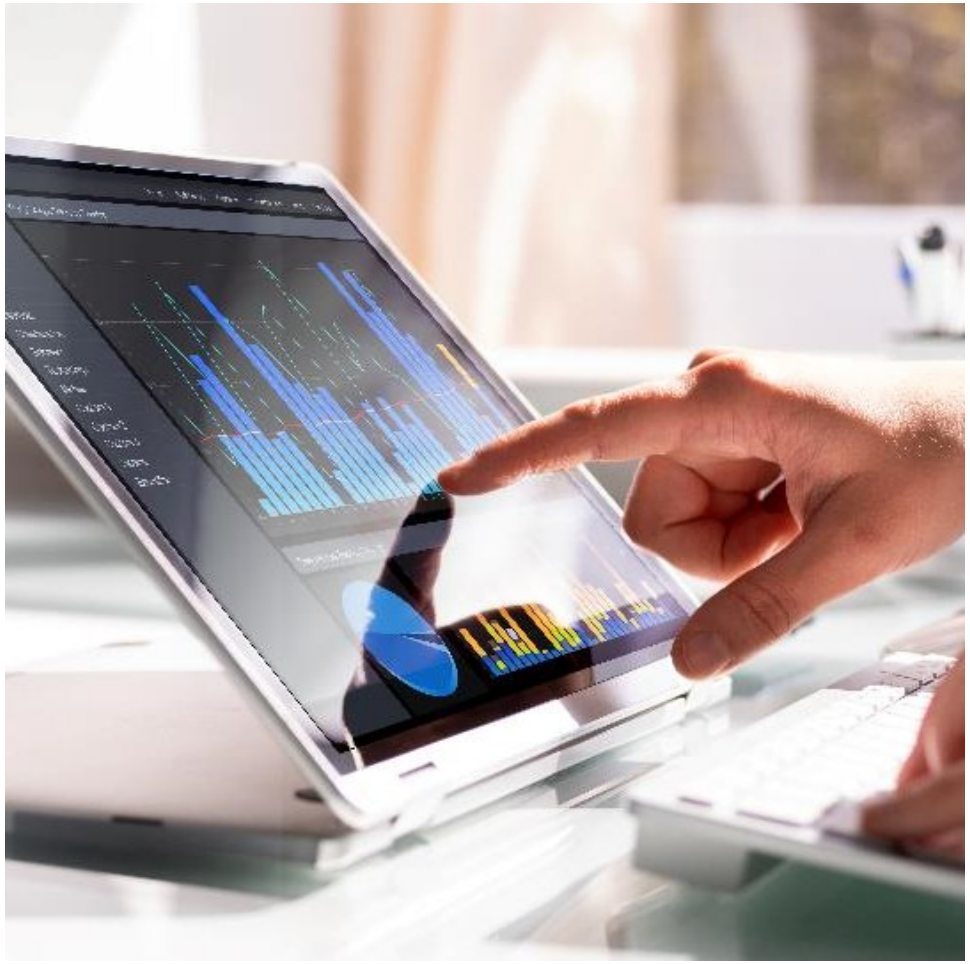


Data protection is top of mind

44% impacted by Ransomware did not have recoverable backups

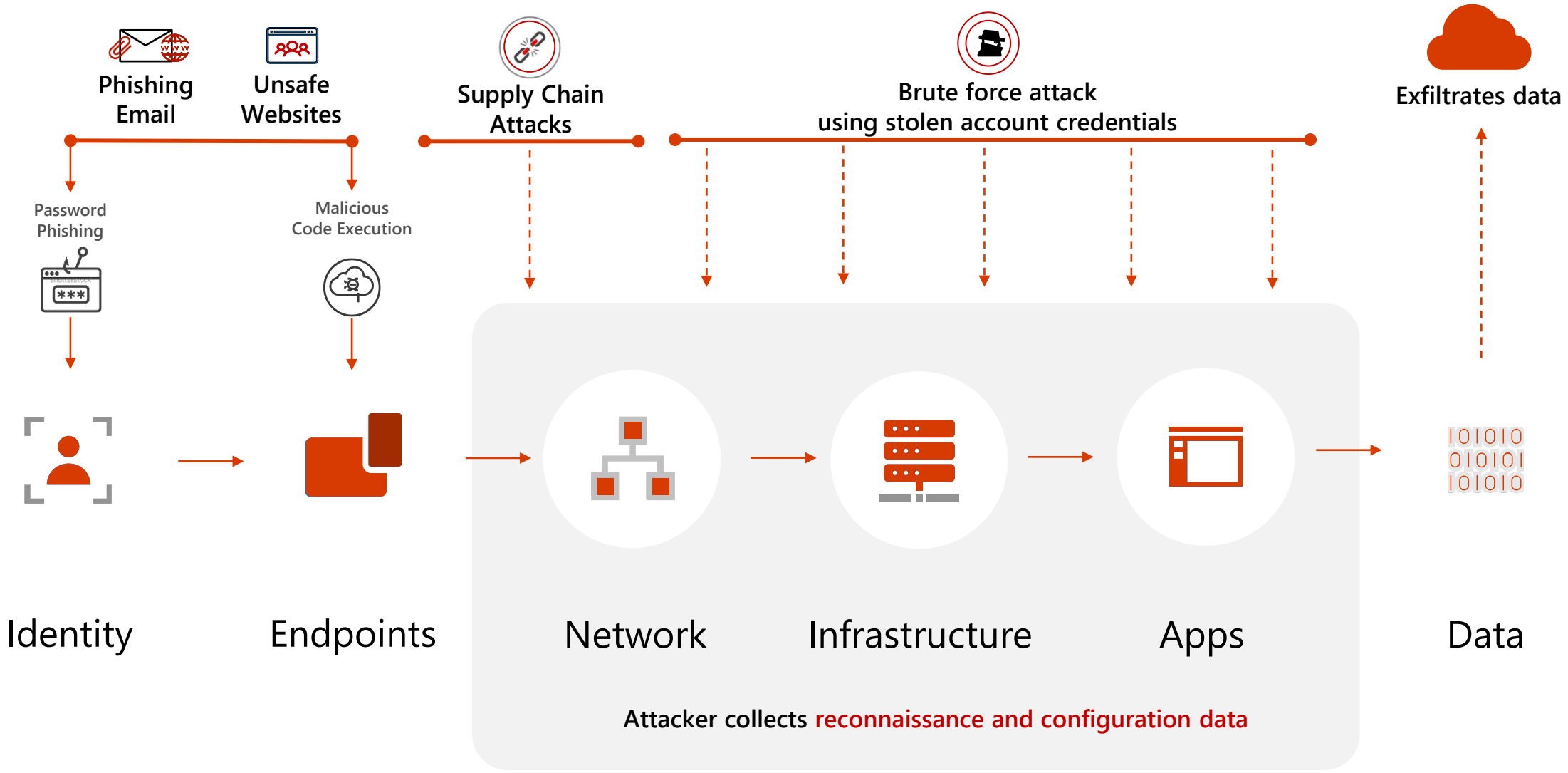
58% accidentally sent sensitive information to the wrong people

63% of organizations fear data leak/spillage during the pandemic



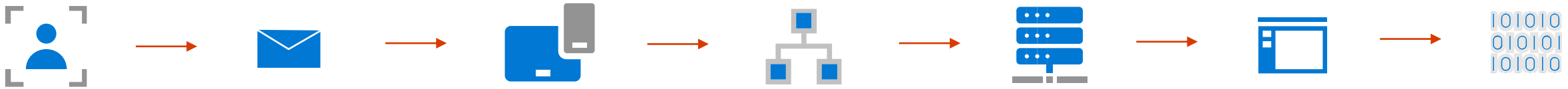
Increasing cyber threats to the Digital Landscape

We are witnessing increasing security threats across organizations



Zero Trust Approach for End-to-End Security

Holistic Security approach extending throughout the IT Estate is critical to digital success



Identity

- Single Sign-On
- Multifactor Authentication
- Self Service
- Identity Protection
- Conditional Access to Applications

Email

- Anti phishing & Anti-spoofing
- Zero-day malware scan protection
- URL click-time protection
- End user trainings & phishing simulation

Endpoints

- Updated systems and patch management
- Next generation AV and EDR tools
- Ransomware protection
- Hardware isolation
- Passwordless access
- Disk Encryption
- Device management

Network

- DDoS protection
- Web application firewalls
- Micro-segmentation

Infrastructure

- Posture Management
- Server & DB security
- Anomaly Detection
- Continuous Vulnerability Management

