Zero-Trust ABC Financial Services

Introduction – ABC Financial Services

- Multi-national company headquartered in Columbus, OH
- 30,000+ employees, 10,000 producers, and many business partners and customers.
- Two data centers in The Ohio Area - AWS and Microsoft Azure.
- Five office locations
- Several sales/service offices, call centers, sales representatives are not employees.

Introduction – ABC Financial Services (Cont.)

- Access the network with mobile devices/company and personally-owned devices.
- Offers remote or work-from-home.
- Mobile application to customers and access to website.
- Business partnerships – provide each other's applications using API, file transfer, direct network interface, and event streaming.
- Access from IoT devices using edge devices
- Implementing a zero-trust architecture is crucial and beneficial.

Zero-Trust Architecture

EVERY USER, APPLICATION, AND DEVICE HAS THE POTENTIAL TO BE A THREAT.

NOT TRUSTING ANY USER, APPLICATION, OR DEVICE IS BY DEFAULT.

EVERY REQUEST HAS A VERIFICATION PROCESS BEFORE GRANTING ACCESS.

ACCESS IS GRANTED ON A NEED-TO-KNOW BASIS.

Zero-Trust Architecture (Cont.)

- User must be authenticated and authorized before having access granted to any resources.
- Provide security across networks, applications, and endpoints.
- Secures assets, applications, users, and data from unauthorized access and data breaches.
- Assets should be identified and classified as what they are and where they belong.

Zero-Trust Pillars

Identity involves user authentication and risk assessments.

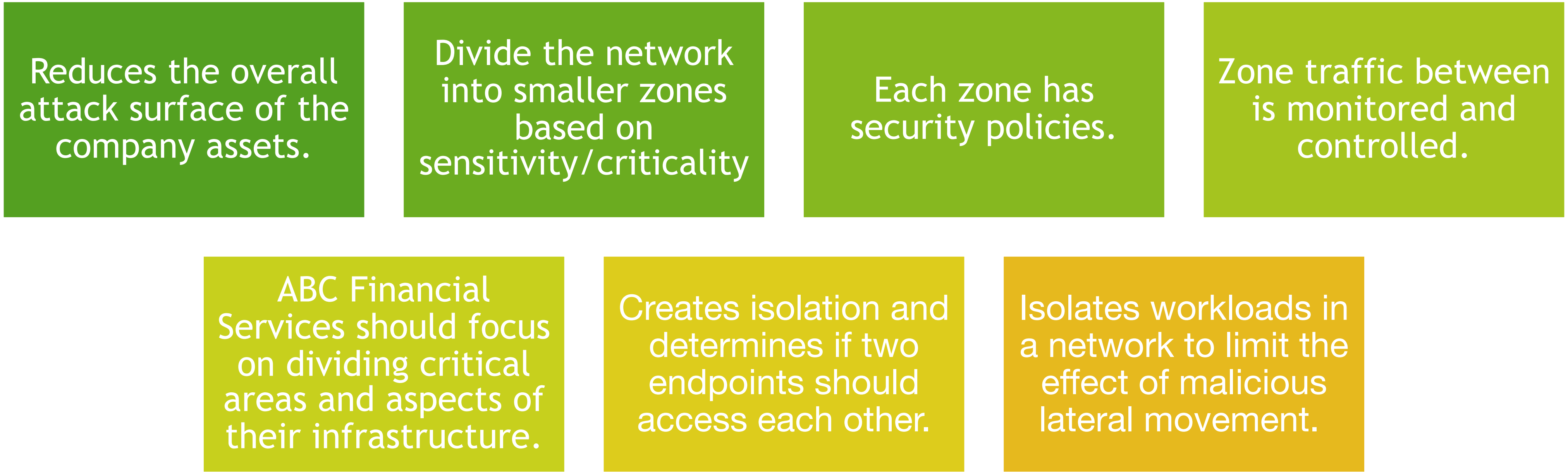
Device addresses asset tracking, access, and compliance with security protocols.

Network/Environment includes hardware, wireless, and internet connections, as well as encryption, threat identification, and network configuration.

Application Workload analyzes access, security measures, and threat identification for systems and applications.

Data involves securing data storage, access, encryption, and inventory management.

(Micro)Segmenting



- Reduces the overall attack surface of the company assets.
- Divide the network into smaller zones based on sensitivity/criticality
- Each zone has security policies.
- Zone traffic between is monitored and controlled.
- ABC Financial Services should focus on dividing critical areas and aspects of their infrastructure.
- Creates isolation and determines if two endpoints should access each other.
- Isolates workloads in a network to limit the effect of malicious lateral movement.

