able

Technology whitepaper

Implementing zero trust architecture in Higher Education

Abstract

The digitisation of the teaching, research, and administration within universities has brought immense benefits to Higher Education. However, it has also introduced new threats to the organisation that can be impossible to predict, difficult to contain, and costly to remediate. This whitepaper introduces zero trust architecture in the context of Higher Education and explains how an identity-centric security strategy can help to protect the institution from these threats.

Document Date: March 2021

Author: Josh Howlett

new era. TECHNOLOGY

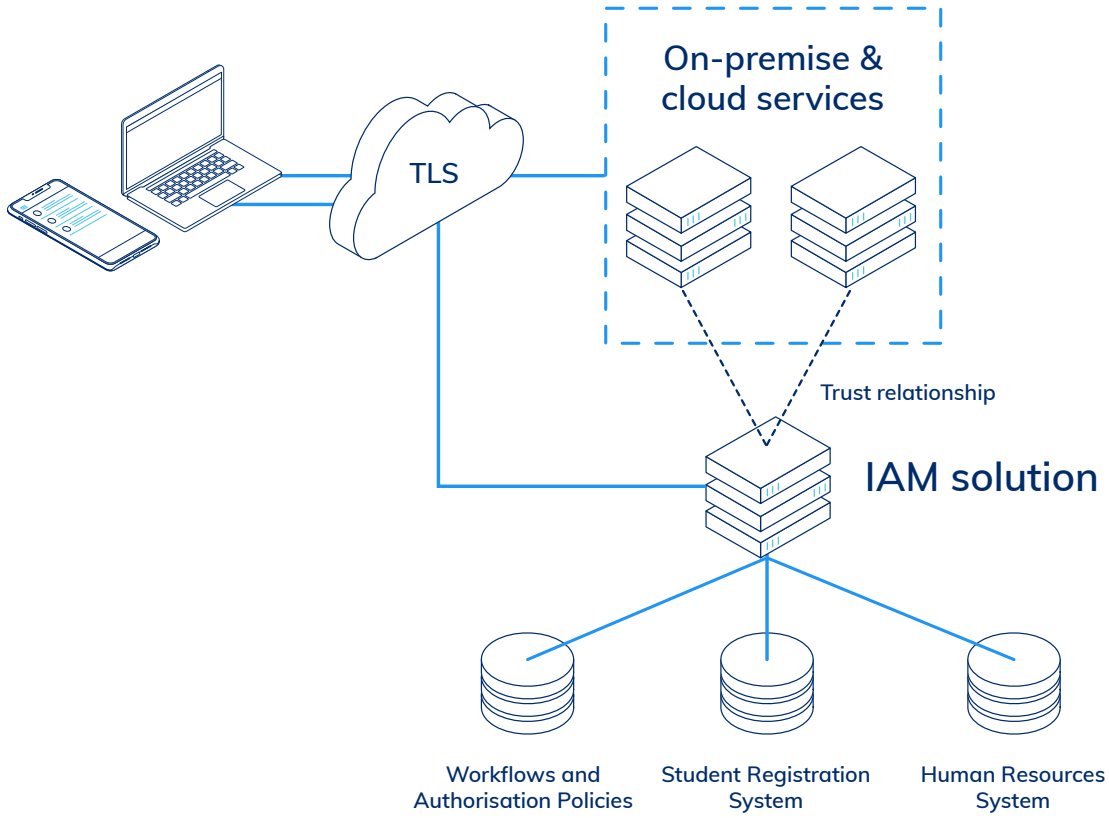
Introducing zero trust architecture

Until relatively recently, perimeter-based network security models were considered the most effective approaches to protecting an organisation's assets.

However, since 2019 the UK's National Cyber Security Centre (NSCS) has recommended that Enterprise architects consider a 'zero trust' approach to IT architecture.

The early driver for zero trust architectures was ecommerce, where it is impossible to assume safe passage of data between merchant and consumer across the internet. This led to the ubiquitous deployment of browser-based authentication and encryption, negating the need for either party to concern themselves about the integrity of the network.

