SOLUTION BRIEF

RAPID IMPLEMENTATION OF ZERO TRUST

CHALLENGE

Enforcing access control policies is easy, but adhering to least privileged access is not. Most organizations have a very efficient means to grant access to users; however, they do a poor job at routinely reviewing access to see if it's still needed and then removing access when it's not. This leads to users becoming over privileged, significantly increasing the risk if their accounts should be compromised.

OPPORTUNITY

Symantec IGA uniquely helps address least privileged access through an integrated suite of identity management and governance capabilities that combines robust functionality with an intuitive, convenient, and business-oriented experience, as well as features to enable the solution to be deployed easily and quickly. This bridges the divide between what access users do have and what access they should have.

BENEFITS

A Zero Trust approach addresses many of the security challenges of today's open enterprise, including remote workforce, BYOD, and cloud migration. Identity Security plays a foundational role in achieving Zero Trust because you cannot enforce appropriate access controls if you cannot verify the identity of the user requesting access. Equally important is adhering to least privileged access to mitigate damages from account takeover attacks and malicious insiders. Symantec IGA can help organizations to streamline the review and certification of user access and quickly find and remove unnecessary entitlements and policy violations.

Symantec by Broadcom Software

The second principle of Zero Trust is to ensure least privileged access; however, many organizations still struggle with over-privileged users, increasing their risks if these accounts should be compromised.

Introduction

Improper user entitlements have been the root cause in a number of public breaches. This is especially true for privileged users because they tend to have very broad entitlements. But, the principle is the same for all users—we need to correct improper entitlements that violate security policies before they get granted ("preventative control"), and terminate any that may already have been granted in the past ("reactive control"). Unless effective controls are in place for both cases, risk will be increased, compliance audits will be more challenging, and zero trust will not be achieved.

In a similar vein, sometimes policies change and access granted long ago now violates a new policy, or access that was once needed no longer is. During regular access certifications, this needs to be made visible to managers so that they can also de-certify these entitlements. However, often access entitlements that were designed for Admins who understood their meaning, are foisted on users and managers, who struggle to understand the "IT-speak" terminology. Increasingly as business users are engaging with corporate identity processes, this non-intuitive experience hampers adoption, reduces satisfaction, and often ends up with business owners approving entitlements without knowing what they mean.

This solution brief not only highlights the key Symantec® IGA features that helps organizations address these challenges and adhere to a least privileged access security posture, but also describes those features that enable organizations to quickly and easily implement Symantec IGA.

Introducing Symantec IGA

Symantec IGA delivers core enterprise-grade identity management and governance capabilities, including:

- **User Provisioning –** Automates the processes to create, modify, disable and delete user accounts and their profiles across IT systems and business applications. This includes assigning roles and permissions during new employee onboarding, changing access when users transition to new positions, and removing access and accounts when users leave the organization.
- **User Self-Service** – Providing a convenient, business-oriented experience is necessary, but not sufficient, for improved user satisfaction and productivity, minimizing the need for users to contact the IT help desk.
- **Password Management** – Provides a comprehensive set of password management services that increase security by enforcing consistent password policies across the organization. These include applying password policy definition and enforcement, as well as password synchronization.
- **Access Certification** – Streamlines the processes associated with user, role, and resource certifications and automates the removal of unnecessary access through integration with the provisioning engine. Access privileges can be automatically gathered and correlated. These processes can be scheduled to run periodically or run on demand.

REALIZE A DRAMATIC REDUCTION IN TIME-TO-VALUE AND TCO, ALLOWING YOU TO ACHIEVE MORE WITH THE SAME TEAM AND BUDGET.

CONFIGURE AND CUSTOMIZE KEY IDENTITY SERVICES IN MINUTES AND WITHOUT ANY CODING, FURTHER REDUCING YOUR TIME-TO-VALUE.

By improving user experience and business user productivity, Symantec IGA dramatically increases the value provided by you existing enterprise identity and access management platform while removing a significant administrative burden from the IT organization. The following sections will focus on those features that enable the solution to be quickly deployed.