(Micro)Segmenting (Cont.)

- Performance increase: subdividing the network into smaller subnets and VLANs reduces the scope of broadcast packets and improves network performance.
- Security increase: access control lists to isolate machines on different network segments. In the event of a data breach, segmenting can prevent the threat from spreading to other network segments.
  - Networks
  - Applications and Application Servers
  - Endpoints
  - Data and Storage
  - Users

Networks

- Must have strong network security practices.
- A major backbone of smooth and professional business operations.
  - Application Programming Interface Security – APIs expose application logic and sensitive data
  - Public Interface Security - exposed to public/external entities
  - Network Access Controls - restrict unauthorized users/devices from gaining access
  - Regular Updates and Testing
  - Monitoring and Incident Response

Applications and Servers

- Must secure potential vulnerabilities that compromise the confidentiality, integrity, and availability of critical business systems and data.

    - Secure Configuration
    - Application Security - prevent data or code from being compromised
    - Application Server Access Control - restrict access to application servers
    - Monitoring and Incident Response
    - Authentication and Authorization – prevent access to sensitive data or resources
    - Regular Updates and Testing

Endpoints

- These devices store and contain important sensitive information for the company.
- Proper security will help prevent unauthorized access throughout the endpoints on the network.
  - Endpoint Protection – end-user devices
  - Endpoint Management - evaluate, assign, and oversee access rights
  - Endpoint Access Controls - security measures to restrict access
  - IoT Endpoint Security
  - Regular Updates and Testing
  - Monitoring and Incident Response – detect/respond | mitigate damage

Data and Storage

- ABC Financial is a large company, that houses lots of valuable data that will need to be properly secured.
  - Database Security - protect data from internal/external
  - Data Classification - add extra security measures to highly sensitive data
  - Cloud Access Controls - remote access
  - Software Protection
  - Secure Configuration - network devices are configured to follow all security measures
  - Regular Backups and Updates and Testing - ensures quick recovery time in case of attack
  - Monitoring and Incident Response

