Exercise Overview for SSTL Inc.

SecureSmarterTech Logistics, or SSTL Inc., is a mid-sized supply chain and logistics company specializing in the transportation and warehousing of high-value goods for the healthcare, electronics, and manufacturing industries. The company operates globally with regional offices, distribution centers, and a network of third-party logistics vendors. They hire contractors for both pick-up and delivery, as well as the installation of technology tools. They maintain data centers in five major global hubs and are gradually phasing out these data centers as they migrate workloads to the cloud. Due to the original company's multiple mergers and acquisitions, many complex and confusing security tools and systems often overlap or counteract other security measures. The subscriptions and maintenance fees to keep these systems active are expensive.

Key Business Elements

1. **Operations:**
    - Transport management via a centralized platform.
    - Warehousing with real-time inventory tracking systems.
    - Just-in-time delivery coordination with manufacturers and retailers.
2. **Clients and Vendors:**
    - Direct contracts with major manufacturers, requiring secure integration of inventory and order systems.
    - Third-party logistics providers handle last-mile delivery in multiple countries.
3. **Remote Workforce:**
    - Employees, external clients, and vendors access corporate resources remotely via VPNs. The VPN appliance sits behind a stateful or dynamic firewall in the DMZ.
    - Vendors and contractors log in using external accounts to view shipment statuses and process orders. All user IDs are created and managed manually, and accounts are stored locally. In most situations, users only need to supply a password to login.
4. **Technology and Applications:**
    - Legacy warehouse management systems (WMS) running on-premises.
    - Customer-facing web applications hosted in an IaaS cloud environment.
    - Business-critical ERP and CRM platforms are currently on-prem but slated for migration to the cloud.
    - Customer data of various sensitivity is stored on servers and backup devices in local data centers. Some critical data is backed up offsite to the cloud. Highly critical data is stored in replicas across availability zones in the cloud.
    - Some endpoints are simple and dual-process scanners that behave as POS for field transactions. Other endpoints are laptops and BYOD smart devices that are unmanaged.

-

Network Architecture

1. **Trusted Zones:**
    - Internal corporate network housing ERP, CRM, and other business-critical applications.
    - Employee workstations with direct access to internal servers.
    - Utilize F5 Big IP and Palo Alto NGFW.
2. **Untrusted Zones:**
    - External internet-facing applications, such as customer portals and APIs used by third-party vendors.
    - Endpoints used by remote workers and vendors.
3. **Demilitarized Zone (DMZ):**
    - Web servers hosting customer portals and vendor access points.
    - Public-facing APIs for integrating with supply chain partners.
4. **VPN Usage:**
    - Employees and third-party vendors use VPNs to access internal systems.
    - VPN connections also integrate systems with third-party processors for payment, order management, and delivery tracking.
    - Field scanners attach to the data center network via the VPN initiated by a script that logs into the fulfillment and logistics systems for processing. The scanners are given access to the network based on enrolled MAC addresses.
5. **Authentication and Authorization:**
    - User IDs and passwords are the primary methods for authentication.
    - No multi-factor authentication (MFA) or granular user access policies
6. **Microsoft AD and Azure Cloud for storage. For MDM, they use Intune**

Business and Security Risks

- **Network Perimeter Reliance:**
    - Assumes a clear boundary between trusted and untrusted zones, making the organization vulnerable to lateral movement by attackers once inside the network.
- **Weak Remote Access Security:**
    - VPNs provide broad access to internal resources, but lack granular control.
- **Legacy Systems:**
    - Older applications lack modern security features and are challenging to secure.
- **Third-Party Risk:**
    - Vendors and partners often have less stringent security measures, increasing the risk of compromise.
- **Single-Factor Authentication:**
    - Password-only authentication leaves systems vulnerable to phishing and credential-stuffing attacks.

-

Why Zero Trust is a Great Fit

Zero Trust implementation can transform SecureSmarterTech Logistics Inc.'s security posture by addressing its reliance on traditional network perimeters and weak authentication mechanisms. Key benefits include:

1. **Identity-Centric Security:**
   - Implementing MFA and conditional access policies ensures that users and devices are verified continuously, regardless of location.
2. **Least Privilege Access:**
   - Users and vendors gain access only to specific resources they need, reducing the attack surface.
3. **Microsegmentation:**
   - Network resources are segmented, preventing lateral movement by attackers.
4. **Secure Legacy and Cloud Integration:**
   - Modernized security controls protect legacy systems and enable secure migration to IaaS platforms.
5. **Monitoring and Threat Detection:**
   - Continuous monitoring and logging of all access requests enhance the ability to detect and respond to threats in real-time.
6. **Vendor Management:**
   - Access policies for third-party vendors can be tightly controlled and monitored.

SecureSmarterTech Logistics Inc. is an ideal candidate for a Zero Trust architecture, which will help it future-proof its business operations while maintaining robust security for its sensitive assets and processes.