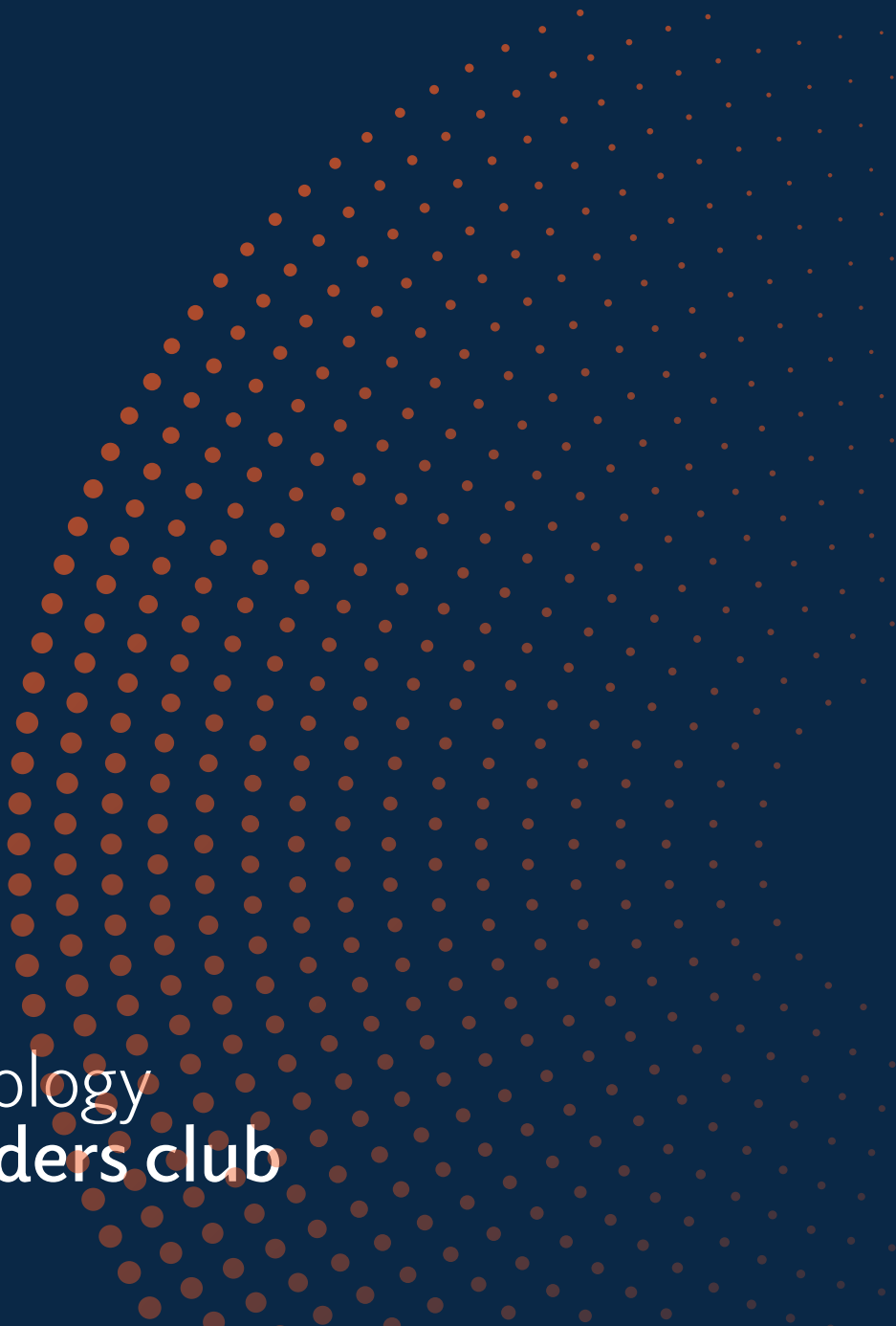
KeyData | SailPoint

Identity is the New Security Perimeter

Whitepaper – 7th July 2021



rela8 group

technology leaders club

Identity is the New Security Perimeter

In an increasingly digital world, safeguarding critical infrastructure starts with strong identity security. Improved business processes need effective identity governance. By automating and accelerating how you manage a user's identity entitlements systems, data, and cloud services, you can gain unmatched visibility and intelligence.

