ironsphere

MASTERING IDENTITY GOVERNANCE & ADMINISTRATION

White Paper

Abstract

Enterprise networks have never been more important, as nearly every aspect of global businesses is being digitally transformed. As more and more applications support work getting done, from workflow and communications, to customer attraction and retention, and the very digital products and services enterprises offer, networks are fundamental to success.

Enterprise networks have also never been more vulnerable, whether from intentional attacks by increasingly sophisticated criminals, or unintentional but equally as devastating changes to network policies by a greater number of internal and external administrators. The latter threat has become more pervasive as enterprises move to SaaS models, switch from traditional infrastructure to private, public and hybrid cloud, and need to manage a much broader and dispersed set of endpoints, whether mobile devices or IoT endpoints.

A heightened awareness by Chief Information Officers, Chief Security Officers, Chief Compliance Officers and IT leaders, along with investments by service providers to ensure quality of service and quality of security is built into their next-generation offerings, has driven a movement in mastering the art and science of IGA – Identity Governance and Administration. In this White Paper, you'll learn how the best enterprise networks protect critical assets by securing and managing access with the most robust and cost-effective identity governance software, policies, and approaches.

Mastering The Solution Requires A Comprehensive Understanding of the Challenges

As enterprise networks become more complex, more and more devices are connected and systems have to be supported, and as enterprises continue to outsource certain applications and functions, it's critical to have full transparency into which entities are interacting with those networks.

The human capital necessary to keep an appropriate watchful eye on the network makes manual monitoring costly; thus, IT leaders are seeking out network automation solutions, including those which use software and the cloud to authenticate, authorize and account for all the activity on the network, while also providing real time information on resource consumption.

Effectively and automatically aligning enterprise's policies with the identities and access privileges of its users is a vital security control for today's enterprise. Global enterprises recognize that their employees, customers, partners and vendors are among the main entry points into their organization. With the rapid adoption of cloud solutions, mobile computing and bring-your-own-device programs, and more, the enterprise perimeter is expanding exponentially, dramatically increasing the number of entry points.

The cost of securing every entry point even as those entry points are provisioned can become exponentially more expensive, unless enterprises take a fresh look at what they have been paying per end-point, for example, in the past, and "do the math" going forward. What is the true total cost of ownership (TCO) for governing and reporting on security in a world where hyperconnectivity will drive the requirement for more licenses, for example, as each endpoint is provisioned?

Are traditional security suppliers keeping pace with change, and the move to an all-software world, where even the most physical products are connected and include digital services? While the expansion of the enterprise network edge is exciting for traditional security suppliers who write about the "billions of endpoints" that will generate even more billions in profits beefing up their bottom lines, how can enterprises foresee the future costs associated with quality network security and compliance, and ensure they are making the right investment for the right return?

Mastering IGA is as much about the economics as the technology, software, service delivery models, opportunity for automation, and alignment with business policy.

Mastering The Solution Requires A Comprehensive Understanding of the Challenges

The principle of controlling which entities are accessing an enterprise network or using enterprise network equipment is known as Authentication, Authorization and Accounting (AAA).

- **Authentication:** Understanding who an entity is before allowing them to perform certain or any actions.
- **Authorization:** Ensuring the entity has the privilege to actually perform the actions.
- **Accounting:** Historical and accurate records detailing the actions that have occurred or the resources consumed.

The concepts of AAA may be applied to many different aspects of a technology lifecycle. Device Administration and Network Access are considered the two main AAA types for networking.

The two main AAA protocols commonly used for device administration in enterprise networks today are TACACS+ and RADIUS.

Device Administration

Controlling access to who can login to a network device via SSH/TELNET sessions makes device administration very interactive in nature. Users are authenticated once, but can be required to authorize many times during a single session in the command-line of a device.

Policies that enforce privilege-level and command-set permissions are required in order to successfully govern access and actions. For example, one user may have the privilege to execute only monitoring (read-only) command-sets, while another user may have the privilege to change the configuration of devices.

Both RADIUS (Remote Access Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System) can be used for such scenarios.

Given, however, how interactive device administration must be to fully secure critical assets, TACACS+ is able to separate authentication, authorization and accounting as independent functions, thereby supporting more granular privilege levels for device administration.

Network Administration

Network Access Administration ensures the identity of a user is authenticated before that user is permitted to connect to the enterprise network; both TACACS+ and RADIUS are used.

The expansion of the traditional enterprise perimeter is further challenging organizations to effectively secure all access points. Organizations as a result are directing new attention at protecting applications and data from unauthorized or criminal access across all enterprise entry points. And while identity and access management has typically been seen as a traditional IT process, it is becoming an increasingly important security measure, and a critical part of any solid enterprise security and compliance program.

Identity governance is also key to risk management, by mitigating the risk of data or access being compromised. It is a key line of defense in protecting enterprises, governments and other organizations from fraud by removing out-of-policy accounts before they can cause chaos that can take days or even weeks to control.