Zero trust architecture derives its name from its core assumption that the network is already compromised and cannot be trusted. Instead, trust is established at application layer, within encrypted sessions between mutually authenticated endpoints. Consequently, the security of the session does not rely on the presence of a trusted network. Instead, it relies on the integrity of the endpoint and user identities.



The principles of zero trust architecture

Identity and authentication, therefore, are key to zero trust architecture. In fact, four of the six “zero trust principles” highlighted by the NCSC are directly related to identity and access management (IAM).

A single strong source of identity

A consistent, overarching system of identity enables applications to reliably identify users. Users’ identities must be based on the most authoritative sources of data, ensuring that users’ digital identities keep in step with reality.

User authentication

Users must prove their identity by authenticating when accessing any system. Single sign on (SSO) can be used to avoid repeating authentication; and multifactor authentication (MFA) can be used to secure users’ SSO credentials from misuse, if compromised.

Access control policies within an application

Recent applications that support modern approaches to identity can be exposed directly to users. Access decisions are taken by the application based on user information provided by the institution’s authentication system at time of access.

Authorisation policies to access an application

Legacy applications that do not support modern approaches to identity can be segregated behind an SSO-enabled portal. The portal is used to manage authorisation policies and enforce them, based on users’ authenticated identities.

The other two principles (machine authentication and machine integrity) are closely aligned to these, being concerned with the identity of devices (rather than users) and authorisation based on software configuration (rather than a user’s entitlements).

Planning your institution's zero trust strategy

The principles of zero trust architecture are often recognisable within many institutions' Enterprise architectures today. This owes itself, in part, to the aspiration of the pioneers of academic networking to provide a service offering early users unhindered but authenticated access to campus services (it is no coincidence that Kerberos, the core authentication technology within Active Directory, was developed and is still maintained by a team within the IT services department at MIT).

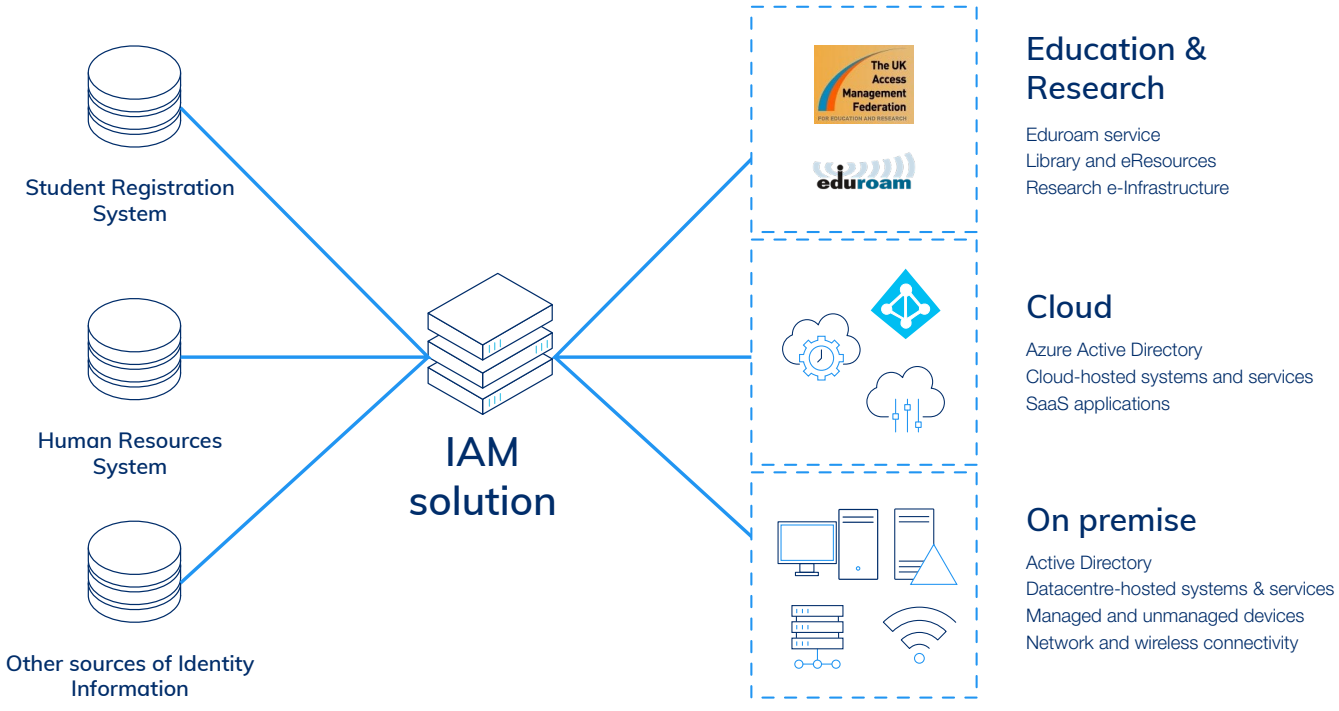
Subsequent innovations, such as Eduroam, Shibboleth, and Moonshot, which facilitate access to WiFi, academic content, and research services respectively, had similar goals. As a result, these have led to the deployment of the technologies, such as EAP and SAML, that are central to zero trust.