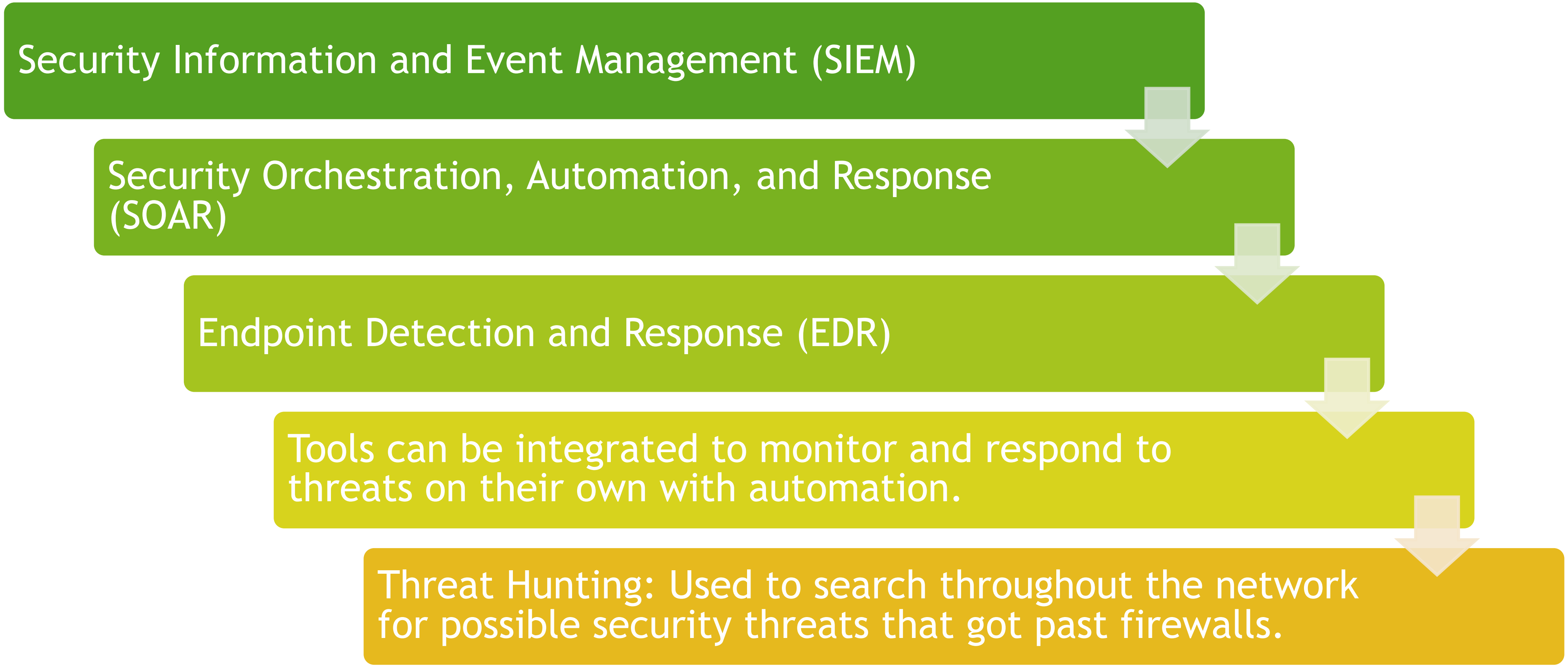
User Experience

- ABC Financial Services should focus on balancing user experience with security.

- It is beneficial to ensure security controls implemented do not interfere with productivity or satisfaction with employees.

  - Risk-Based Authentication - assess risk level
  - Seamless Access – Single sign-on
  - Educating Users
  - Context-Aware Policies – increased security controls from access outside corporate network
  - User-Friendly Security Controls - biometric authentication
  - Monitoring User Behavior

SIEM, SOAR, and EDR



Security Information and Event Management (SIEM)

Security Orchestration, Automation, and Response (SOAR)

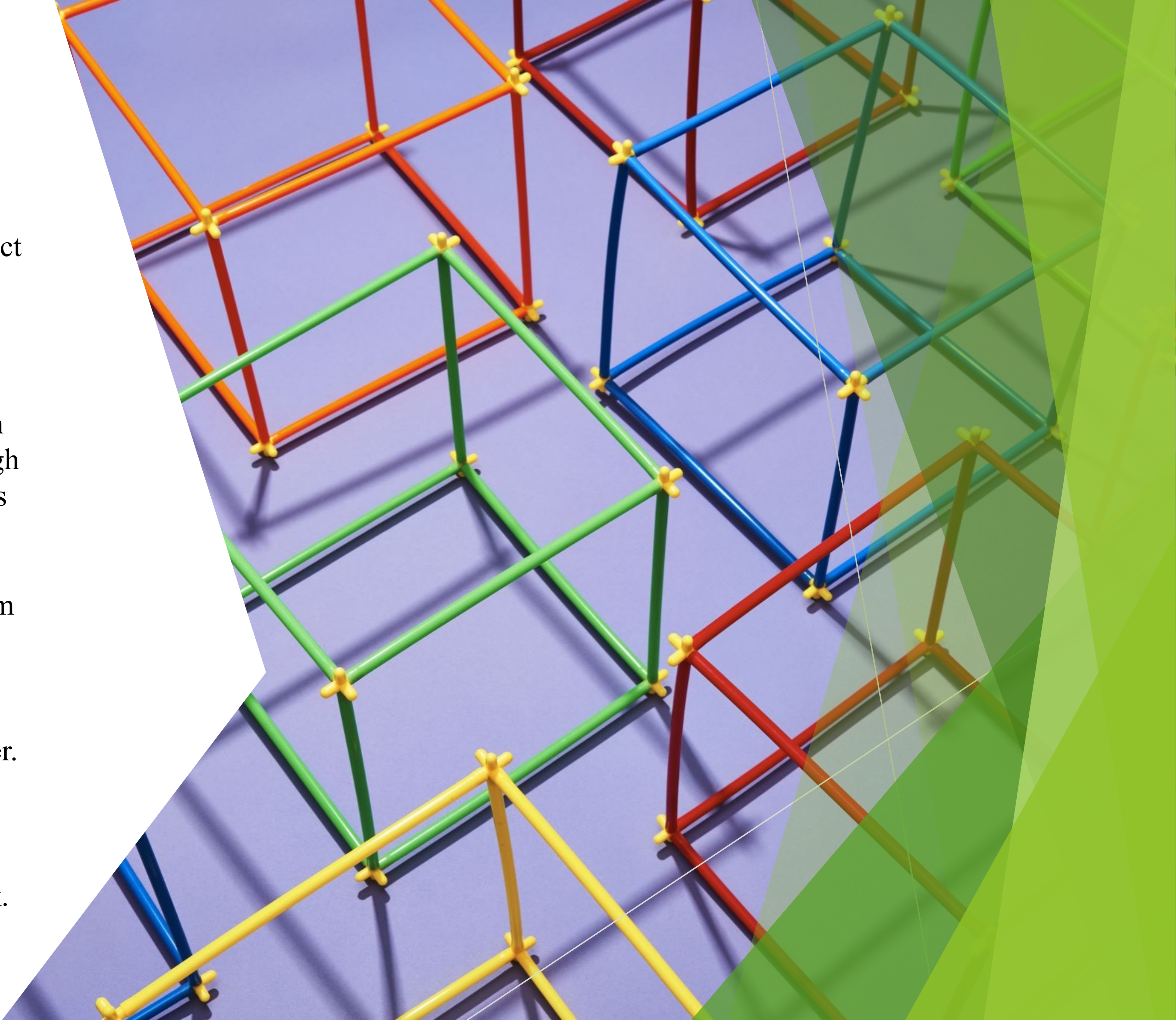
Endpoint Detection and Response (EDR)