The right identity governance and intelligence solution can help organizations control access risks and ensure separation of duties with automated, business policy-driven software solutions used to set up and manage users and their roles based on access policies and risk profiles, ensuring day-to-day operations as well as supporting the important requirements for audits and forensics, should authorized users attempt to compromise the enterprise.

Enterprise leaders must be able to answer questions quickly should critical assets be stolen or systems disrupted. Who had access to what resources and when? How did those users get access to those resources and why?

Mastering Integration Means Minimizing Cost While Also Minimizing Risk

Effective IGA solutions integrate seamlessly with existing enterprise applications, including workflow, customer relationship management, financial systems, human resource systems, web and mobile applications, Internet of Things platforms, real time communications (voice, messaging, collaboration), and virtually any digital service that runs on enterprise networks.

Given the dynamic nature of the new digital enterprise and increasing pressures to do more and more online, and to diversify the architecture (from premise to cloud, from private to public to hybrid networks, and from the simplest to the most complex applications), IGA can rapidly become a huge cost center without considering in advance how it will be practically designed, implemented, managed and governed over time.

Enterprise leaders are not looking at IGA in a "steady state," rather they are planning over the long run, knowing that they must invest in more big data, analytics, artificial intelligence, and more futuristic technologies in order to remain relevant and competitive.

There is nothing more critical in selecting an IGA solution than to make sure it integrates with identity databases such as Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) databases. The solution should make it possible to create policies based on groups or subgroups which are already configured in these identity databases.

Six key points for enterprise decision makers to take into consideration when planning their IGA systems going forward.

1. The solution should include built-in support of internal or external RADIUS and TACACS+ servers to provide AAA (Authentication, Authorization and Accounting) services.
2. The solution should enforce user, source address, device type or date & time based policies.
3. The solution should include built-in integration support to NMS and SIEM systems in order to provide advanced audit capabilities.
4. The solution should include high availability support, granting with Active-Active or Active-Passive mode support, full database synchronization, and geosite redundancy features.
5. The solution should support massive and growing volumes of concurrent sessions with no degradation in performance.
6. If the solution requires additional hardware or complexity (such as Fabric Path) to support geographical redundancy, additional costs will be incurred; this is unnecessary with the most modern software solutions.

Mastering "Trust & Verify": Get Work Done Without Compromising The Most Valuable Assets

Enterprise security and IT leaders are extremely aware that it is the people inside their organizations who have the most access to the most critical assets – data that is vital to remaining competitive and profitable. They are also aware of the dynamic nature of organizations, including employees who move from one department to the next (therefore requiring different access levels to different data sets, for example) as well as a greater mix of third-party partners, contractors, consultants, analysts, developers and more.

World class IGA programs are balanced and strong; they support business agility and "getting work done" but never at the cost of compromising data, including private consumer data and competitive customer data, as well as confidential documents and intellectual property.

The best IGA programs include:

- Complete visibility into policy and all access privileges.
- Privileged user access with automation and tools for cost-effective monitoring.
- Proper access is granted only to authorized users with a complete trail for audits and investigations.
- Dynamic and automated logging, including proof of who granted access to whom, and when.
- Rapid identification and alerting of violations.

Maintaining a secure identity governance process can be complex without automation, increasing the likelihood of security gaps while also causing costs to build up as the enterprise perimeter expands. Hire more people - or use better software. Granting a person access in one area requires a process that includes application-specific information about the user's business role. When the user requires additional access elsewhere, the network administrator needs to provision again. The cycle continues - with each user requiring new access entitlements to support new job duties. Multiply this in large enterprises and the exponential increase in complexity, if not managed upfront with the right IGA solution, will lead to exponential and potentially "out of control" cost to ensure uncompromised security.

Conclusion

A solid IGA strategy and program brings together business policy, security and compliance with identity management processes and is made sustainable using the best software and automation solutions.

When enterprises upgrade their IGA programs, they can more effectively understand and control their digital platforms and networks, and make better decisions related to access and risk, protecting their most critical assets today and in the even more dynamic and competitive future.

Ironsphere's IGA Solution

Ironsphere's solution integrates with identity databases such as Microsoft Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) Databases. Policies can be created based on groups or subgroups which are already configured in these identity databases.

Ironsphere has built-in support for internal or external RADIUS and TACACS+ servers to provide AAA (Authentication, Authorization and Accounting) services, and can enforce user, source address, device type or date & time based policies. Built-in integration support to NMS and SIEM systems provides advanced audit capabilities.

Ironsphere features built-in high availability support, granting with Active-Active or Active-Passive mode support, full database synchronization, and geosite redundancy features.

Ironsphere supports tremendous volumes of concurrent sessions with no degradation in performance. No additional hardware or complexity (such as Fabric Path) is required to support geographical redundancy. Ironsphere eliminates customer's concerns over the EOL for ACS. It provides more comprehensive functionality than ACS and even over ISE.

Ironsphere's implementation is seamless and can leverage current ACS configurations.The cost model (resources and licenses) for Ironsphere is 40-60% less than a traditional ISE upgrade and the time-to-value is significantly reduced.

Learn more about Ironsphere by visiting ironsphere.com