The good news, therefore, is that your institution may be more prepared for zero trust architecture than you might expect. Nonetheless it still requires a conscious pivot to rethink security through the lens of identity rather than the network.

While the detail will vary between institutions, your planning should consider the following key issues:

- a full inventory and understanding of the user types and roles within the institution and the processes concerned with the registration and maintenance of the most authoritative sources of information, such as the human resources and student registration systems, and the privileges accorded to those user types and roles needed to grant access to services.
- an IAM solution that can create and maintain the single strong source of identity based on the authoritative sources of information, authenticate users, and authorise access or provision authorisation information to services.
- an Enterprise applications and networking architecture that can provision access to services based on authenticated and authorised user identities, and other contextual or compliance information, such as machine health; with the network focussing on connecting users to services, efficiently and effectively, and the IAM solution on security policy enforcement.

Finally, because zero trust touches all aspects of an institution's digital architecture, it should be treated strategically, joining together a range of activities across the institution, rather than as a discrete project.



Choosing and implementing your IAM solution

Many institutions are still using their own bespoke IAM solutions. These can be difficult to maintain and develop being reliant on just one- or two-people's knowledge. In recent years, some institutions have migrated to commercial products, but these implementations can falter when these products lack the flexibility needed to address the requirements of Higher Education.

Every institution is different, but successful IAM projects and solutions tend to have the following in common:

