Background

DBS is a leading financial services group in Asia with a presence in 18 markets. Headquartered and listed in Singapore, DBS is in the three key Asian axes of growth: Greater China, Southeast Asia, and South Asia. The bank's “AA-” and “Aa1” credit ratings are among the highest in the world.

Recognized for its global leadership, DBS has been named “World’s Best Bank” by Euromoney, “Global Bank of the Year” by The Banker and “Best Bank in the World” by Global Finance. The bank is at the forefront of leveraging digital technology to shape the future of banking, having been named “World’s Best Digital Bank” by Euromoney and the world’s “Most Innovative in Digital Banking” by The Banker. In addition, DBS has been accorded the “Safest Bank in Asia” award by Global Finance for 12 consecutive years from 2009 to 2020.

Challenge

Security configuration management at DBS involves compliance checks and guidelines set by international organizations to enhance overall security. These security configuration definitions are converted into an automated capability to scan servers in the bank for the purpose of non-compliance reporting and rectification.

Prior to 2018, security configuration management was a manual process consisting of regularly generating reports, reviewing them, and subsequently remediating the security configurations in between cycle periods. This end-to-end effort was maintained by a team of 13 people. Furthermore, as the number of servers increased each year, the total time required for this lengthy scanning and reporting process increased. This led DBS to search for and develop a new solution that would be more efficient to manage the process. But in order to...
Challenge (continued)
accommodate in-house processes, DBS required heavy customization to automate the security configuration management.
Following multiple rounds of evaluation, DBS narrowed down their selections to Puppet Enterprise. Puppet Enterprise (PE) enables DBS to manage policy enforcement and reversion to baseline security configuration while also handling deviations. PE also serves as the automation orchestrator engine for their proprietary solution, SecureSys.

Solution
To meet their goals, DBS developed an in-house security system, SecureSys, to enforce security conformance end-to-end. Built on Puppet automation, SecureSys serves as the overarching framework that underpins their automation. Puppet Enterprise acts as the automation orchestrator engine and serves as the backend support for all other components.

DBS applies this automated capability to approximately 18,000 operating systems and 15,000 sub-systems (i.e. database and middleware software) to support their hybrid cloud model of on-premise data centers across six countries and a public cloud environment.

The overall enterprise architecture of Puppet is set up to support the regional architecture; which is simple and highly scalable. In detail, Puppet is split into three layers.

On the topmost layer is the primary server, with two instances of this component to provide high availability (active passive). The primary server coordinates and manages the compilers, hosts the certificate authority for agent registration and communication, runs the orchestration service, and manages the Puppet database (PuppetDB).

Next, the compilers sit on the second layer and build and compile Puppet code into a catalogue. It handles the compilation of tasks that the agent needs to run on the endpoint. The results of the catalogue run and the catalogue is synchronized between these compilers. These compilers sit behind a load balancer that allows for horizontal scaling of the infrastructure to support more agents for catalogue requests. If DBS needs to expand the coverage of the Puppet infrastructure, it is as simple as adding a new compiler.

Last, the third layer has the agents in the endpoints running on each server. Agents are authenticated through the internal certificate mechanism and run two services: the Puppet service, which is the main agent daemon, and the PXP service, which enables execution of actions on remote nodes.

With this three-layered approach, DBS can scale the architecture easily as they implement it in the public cloud. Auto-scaling is easy in the public cloud as the DBS team simply spins up and down the compilers using AMIs baked with the application on the image itself. On-premise scaling capability is semi-auto and taken care of through capacity management. With the amount of checks in place, a compiler with a configuration of 4 CPUs and 16GB RAM can support 1000–1500 nodes.

DBS also has three different engines on top of the Puppet automation orchestrator, including a Policy Engine. The agents allow the server to subscribe to a policy based on the group definition identified by a Puppet fact, run these policies against the server, report its state and automatically enforce the standards.

If DBS needs to expand the coverage of the Puppet infrastructure, it is as simple as adding a new compiler.
With the strategy set, DBS has packaged Puppet by default as a layer product that is part of the server standard build. All operating system platforms are equipped with the agent and are set to automatically register to the primary server and acquire the policies assigned to its profile.

For every software that is released in the production environment, there are checks that need to be carried out to ensure that it conforms to the security standards of the enterprise. DBS models these security standards after the best practices of other successful organizations or internationally recognized security standards, such as the Defense Information System Administration’s (DISA) Security Technical Implementation Guides (STIG). STIG is a compilation of guidelines aimed to standardize security protocols to improve security. These guidelines are then translated into the context applicable to DBS, specifically regarding the configuration and settings set on the software build. This ensures that configuration settings are consistent across all deployments. The number of policies ranges from five to 200, depending on the complexity of the platform.

DBS also uses the management console in Puppet Enterprise, which is a web application used to manage the entire infrastructure, including certificate authorization and the database. Exposing this console to users in the organization introduces complex role-based access control (RBAC). DBS’s objective for a user console is to enable users to view security reports on systems that they are managing, allow them to activate the auto-healing capabilities (for servers still in “NoOp”), and manage deviations. The SecureSys portal handles the reporting and deviation management capabilities and is built on top of the Puppet database. Multiple user personas are defined in the portal, from executive management to auditors, information security personnel, risk managers, system administrators, tech support and application teams. This enables DBS to provide custom console views based on location and business units. The portal allows for a single view of the reports and the required fixes (if needed) on endpoints.

Lastly, not all applications can comply fully to existing configuration settings, especially if the application is an off-the-shelf product. There will nearly always be one or more settings that need to vary from the baseline values for the application to work. DBS allows for these deviations if an explicit approval is sought from the security team and a corresponding authorization from the head of the department is granted for the acceptance of risks. This entire process of discovering deviations (when the agent is in a “NoOp” mode) to raising a deviation request, routing to approval, and actual implementation is done through the SecureSys portal.

Results

With Puppet Enterprise, DBS has made significant progress with their SecureSys framework, moving from monolithic and manual configuration management to an automated and scalable solution. They have seen substantial benefits, including reducing the equivalent of 13 staff to three. This frees up the time and energy for engineers to invest in other value-driven innovation or projects that the organization could benefit from in the long term. All drifts in mandatory configurations are being auto-healed, removing toil on both infrastructure and application teams who no longer need to coordinate with each other for fixes. Reporting overheads are also reduced, and reports can be generated nearly in real-time, with scans running every 30 minutes. With all these frameworks in place, DBS is set to keep pace with the ever-changing needs of their ever-growing organization.