LTIMindtree

Case Study

Securing the Future: A Case Study of Zero-Trust Enabled Azure Cloud Migration for a Major Insurance Provider

Client

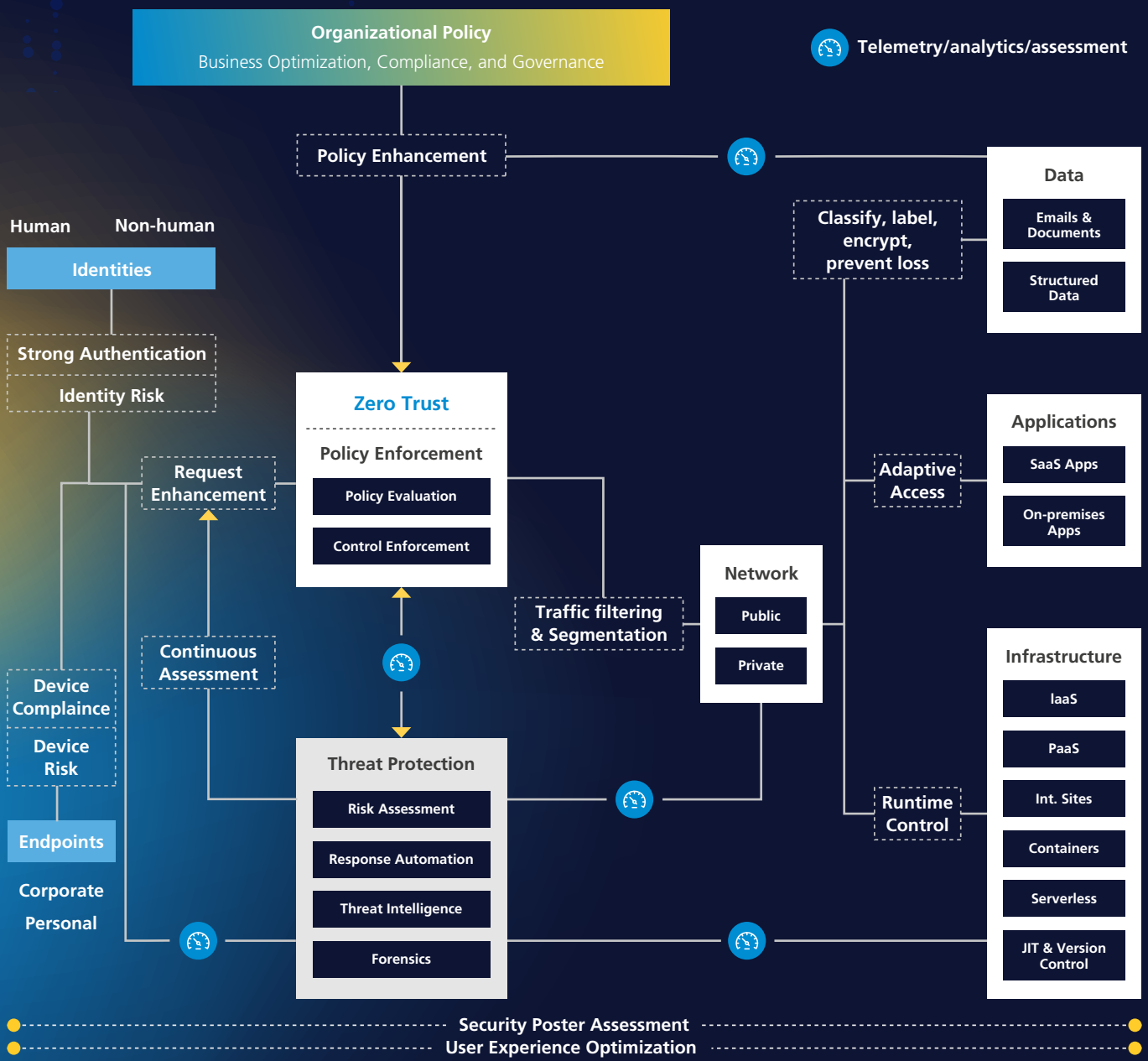
The client is one of the world's largest insurance brokerage services providers. They were managing the workloads on-premises and facing difficulty in keeping up with the latest security best-practices and timely detection and response to security breaches. They wanted to migrate all their entities to Azure cloud for continuous updates, greater scalability, and enhanced protection against cyber threats. They also wanted to establish a security operation center that helps them monitor and detect potential threats.

Challenges

- Lack of a centrally managed Azure security program across the entire customer base.
- Inconsistent governance across all tenants.
- Lack of a centralized SIEM solution to monitor and detect threats in real-time.
- Inability to fully utilize the Azure advisory services across the subsidiary base.
- Lack of security controls, integrated and automated threat mitigation system.

