Guidepost

RED-LIGHT, GREEN-LIGHT – THE CASE FOR A CONVERGED AND INTEGRATED IDENTITY ACCESS MANAGEMENT PLATFORM

In developing, deploying and managing physical and cyber security platforms around the globe, I often am asked about the latest lessons learned and best practices we recommend surrounding Integrated Identity Access and Identity Management (IAM). Current, traditional models for IAM do not address the vulnerabilities that have evolved throughout the security protection landscape, and corporations would be advised to take a fresh approach to their integrated IAM posture.

Traditional IAM

IAM is implemented in the corporate environment via three distinct paths; employee logical access, employee physical access and contractor access (either logical, physical or both).

The deployment of IAM across these domains is typically handled in a segregated and "siloed" fashion with the IT organization managing logical access, the security organization managing physical access, and requests being generated from procurement / contractor management for access authorization for contractors.

There are typically one or more baseline integrations with a company's HR platform (PeopleSoft, Workday, SAP, etc.) to "feed" information to the IT and security organizations on inbound new hires. These data artifacts can be used to prepopulate fields within Active Directory and the physical access control platform. This is accomplished with either a real-time Dynamic Data Exchange or through a scheduled "flat-file" data dump.

Where the Traditional Approach Falls Short

This traditional approach, while relatively easy to manage and inexpensive to deploy, has several severe restrictions

and vulnerabilities in today's threat environment.

The key vulnerability within this "siloed" approach is that each protection envelope within each silo is tailored to address a single-vector threat.

Today's threat environment is multi-vectored. A recent breach that compromised credit card data in the retail sector involved:

- Physical access *to*:
- The logical layer *via*:
- A facilities-managed piece of network-enabled equipment *utilizing*:
- A *compromised contractor credential*.

In the traditional model, who would own this breach?

In this example, all departments can claim some governance over their domains, yet the intruder was able to work *between domains* to accomplish the breach.

The exfiltration of credit card data once the intruder gained access to the network was ultimately the individual silo that broke down in this example, but adequate IAM discipline would have denied this access in the first place.

Convergence and integration within an empirical and cross-functional IAM is the only way to break down the silos and close the gaps between these individual domains to provide a true proactive defense in depth model.

The Case for Convergence

A converged and integrated IAM platform would consume real-time data from all domains (IT, security, HR and procurement / contract management) and parse it out to the respective sub-tier platforms for their use in the management of access rights and privileges. This integration would also be strengthened through a Single Sign On (SSO) identity being established for each individual who gains access so there is a single data point for revocation.

This data-management engine must be combined with robust and auditable business rules at each access approval endpoint to ensure only those rights and privileges that pertain to the individual are granted. Once access is granted, there also needs to be an equally robust credential lifecycle management engine to ensure physical and logical rights and privileges stay in cadence with everyone's changing roles and responsibilities within the organization.

From a strategic standpoint, this deployment would offer a dashboard of "green" buttons that create a more convenient workflow in the onboarding process. All departments that have governance can "green-light" an applicant for access within their domain. When all domains are "green", physical and logical credentials can be issued.

Outside the realm of convenience, a much more critical feature would allow any stakeholder to "red-light" an employee or contractor at any time. A "red-light" from any domain would immediately revoke credentials within all domains.

In a complex corporate environment, this revocation workflow can take days and can be a manual process of email notifications and manual systems administration. In a threat environment, you only have minutes, not days, to close gaps.

This level of integration is often deployed within the financial services sector, but any company that is tasked with the protection of sensitive client data or high-value internal intellectual property would benefit from adherence to this higher standard of identity protection. In addition, any company that aspires towards adherence to ISO 27001 or GDPR compliance needs to consider its overall IAM posture when embarking upon a compliance initiative.

At a tactical level, the actual implementation of the converged model can take many forms. There are comprehensive middleware solutions that can reside between all domains and deliver adequate convergence (at a price) to the organization. Some endpoints (logical access management platforms, physical security management platforms) offer integration and Application Programming Interface (API) products that can work in a cross-functional environment.

The optimal discovery and delivery model involves convening a cross-functional working group including the CISO, the CIO, the CSO, Legal, leaders from HR and Procurement / Contract Management and selected internal end-user groups to understand their needs, current deployments and the integration capabilities of their platforms in an environment where "we've always done it this way" is not allowed into the conversation. We worked through the development and deployment of this level of IAM and SSO enforcement for a global publicly-traded company within the entertainment industry and the input from all stakeholders was varied and compelling. The socialization of new business rules and workflows into established, long-held workflows presented challenges that needed to be overcome in both a group and individual setting.

The engagement of an independent third-party consultant at this strategic envisioning phase of the process can become a key enabler for a successful outcome. The consultant should be equally conversant across all domains and should be independent of any technology platforms deployed by the company.

Once all needs have been established and the capabilities of the current platforms have been identified, a matrix of potential solutions can be developed from the simple (manual data exchanges and updated business rules) to the complex (a complete migration to a third-party middleware platform) and a cost-benefit analysis for each can be forecast. This will drive a business case to senior leadership for adequate funding to implement a converged architecture to address the company's unique technology deployment and threat environment. We've prepared these business cases across a wide variety of sectors including finance, data centers, manufacturing, health care, pharmaceutical and software development.

A consultant can act as an interdepartmental go-between to ensure all domains are adequately protected, the solutions do not interfere with established workflows and the end-state environment can be utilized and managed by all stakeholders. The consultant would also act as a "force multiplier" to allow the initiative to be deployed without exhausting existing resources or onboarding interim internal headcount to project manage and deploy the solution.

Standing still is no longer an option

Standing still as an IAM posture is no longer an option. The traditional model for IAM may have checked the boxes within each domain owner's compliance checklist, but multi-vector threats have rendered these domain-centric security solutions inadequate to provide the defense today's companies require to address the evolving threat landscape.

Cross-departmental collaboration is required to envision, stratify, approve and deploy an integrated and converged IAM environment where threat mitigation is combined with ease of use to address the needs of each stakeholder organization that is impacted by the IAM solution.

Take-aways

- "Traditional" IAM provides protection and integrity *within* domains, not *between* domains
- Transactional communication and flat-file transfers cannot provide the immediate response to threats that today's environment dictates
- Converged IAM should be deployed as a convenience in the onboarding process
- Converged IAM should enforce immediate revocation across all domains
- Stakeholders should consider all options and levels of complexity of converged solutions to find a program that is the best fit for their enterprise
- The needs of all stakeholders should be communicated and considered in an open collaboration environment
- A trusted third-party consultant should be considered in the need's assessment, business case development and implementation phases of a successful converged IAM initiative.

MATTHEW WHARTON SR.

President, Strategic Accounts

Matthew Wharton serves as president for strategic accounts. Mr. Wharton is a career security professional with more than 35 years of experience leading security consulting and integration firms. He designs solutions from "The Owner's Perspective" with improved recommendations that meet regulatory and fiscal requirements and transform internal functions from cost centers to sources for corporate investment that deliver increased integrity to the enterprise and enhance shareholder value.