The Virtual Appliance

It's no secret that setting up traditional enterprise software can be tricky. In many cases, simply installing the software components and making the adjustments to meet corporate policies can be a confusing, time-consuming and error-prone process. You generally have to install new operating systems, application servers, directories, plus the product itself. You also have to manually set up clustering configurations for these components and use only corporate approved configurations. Finally, you have to run a number of manual hardening steps to ensure that the highest security standards are met. This painful process typically takes days to complete, and even longer if problems or major questions arise.

You could look to the cloud to eliminate many of these challenges, but then you are relying on a third-party SaaS provider to secure your critical identity management system and data from external hackers, or...you could deploy the Symantec IGA virtual appliance (vApp), which offers a delivery approach designed to help you deploy your identity management solution in minutes. How? By eliminating the traditional installation phase and providing a pre-installed, preconfigured virtual machine image that's ready to run in production configurations under common virtualization platforms.

To deploy identity services, simply drag the service name onto the appropriate machine name, and the installation will be done automatically for you. If you drop the same service onto multiple machines, all the communication mechanisms for high availability (load balancing, failover, etc.) will be configured as well. No time-consuming, error-prone manual configuration is required. The time savings are dramatic.

The outcome of this approach is a dramatic reduction in time-to-value and TCO, allowing you to achieve more with the same team and budget. This method can also save thousands of dollars a year in software licensing costs because all the core system components can be freely deployed without the need for additional licenses.

Xpress Technologies

After you have successfully deployed Symantec IGA, the next hurdle is configuration, but we have you covered here too. Deployment Xpress represents a radical improvement on how identity management software is deployed. It consists of a collection of preconfigured user scenarios for common use cases that most organizations would typically require, including user onboarding, password reset, access certifications, partner onboarding and the like. Each scenario consists of all elements needed for an easy deployment, such as template user interfaces, workflows and policy definitions. Managers simply pick the scenarios they need, add them to the shopping cart, and then check out. At that point, all of these key elements are automatically loaded into IGA and deployed. Customizations can be made to these elements (such as corporate branding for the interface), but there is no custom code required. These scenarios speed the deployment process and can significantly reduce the time-to-value for deployment of typical identity services.

Additionally, Symantec IGA also provides three other Xpress tools:

- **Connector Xpress** is a wizard-driven utility that enables you to generate custom connectors to homegrown and cloud-based apps via a graphical user interface without coding. This capability greatly reduces the level of technical expertise required for creating connectors and enables the creation of custom connectors within hours rather than days or weeks.
- **Config Xpress** is a utility that provides system administrators the ability to easily move components between staging environments for simplified configuration management. It also provides a change analysis report that highlights differences between environments as compared to a current and baseline installation, as well as a "push-button" documentation process that records system components as a part of a system recovery plan.
- **Policy Xpress** lets you configure policies that execute your unique, complex business processes. Previously done through custom code, this wizard-based tool lets you build policies in-house within hours, rather than requiring weeks of programming.

BRIDGE THE GAP BETWEEN BUSINESS USERS AND IT TERMINOLOGY TO IMPROVE SATISFACTION AND ADOPTION.

Business Entitlements Catalogue

Another challenge that organizations often face when deploying an identity management solution is that the user experience for identity services is usually highly IT-centric. In the past, this might have been fine, but as identity services have extended past the domain of the pure IT user, this approach no longer is effective. Terminology and processes that might be second nature to an IT-savvy user can be confusing and frustrating for most business users.

Symantec IGA helps bridge the divide between current IAM technologies and business users through the user-friendly Business Entitlements Catalogue, which translates cryptic resource names, such as "TSS_MNG_per_view" into more intuitive ones, such as "Online Payroll". This makes it easier for business users to locate the roles and resources they need when requesting access, as well as for managers when reviewing and certifying access. The solution goes even further, allowing you to group applications and roles into logical categories for ease—for instance, creating a group named "SRM access" that includes the SAP apps, Oracle apps, and SalesForce capabilities business users typically need—all defined in terms familiar to those users. The Business Entitlements Catalogue enables you to create a mapping between business-friendly and understandable terminology and the IT-centric names that actually exist. This not only increases user satisfaction, but also increases adoption of the solution.