We hosted a roundtable of security architects, IT, networks and security operations directors, process and innovation professionals to take a deeper look at:

- The relationship between IT modernization and identity security
- Ensuring that user access remains appropriate and relevant
- The need to grant and manage access for non-employees, contractors and business partners

With attendees from sectors as diverse as energy regulators, finance, government, construction and the law, the discussion was a journey of discovery for many. Here is what they had to say.

Rela8 Group's Technology Leaders Club roundtables are held under the Chatham House Rule. Names, organizations and some anecdotes have been withheld to protect privacy.

About SailPoint and KeyData

Together, KeyData Associates and SailPoint are on a mission to help businesses securely access technology with identity security solutions.

KeyData has been delivering Identity and Access Management (IAM) services since 2005. KeyData is a trusted advisor, guiding clients of all sizes through IAM strategy, governance, processes redesign, role-based access control (RBAC), technology selection and implementation, as well as IAM managed services and training.

SailPoint is the leader in identity security for the cloud enterprise. Its identity security solutions secure and enable thousands of companies worldwide, giving customers unmatched visibility into the entirety of their digital workforce, ensuring workers have the right access to do their job.

KeyData | SailPoint

Many of us can remember when the perimeter of our organization was visible, contained, and defendable by a firewall. That has all changed. Remote working, the cloud, BYOD, a transient workforce, contractors and third-parties all make today's situation more fluid and complex. Every access point into our systems, networks or data presents a potential risk. In most cases primary access points are people, whether employees, contractors, or even customers. Making sure the right people have access to the right things for the right reason and at the right time is governed by identity access management.

For security in a cloud environment, identity is everything.

The issues around identity access management cover many levels. Big issues like trust, privacy, and identity. Are you who you say you are? Can you verify it? How much information should I hold on you? Who can see it? Balancing these big issues with the need to protect an organization's assets and reputation needs a considered approach.

IT modernization and identity security

As enterprises move forward with digital transformation initiatives, more and more systems are being deployed to the cloud. Multiple SaaS applications can mean multiple identities. As individuals do more and access more, their identity becomes spread out and is more difficult to manage.

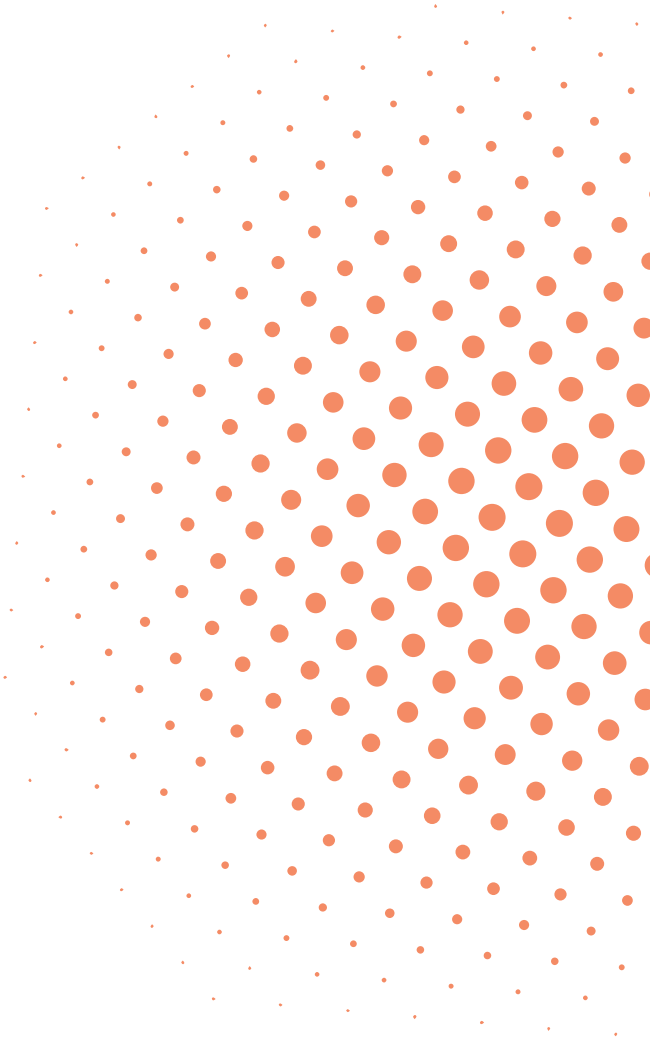
Regardless of the size of a business, or a department, managing identity and access is riddled with complexity. A strong foundation is the best starting point for trying to simplify this complexity and make it manageable.