Apps

- Secure Development
- Vulnerability assessment
- Penetration testing

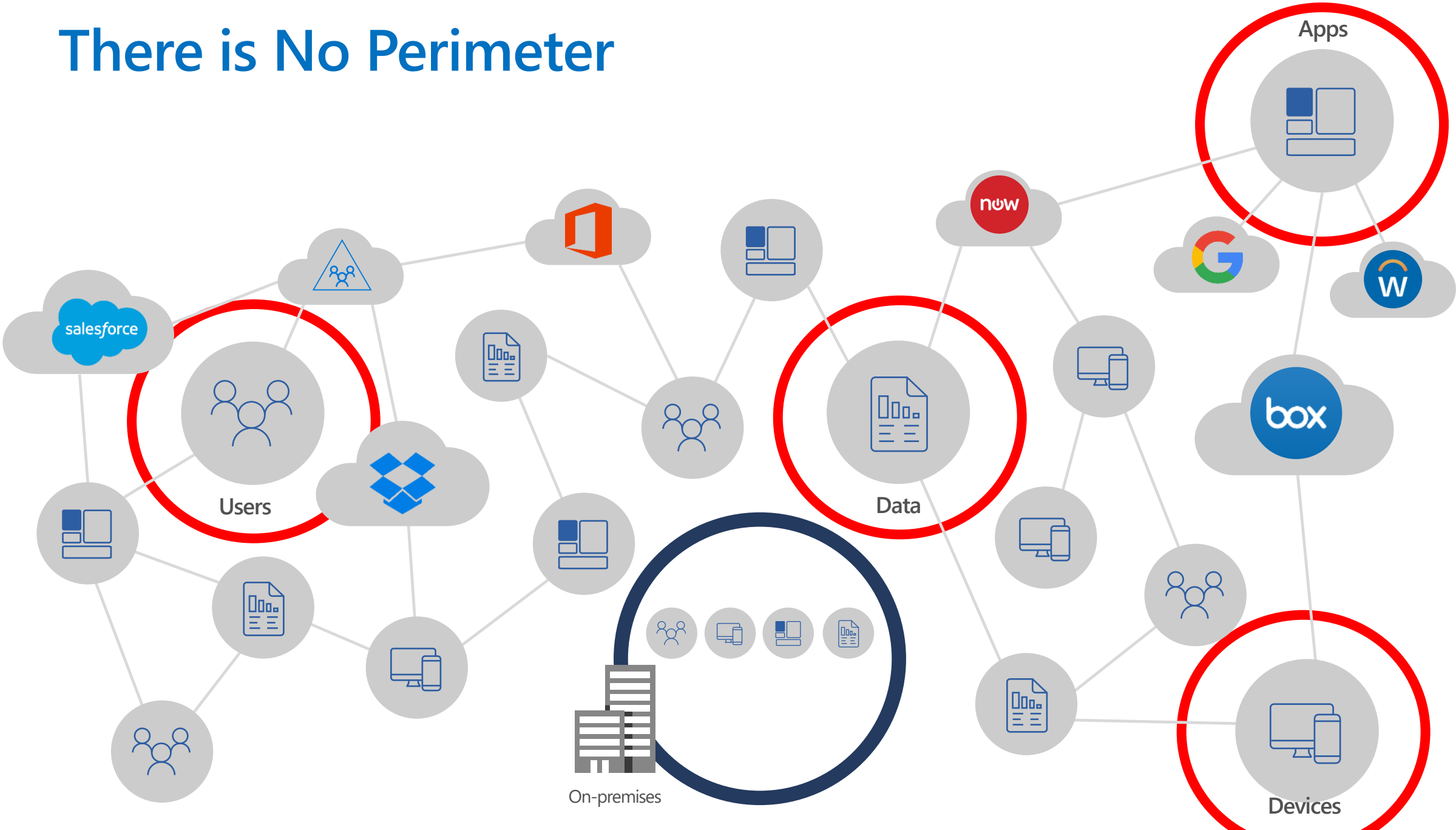
Data

- Data Labelling & Classification
- Email encryption
- Document encryption
- DLP controls
- Recoverable backups

- Continuous monitoring
- AI/ML based detections
- Threat Intelligence
- Response Automation

In Summary…

There is No Perimeter



Top Three Recommendations for MSMEs

Secure Front Door

Secure Devices

Secure Data

G20 – Coming Together for Building Trust In Technology

Cyber Norms

Critical Infrastructure Safety

Mitigating & Investigating Cyber Incidents across borders

Protecting Software Supply Chains

Respecting International Law & Rule of Law in Cyber Space

Capacity Building – MSMEs in mainstream

Discussion