FORMULATE, ENFORCE, AND VALIDATE SECURITY POLICIES AND LOGICAL CONSTRAINTS TO ACCESS ENTITLTMENTS ACROSS DIFFERENT APPLICATIONS.

Business Process Rules

Improper user entitlements have been the root cause in a number of breaches. Part of this is because users were assigned entitlements that they did not really need, and part of this is because access was not removed when users transitioned to new positions or left the company. In either case, over-privileged users are a risk, but this risk is further compounded when the excessive privileges violate security policies. Ideally, you would want to correct improper entitlements that violate security policies before they get granted ("preventative control"), and if not, be able to quickly identify and rectify those that may already have been granted in the past ("reactive control").

Symantec IGA enables you to formulate, enforce and validate sets of business process rules (BPRs) to implement segregation of duties and other logical constraints regarding relationships between users, roles and privileges. For example, a BPR can model a constraint of "people with permission to access X cannot have permission to access Y," or a dependency relationship such as "only people with access A can have permission to do B." So, instances that violate these security policies can be prevented before they occur.

The solution can also warn you if conflicting rights are being requested (the Preventative Controls described above). It assigns a risk score based on the access being requested and the related policy. The risk score is based on the user, their other entitlements and any contextual factors that might be relevant. The requester is provided with this risk level when the approval request is made, so as to warn her of a potentially improper request. Similarly, the approver sees this risk score during the approval process, providing full visibility that can prevent granting high-risk access.

Symantec IGA also provides Reactive Controls to remediate improper access that has already been granted. At the time of certification, the solution runs policy checks against access and highlights wherever the user has improper access rights that violate any policies. The Manager sees violations clearly marked for each user in order to allow for immediate correction. Both types of controls can significantly reduce the risk of improper entitlements being granted, or remaining undetected.

THE SOLUTION OFFERS CAPABILITIES AND BENEFITS NOT AVAILABLE IN OTHER SOLUTIONS.

Summary

The identity management and access governance capabilities of Symantec IGA enable organizations to quickly provision users to a broad range of applications; simplify and streamline identity management processes; enable convenient self-service; and reduce overall security costs. The solution offers also provides capabilities and benefits not available in other solutions, such as:

- **Intuitive, business-oriented user experience** – The user experience and convenience offered by the solution is unmatched in the industry. Key identity management capabilities such as provisioning, self-service, access requests and entitlement management are available in an intuitive, business-oriented experience. The result is improved user satisfaction and increased productivity.
- **Reduced total cost of ownership (TCO)** – Deployment Xpress enables you to get up and running with common identity use cases in a fraction of the time it usually takes with other solutions. Connectors to custom applications can also be deployed easily using Connector Xpress. Our customers have found that deployments are simpler, quicker and require less ongoing code maintenance.
- **Strong, robust connectivity with target systems** – Symantec IGA includes connectors that provide deep functionality, rather than simple connectivity. For example, the Active Directory (AD) connector enables management of groups and distribution lists directly, simplifying management of AD user information.
- **Proven enterprise-scale** – Symantec IGA is being used today in some of the largest and most complex IT environments in the world. It can meet your needs for scale now and into the future.

For more information, please visit
broadcom.com/symantec-iam

About Broadcom Software

Broadcom Software is a world leader in business-critical software that modernizes, optimizes, and protects the world's most complex hybrid environments. With its engineering-centered culture, Broadcom Software is building a comprehensive portfolio of industry-leading infrastructure and security software, including AIOps, Cyber Security, Value Stream Management, DevOps, Mainframe, and Payment Security. Our software portfolio enables scalability, agility, and security for the largest global companies in the world.

For more information, visit our website at: software.broadcom.com

RAP-IZT-SB100 September 2, 2022