# Understanding the Business Value of Authorization

Supported by The Cyber Hut

plainID

# Understanding Business Outcomes

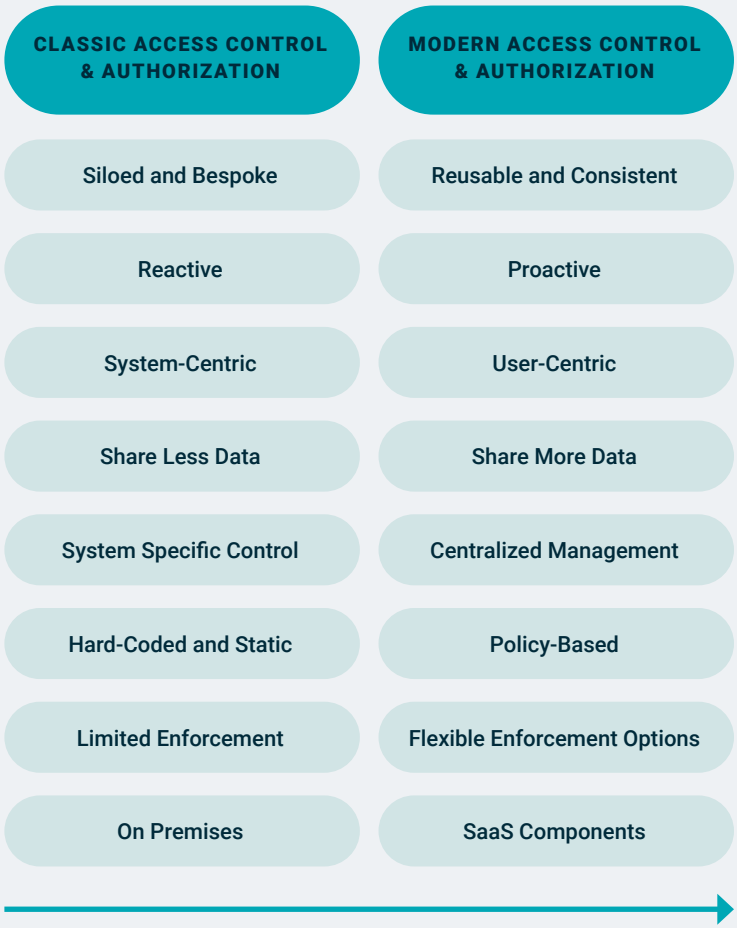
Authorization has historically — and in line with the broader identity and access management sector — been driven by operational constraints. This has often resulted in access control solutions that are reactive to technical challenges, heavily system centric and tactical in their feature evolution.

Today access control can be seen as a business enabler — allowing those not necessarily involved in the day-to-day access control life-cycle to benefit from the services it provides.

Organizations want to share more data to more organizations, within teams, across teams and to supply chain partners. Yet, they want to do this in a secure, compliant and user-friendly way.

The successful outcomes for authorization are becoming varied and distributed and benefit new and emerging stakeholders within the organizational landscape.

It is important to be able to map technical controls and performance metrics, with outcomes that not only impact the organization, but can also be communicated to a range of non-technical stakeholders. This helps to monitor the performance and productivity of a vendor and allows total cost of ownership and return on investment to be calculated and future authorization funding analyzed.



## Operations Optimization

Improving the productivity and efficiency of operations is a key success criteria for historical IT investment. Employee productivity must at worst not be impacted and at best, improved inline with technology change.

| BUSINESS OUTCOME | DELIVERED BY |
|---|---|
| **Improved Employee Productivity** | **Reduced Access Request Fulfillment Speed** — Essentially speeding up the time it takes to associate a subject (identity) to an object (piece of data, process, task) with the necessary permissions. |
| **Improved Security Administration** | **Reducing Excessive Permissions** — By aligning users and services more succinctly via policy, permission management and removal becomes less burdensome. |
| **Improved Compliance Performance** | **Knowing Who Has Access to What (and Why)** — By leveraging a more holistic, observable and policy-based approach to access control, reporting and insights can be improved. |

## Improved Business Agility

Whilst authorization may not immediately be linked with higher-level business functions, it is becoming increasingly clear that the secure collection, handling and sharing of important information and data can improve collaboration across both the supply chain and application management functions.

| BUSINESS OUTCOME | DELIVERED BY |
|---|---|
| **Faster Business Partner Integration** | **Improving Data Sharing Capabilities** — By making it easier to share information, by data owners and administrators with trusted business partner identities. |
| **Improved Supply Chain Management** | **Securely Opening More APIs** — The API economy allows for improved integration options across both the upstream and downstream ecosystems. |
| **Improved Competitive Responsiveness** | **Reducing Application Release Time** — A more programmatic and external access control framework creates reusable components that can speed up application release times. |

## Improved Security Performance

Security metrics are becoming a critical tool in the spend profile of the CISO and senior security management team. Cyber security metrics for the coverage, performance and effectiveness of security helps to understand the return on investment and the level of support of the controls with respect to the risk management process. Authorization has a key role in improving the security control landscape.

| BUSINESS OUTCOME | DELIVERED BY |
|---|---|
| **Reducing PII Theft** | **Securely Protecting APIs** — The security of APIs at both the north/south entry point and east/west intra-service communications layer is key in preventing data loss. |
| **Reducing IP Theft** | **Providing Secure B2E Controls** — The theft of intellectual property relies heavily on excessive permissions, a lack of visibility and hard-coded permissions. Movements to a more dynamic policy-led approach can help reduce this threat. |
| **Improved Audit Reporting** | **Knowing Who Has Access to What** — Reporting from a compliance perspective is often compulsory, but can be turned into a security productivity enhancer through the ability to visibly see, report and analyze which users have access to which systems — and why. Making audit insight and performance a direct benefit. |

## Reduced Business Friction

A key issue many CISOs face is knowing how to allocate finite resources — such as people, license spend and effort — and how to do so against an ever-growing list of security threats. However, this battle needs to be completed under the continuous eye of the business — where security controls that are too inhibitive or introduce and amplify friction will not only be unacceptable but often avoided by end users if they are implemented.

| BUSINESS OUTCOME | DELIVERED BY |
|---|---|
| **Improved Employee Onboarding** | **Reusable Policy-Based Access** — By allocating users with the correct access when they join an organization, the speed at which they can start working is greatly expedited. The use of modular policies to allocate access (often incorporating RBAC, ABAC and contextual information) supports this approach. |
| **Optimized Team Working** | **Improved Line of Business Access Management** — By providing non-technical line of business managers with the ability to perform permission management (users to objects) or be part of the policy design process means the right staff members get the right access they need. |
| **Optimized Hybrid Working** | **Improved Intra-Team Data Sharing** — Data collaboration is a key component of a modern enterprise's ability to solve complex problems in an agile and timely fashion. The ability to share to other teams (even from other organizations) can be designed using dynamic policy-based access control that contains identity data, context and a broad array of data assets. |

## ABOUT PLAINID

PlainID is The Identity Security Company™ We help identity-centric enterprises defend themselves from adversaries who use identity-based attacks. Our Identity Security Posture Management Platform provides Identity Insights, SaaS Authorization Management, and Dynamic Authorization Services to create identity-centric security across SaaS, APIs, microservices, apps, and data powered by policy-based access control. Visit PlainID.com for more information.