Tools can be integrated to monitor and respond to threats on their own with automation.

Threat Hunting: Used to search throughout the network for possible security threats that got past firewalls.

Firewalls

- **Perimeter firewalls** monitor and protect from malicious traffic incoming and outgoing, from the outside.
  - Traditional Approach
- **Internal firewalls** monitor traffic from the inside that may have slipped through the perimeter from reaching other areas of the network.
- **Cloud firewalls** monitor all traffic from the internet before it reaches the cloud.
- **Application firewalls** watch for malicious traffic at the application layer.
- **Remote access firewalls** provide the ability to control and monitor network devices connected to the same network.



Security Policy

- Ensure a security policy that aligns with ABC Financial Services zero-trust architecture that has all employees aware of their roles and responsibilities.

- ***Mobile Device Management -*** ensures control and secures mobile devices, that are used to access sensitive data and systems.
- ***Role-Based Access Control -*** ensures control and restricts access to sensitive resources from specific user roles and responsibilities.
- ***Strong Authentication and Access Controls -*** verify the identity of users and devices while restricting access to sensitive resources based on authentication factors.

Security Policy (Cont.)

- ***Third-Party Access Control -*** manage and secure access to sensitive resources from third-party entities that are not automatically trusted solemnly.
- ***Regular Training and Awareness-*** education employees have about potential security threats and promotes a security awareness and best practices environment.
- ***Incident Response Plan -*** responds to and mitigates the impact of security incidents.
- ***Continuous Monitoring -*** detection and response to potential security threats while maintaining security and visibility over resources

Software Recommendations

Advanced security features with frequent updates and more reliable support is critical.

- *Microsoft Azure Active Directory* - IAM, MFA, MDM (MAM).
- *VMware NSX* – Network (micro) segmentation
- *CrowdStrike Falcon* - EDR.
- *Splunk Phantom* - SOAR.
- *Splunk Enterprise Security* - SIEM.
- *Snort* - IDS and IPS.
- *Okta* - SSO and RBAC.
- *Microsoft Azure Security Center* - Cloud Security.
- *Auth0* - API security.
- *IBM Sterling Secure File Transfer* - Secure file transfer.

Plan Layout

This plan should be implemented in phases, starting with the critical components, then expanding to cover the entire environment.

The initial timeframe of 12-24 months is the budget for this zero-trust architecture plan implementation for ABC Financial Services.

Plan Layout (Cont.)

Zero-Trust Architecture:

- IAM solution with MFA
- Segmentation and micro-segmentation
- Data protection and access controls
- Endpoint protection – EDR/SIEM
- SOAR – continuous monitor/threat detection
- SIEM
- Firewalls - Networks and Applications

Endpoint Security Controls:

- Company-owned devices - protection software and device management
- Personally-owned devices – MFA/MDM
- IoT devices with access controls and network segmentation

Secure Cloud Environments:

- IAM/MFA for secure cloud access
- Access controls and encryption
- Patch management and Vulnerability scanning

Seamless User Experience:

- SSO – access multiple applications
- Risk-based authentication
- Biometric authentication
- Self-based password reset

Security Policies Implemented:

- Role-based and least privilege access
- Data classification
- Incident response/disaster recovery
- User awareness

Business Partners Secure Integration:

- API security
- Secure file transfer