Initial questions to answer include: How do I know who has access to what? Should they have access? Understanding who is in the organization, what they do and what access they need to do their jobs are the building blocks for an identity infrastructure.

Appropriate and relevant access

In business, data is currency. It is important to know what your data is, its value to your organization and where it is. Knowing what resides inside applications, ERP systems and databases is one nut to crack. A tougher one is the unstructured data within files, messages, PDFs, scanned documents, etc. It is often not IT or security's role to decide what is important within this data and who has access to it.

Many organizations assign ownership to the business unit to determine who has access to it and put in place access controls. For example, if someone only needs access once a month or twice a year, do they need access at other times? These situations are ripe for breaches.



Granting and withdrawing access

When a new employee joins a company, their hiring manager will ensure they have access to the right systems to do their job. Oftentimes, their contract will include data privacy, IP, security clauses, etc. All can be neatly managed by HR. More difficult to control is the use of consultants, third-party contractors, temps, etc. that make up the transient workforce. When contracts end, or an employee stops working on a project, whose responsibility is it to disable access? Or rather, whose responsibility is it to inform IT or Security to disable access? It is not always clear cut. The worst scenario is that they go to work for a competitor and still have access to your systems and data.

Similar problems can occur with employees who have decided to leave and download information ahead of their departure. Activity monitoring and User Behaviour Analytics (UBA) can trigger alerts that something is happening that needs attention.

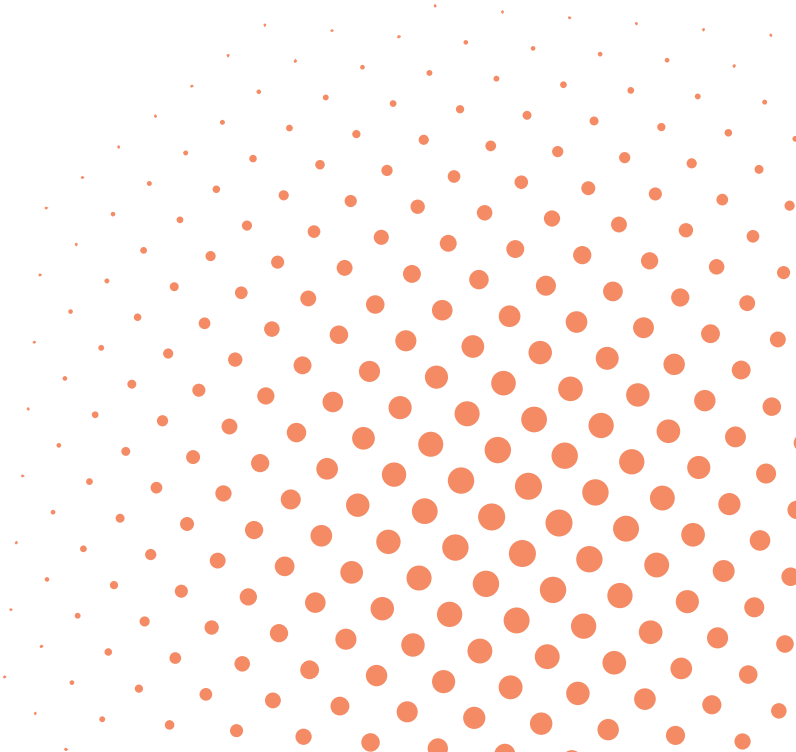
In these cases, access should be linked to Identity Lifecycle Management, managed by HR.

Changing mindsets

Ultimately, the heart of the relationship between IT modernization and identity is the need to protect information. The challenge can be cultural. Unless people see information as an asset, they copy data to a memory stick or export it to a .csv file to work on at home for convenience. Once people treat it as a company asset, and classify or tag it correctly, they take fewer liberties with it. One delegate said, "in security, the hardest thing to do is changing people's minds and how they do things. It's much easier to put technology in place than convince someone to change the way they work."

Without doubt, identity plays a central role in our new ways of working and in digital transformation; in our move to the cloud. There are tools available to solve, automate and streamline the challenge. Using them effectively, again, needs that core understanding of who has access to what, why and when. Is identity the new perimeter, or is it really the core?

> For security in a cloud environment, identity is everything.



KeyData | SailPoint