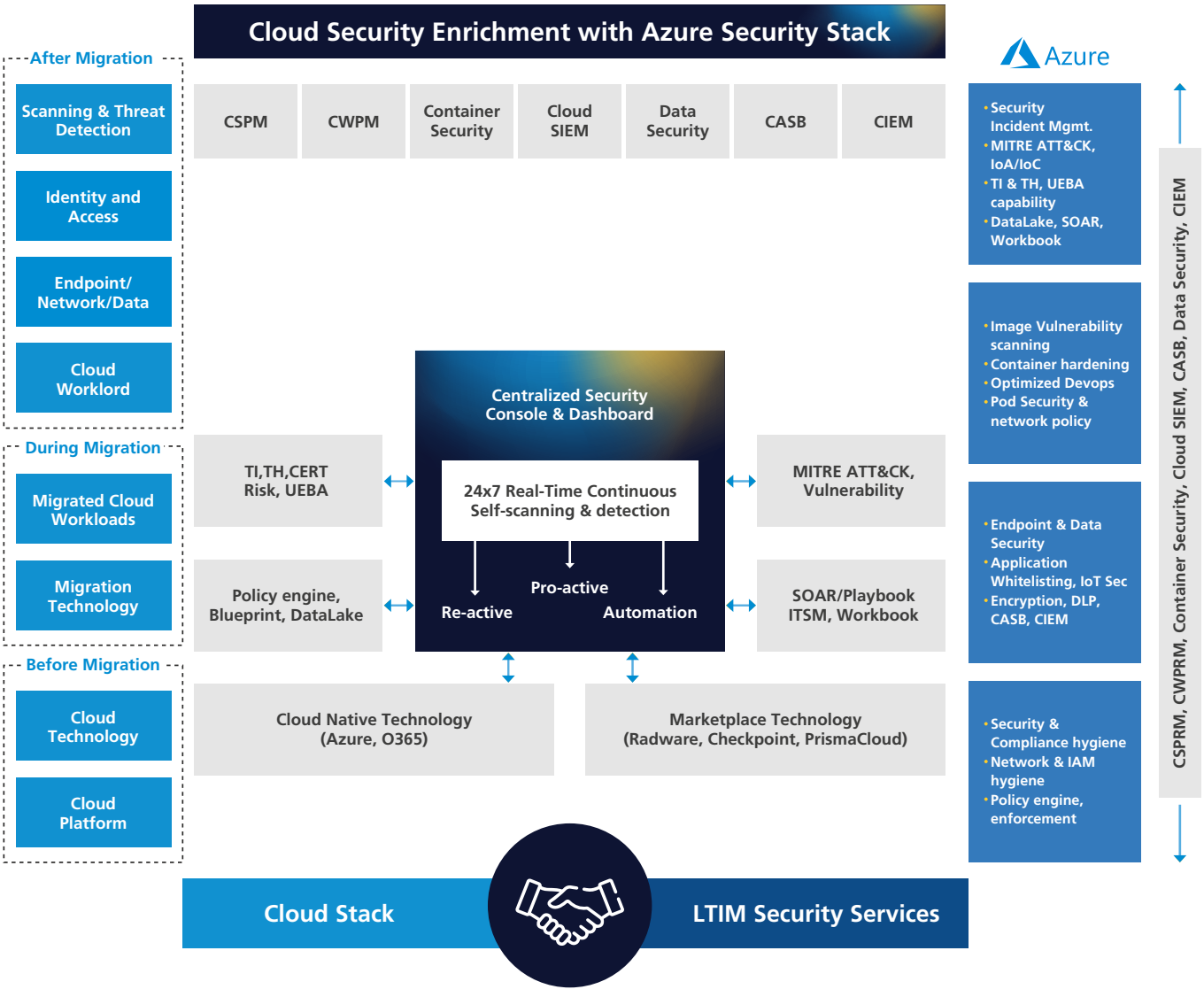
LTIMindtree Solution

LTIMindtree helped the client migrate from the current data center to Azure cloud and implemented a security operation center leveraging zero trust approach to secure the Azure cloud environment. Our zero-trust approach effectively adapts to the complexities of the new environment, protecting applications, assets, and data across the cloud.



Zero Trust Reference Architecture

With the zero-trust approach no entity inside or outside of the network can be trusted by default, every user and device are authenticated and authorized before allowing access to any resource or data.



Design supports both Multi-Cloud (Azure, AWS, GCP, O365...) and Hybrid Cloud environment

LTIMindtree Azure cloud Service Offerings

Key Solution Highlights

Enabled 24x7 Threat Detection and Monitoring to identify and monitor threats.

Azure AD Integration with on-premise DC and MFA enablement – PIM/PAM.

Consolidated all tools and utilized cloud-native security tools to improve security, enhancing security posture.

Utilization of Azure advisory services across the Subsidiary base, such as Service Health, Azure Advisor, Azure Monitor, and Security Center.

Tracking, Monitoring, and Maintaining Compliance with Security Policies.

Implementation of DLP policies and controls.

Implementation and operations of DDOS Protection.

Creation and consolidation of 250+ Production Azure Virtual Desktop Systems and 20 to 30 Non-Production Azure Virtual Desktop Systems.

Migration of applications from on-prem to Azure cloud where LTIMindtree designed and implemented Microsoft Sentinel SOC – A Cloud Native SIEM, SOAR, Threat Intel, and Threat Handling solution.

Business Benefits

- Reduced Mean time to detect, contain and respond
- Provided cloud security benchmarking with a zero-trust security approach
- Improved Threat Detection Efficacy to 75%
- Protection of application layer from layer 7 attack
- Reduction in the overall attack surface
- Enhanced data security by the application and finetuning of DLP policies
- Protected 10+ phishing campaigns and 3 ransomware attacks within the first two months of starting of SOC operation

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 84,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit **www.ltimindtree.com**