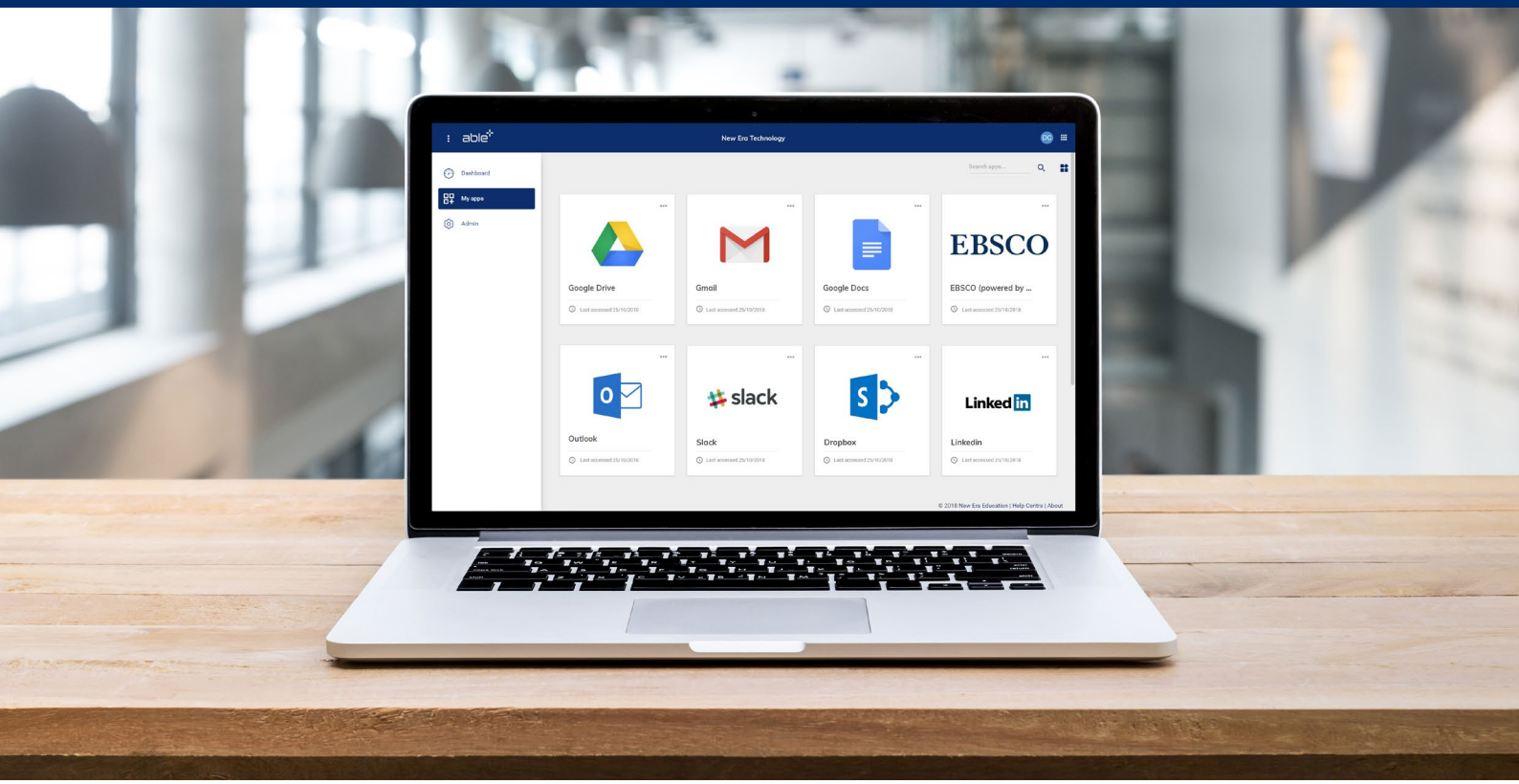
- strong and inclusive project governance that brings together, consults, and aligns the relevant stakeholders across the university.
- a full understanding of users' identity lifecycle journeys and especially the 'long tail' of so-called 'edge' cases, and how their entitlements change along these journeys.
- the organisational and technical capacity to delegate management, so that IAM happens nearest to the user; and
- the technical ability to integrate with all the relevant systems and services, to maximise return on investment, the value from 'network effects', and the opportunity for automation.

About Able+

Able+ is an IAM solution that transforms user productivity by enabling simple and secure single sign-on access to applications and services using corporate or social identities. It's also an identity governance & administration (IGA) solution that makes it easy to align your IAM with organisational policies and processes. The powerful workflow engine and visual workflow editor can bring together different sources of identity data to create a single source of truth. Delivered as a managed service, Able+ can be operated from your choice of public cloud, private, or hybrid infrastructure.

Summary

Zero trust architecture shifts the focus from the network to identity, delivering more secure outcomes that are centred on the end user's needs. Implementing a zero trust architecture requires rethinking and retooling some aspects of provision, but most universities are already well-positioned for the transition. The key consideration is the IAM solution that underpins the identity and authentication requirements of zero trust, and its integration within the institution's digital architecture.



03334 559424
info@neweratech.co.uk • neweratech.co.uk

Powered by new era TECHNOLOGY