TOP 5 PROBLEMATIC APPLICATIONS FOR SECURING DIGITAL TRANSFORMATION

Cyolo

It can be hard to let go of tried and tested enterprise applications. In particular, legacy applications are often intrinsically integrated into business processes, making them difficult to replace or upgrade.

In fact, by 2025, Gartner expects that 90% of current applications will still be in use and have insufficient modernization investment to take them forward.

At the same time, digital transformation is changing the face of the enterprise as networks expand to encompass remote employees, supply chains, cloud applications, and edge devices. Application ecosystems are changing along with the digitally transformed business, but legacy applications cannot always fall into line. Security gaps can sneak in when problematic legacy applications lack support for modern security protocols and standards.

NCCGroup found that 45% of organizations inherited legacy security issues during a transformation project resulting in a downgraded security posture. This insidious problem increases cyber risk and results in non-compliance with current regulations.

LEGACY APP 1

ORACLE

Oracle has promised continued support for its legacy applications, including E-Business Suite (EBS), PeopleSoft, and WebLogic. This is great for companies who want to move from these applications during a digital transformation project but need to proceed slowly. However, it is unlikely that Oracle will update and innovate around these products; this means that support for improvements in access control and zero-trust enablement are unlikely to be a priority for Oracle.

SECURITY PROBLEMS

EBS does not have native support for single sign on (SSO); PeopleSoft does not support identity protocols, security assertion markup language (SAML), or open ID connect (OIDC), limiting its use in modern use cases, including federation. An organization must modernize access to Oracle legacy applications using third-party platforms.

LEGACY APP 2

Microsoft Sharepoint

On-premises SharePoint supports certain types of businesses, for example, heavily regulated industries, where cloud collaboration is seen as less secure. For organizations such as these, security is crucial, and control of data access is an essential part of regulatory compliance and data protection. However, as Microsoft has a strategic focus on cloud applications with Office 365 at its core, legacy on-prem instances of SharePoint may not maintain modern access control options.

SECURITY PROBLEMS

SharePoint for on-premises deployments will certainly lag on cloud-based updates. While the latest version of SharePoint Server Subscription Edition has some modernization features added to help with authentication, including support for OIDC, turning these features on require a specialist and can be complex to achieve. Expansion may be required to fully support a zero-trust approach to controlling access to SharePoint-held resources. Microsoft recommends taking a zero-trust approach to ensure robust SharePoint access control.

LEGACY APP 3

SAP

SAP systems are widely deployed and support many business-critical applications. Some of these deployments have generic user, name, and password (UN&P) that multiple people will use. While this is a security challenge, it is not malicious because the end-users need to get their work done and this insecure set up is the best way to get the job done. Without identity visibility, it is impossible to track which specific user accesses the application making this application a nightmare for compliance.

SECURITY PROBLEMS

Legacy SAP deployments can result in a lack of cohesion when it comes to controlling access to critical business resources. Integration with a third-party identity-centric access control platform can prevent unauthorized access and enforce least privilege access rights as well as prevent lateral movement that leads to control of SAP systems.

LEGACY APP 4

MAINFRAMES

You would be surprised how many are still out there! Research has found that 44 out of the top 50 banks, healthcare, and government agencies rely on IBM Z Mainframes for business-critical applications. Mainframes may cause security problems during digital transformation as business-critical data must be available to cloud-connected users.

SECURITY PROBLEMS

Mainframes are often based on decades-old technology. These mainframes are not agile enough to easily support modern identity, security protocols, and standards. Mainframes need an identity and access control strategy, as many remain critical to a business.

LEGACY APP 5

HOMEGROWN APPS

Homegrown applications may have been kicking around an enterprise for years, but the original coders are long gone. A lack of expertise in secure application coding can lead to inherent vulnerabilities in homegrown apps. In addition, homegrown legacy apps are unlikely to have included support for modern identity and access management needs, such as secure remote access, zero-trust identity checks, multi-factor authentication (MFA), and single sign-on (SSO). Support for modern identity protocols is also a specialist area of knowledge, making homegrown apps unlikely to support modern access control requirements.

