Case Study

ZTNA to Multiple Data Centers

For Operations, R&D, and Technical Support Employees

Introduction

An international financial technology company, headquartered in London, UK, operates a Software-as-a-Service, AI-enabled, distributed-ledger technology platform for all stages of the pre- and post-trade lifecycle and portfolio services.

The company services large financial organizations including banks and brokers, demand-side firms, fund administrators, and prime and clearing brokers. It must, therefore, adhere to strict regulatory compliance. It has undergone external audits and subjected its processes to strict industrial certifications by accredited third parties to ensure the integrity, availability, and security of its operations.

The Challenge

The company has NOC and R&D operations in the UK, US, and several additional locations, monitoring and supporting the infrastructure of their solution suite.

One of the main challenges facing the CIO was demonstrating governance over which employees could gain access to sensitive environments containing customer transactions data. The conditions under which the access would be granted was another important aspect. Data centers hosting earlier generations of the services provided by the company to its customers were accessible via VPN solution from the corporate headquarters network.

The access policy was managed by the NOC. Providing accurate reports on which employees were accessing different parts of the data centers was challenging and time-consuming. This negatively affected the time it took to onboard new customers to the company's services.

Infrastructure with Built-in ZTNA

When the company developed the new generation of its financial services solution suite, they decided to build a state-of-the-art virtualized infrastructure, leveraging the latest technologies from Amazon Web Services (AWS). The solution is elastic, and its continuous cycle of software updates is based on the immutable infrastructure concept. To monitor and support the new solution, teams such as the NOC, business analysts, DevOps, IT Infrastructure, and sometimes even account executives, require access to various servers/components of the virtualized infrastructure.

The company chose Symantec® Secure Access Cloud™ as the infrastructure for providing secure access only to relevant resources while enforcing Zero Trust principles and leaving all other resources cloaked. The Symantec platform was then integrated with the company's chosen Identity and Access Management (IAM) solution that defines corporate identities for all relevant parties and configures conditional access clauses. The IAM solution takes into consideration the location of the user, the security posture of the device, and several additional parameters. The integration with Symantec allows these attributes to define the access policies on the user/server level, throughout the entire lifecycle of each access session.

"Break glass" access procedures were defined to make the access control very strict and to tie each accessing process to a ticket in the enterprise ticketing system, integrating the approval cycle with their corporate communications systems, Office 365, and Slack. The resulting access policy is based on the following scheme:

As a result, the moment any kind of resource (compute, storage, database, application) is initialized in the environment, it is immediately associated with the relevant organizational roles that should get access to it, providing they meet the conditions required by the "break glass" access procedures. The implemented infrastructure is used to access the following types of corporate assets:

- Web portals (analytics, monitoring, configuration/ administration)
- REST APIs
- Linux servers (SSH)
- Windows servers (RDP)
- Database servers (SQL, NoSQL, Redis, and so on)

Access to all of the above resources is achieved through Symantec Secure Access Cloud, without the need to provision any endpoint agents and without providing any user network access privileges on the data center network. This is a critical advantage in a large distributed environment, and a critical element of governance tightening the control over sensitive customer data.

Integrations with Organizational Processes

After verifying the access policy scheme with a limited group of people (~30), the entire technical organization, consisting of a few hundred employees, has started using Symantec Secure Access Cloud daily. To scale the operation flawlessly, the following processes were taken into consideration:

- Onboarding of employees
- Onboarding of special applications and services used by various role-players
- Monitoring availability of various resources for access
- Automation of all operations processes

As all corporate IT applications (self-hosted or consumed as SaaS) are integrated with the same Identity and Access Management solution, onboarding of employees went very smoothly. The user experience of accessing all corporate resources became unified and was accessible to the users based on their identity and access conditions defined in the corporate IAM policy. The access was so convenient that various role-players have raised proactive requirements to add their special applications (Business Analytics tools, Database Management tools) to the access scheme so that they could benefit from the same streamlined access using any approved device.

Taking Cloud Technology to On-Premises Data Centers

After months of running the solution successfully in the AWS environment of the company, the IT/Operations department decided to migrate the access to existing self-hosted data centers located in New York and Chicago to the same access paradigm.

After a smooth migration, two VPN gateway clusters were taken offline and access to data centers hosting traditional solutions was turned into Zero Trust as well, not exposing any open ports to the internet and supporting connectivity for all the teams that require access to various components.

Summary and Benefits

With Symantec Secure Access Cloud, a leading international Fintech company has managed to implement a complete ZTNA infrastructure for both their cloud-based (AWS) and traditional on-premises data centers. Hundreds of people located on three continents are using this system on a daily basis, benefitting from a modern user experience, and performing their duties in any approved location using any approved device. The main benefits reported by the organization were the following:

- Improved security posture of production data centers, in comparison to a traditional VPN solution
- Ease of auditing and governance—identity-based access demonstrates exactly which role-players can get access to what resources
- Tremendous flexibility—users can access relevant resources from various approved locations, easy onboarding of additional services and users
- Flexible integration into existing organizational processes and infrastructure

Symantec enables security and IT teams to create Zero Trust Application Access architecture without traditional VPN appliances. Symantec Secure Access Cloud securely connects any user from any device, anywhere in the world to corporate on-premises and cloud-hosted applications while all other corporate resources are cloaked. No direct access is ever granted to prevent any lateral movements to other network resources while eliminating the risk of network-based attacks. The platform is agentless and can be deployed in less than five minutes, without forcing a disruptive change in the organization's existing architecture, user permissions, and applications. Symantec Secure Access Cloud™ provides full governance and real-time enforcement of users' actions in each corporate application.

SYM-ZT-Data-Center-DevOps-CS100 November 10, 2021