SECURITY PROBLEMS

Homegrown legacy applications will need an agile solution that can bridge the gap between an older code base, human users, and modern zero-trust environment architectures. The best solution is a zero-trust access platform, such as Cyolo's, than can overlay MFA capability with legacy applications without compromising the user access experience.

Cyolo understands the challenges of securing legacy and homegrown applications.

We designed our zero-trust access platform for all systems and applications, including those that do not natively support modern secure access control options.

With Cyolo, the applications you've long depended on can continue to empower your business without adding risk or increasing the attack surface for bad actors.

Five recommendations to ensure that legacy applications are as secure as modern systems:

1. KNOW YOUR LEGACY

Start with a thorough accounting of all systems and applications to identify which applications will cause your proposed infrastructure security issues. Extend this audit to include suppliers' legacy applications to prevent them from disrupting your digital transformation program. This audit will lead to the next major security exercise.

2. CREATE A SECURITY IMPROVEMENT PLAN (SIP)

According to a Ponemon report, 82% of organizations have experienced at least one data breach during digital transformation. A security improvement plan (SIP) is a series of guidelines that develop procedures to reduce risk and maintain regulatory compliance and should have specific actions for challenging applications. Digitizing operational processes within a hybrid (cloud and on-prem) environment makes the smooth transition a security challenge. By referring to the SIP an organization can minimize the risk associated with digital transformation projects that include legacy applications.

3. MOVE TO A ZERO TRUST MODEL

A zero-trust model that incorporates your legacy applications is the best practice for modern identity authentication. Your digital transformation initiative will likely involve a hybrid environment. To ensure that data and resources remain secure, you must prioritize access control by implementing multi-factor authentication (MFA) and standardization of password quality across your organization, including external consultants, freelancers, and other third-party users.

4. MAINTAIN COMPLIANCE

The need to comply with regulatory or insurance requirements is a common driver of the shift to a zero-trust framework. As you transform the security model, ensure that your regulatory obligations continue and compliance is maintained. While many systems will easily fit the model, some will not. Carry out risk assessments and Privacy Impact Assessments that include legacy application access. Zero-trust access solutions that overlay modern authentication and authorization protocols will ensure that security and privacy compliance are maintained.

5. IMPLEMENT AN IDENTITY-CENTRIC ZERO TRUST PLATFORM

A zero-trust access platform will secure and administer access to your 'problematic' applications. For example, there may be a long lead time for a legacy application to move from on-prem to cloud and even longer for the deployment of a modern replacement. During this time, security gaps must be controlled. Using a zero-trust access platform, you can overlay access control and security measures, including MFA, SSO, least privilege, auditing, and Just-in-time (JIT) access for third-party vendors and other high-risk users.

THE CYOLO APPROACH TO PROBLEMATIC APPLICATIONS

The Cyolo zero-trust access platform provides secure and seamless access for all users to all applications, including those that present challenges to modern authentication methods.

The Cyolo Identity Access Controller (IDAC) is placed on-site and integrates with your existing identity infrastructure and connects to your network resources and applications. In this model, a user will continue to use their existing workflows, but will first be authenticated by the Cyolo IDAC, which uses the existing identity infrastructure to validate identity. Because the IDAC does not send traffic outside the company network, nor does it store any access information, there is no risk of compromise for users, applications, or services.

CONCLUSION

While digital transformation has greatly improved organizational security in many ways, significant gaps remain and must be addressed. With a firm understanding of what problematic applications or services exist in your environment, the work of applying modern security methods to them can begin. The desired balance between user experience and security controls is ultimately achievable, even for business-critical systems that historically do not support modern identity authentication.

Cyolo exists to help organizations thrive by securely connecting people to their work and bringing modern, identity-based access to all applications and systems, even the ones existing tools struggle to secure. Founded by a CISO and two ethical hackers, Cyolo empowers you to connect anyone from anywhere with the confidence that the entire digital system is protected.

Cyolo

cyolo.io