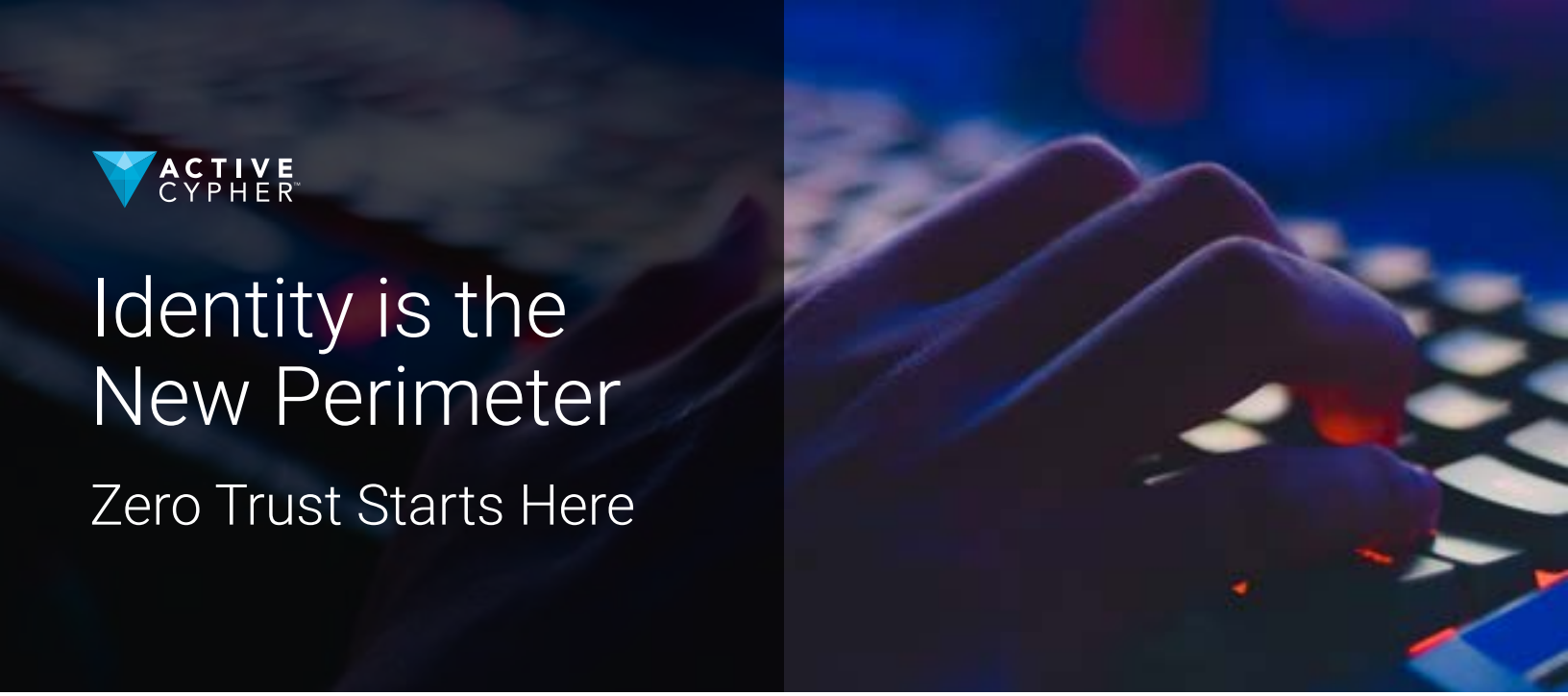


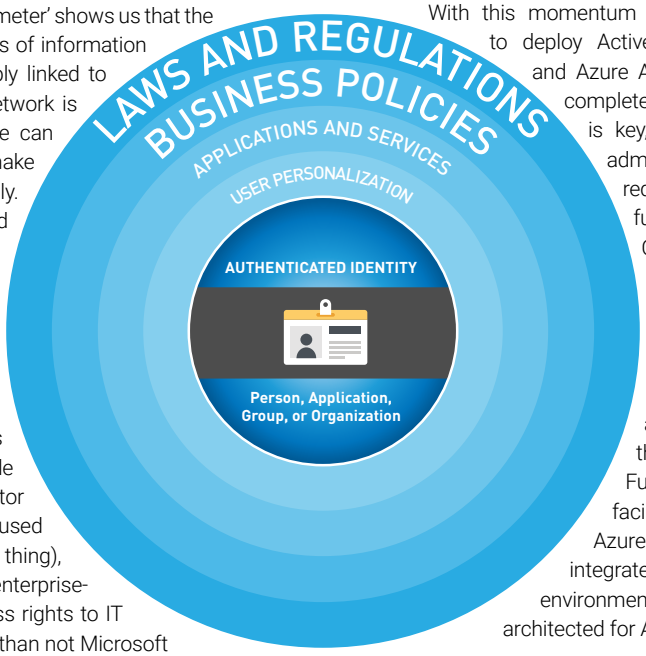
Identity is the New Perimeter

Zero Trust Starts Here

File Encryption and IAM Elegantly Intertwined

The proliferation of applications, devices (personal and at work) and networks (social, work, service provider, etc.) have made traditional forms of information protection increasingly difficult to enforce. Firewalls today have so many holes opened in them that properly managing and monitoring network and system access has become nearly impossible.

The notion of the 'disappearing security perimeter' shows us that the common denominator across most aspects of information protection is identity. An identity inextricably linked to a person, device, application, system or network is today the most dependable 'perimeter' we can rely upon to determine what and how to make information available properly and securely. Basically, it boils down to 'who are you and what can you do?'



The concept of 'identity as the new perimeter' is taken even further in the emerging Zero Trust (ZT) model, where the most critical facet of security is knowing who (or what) the end user is, what device they are using to access systems and files and where they are connecting from. While adjunct technologies such as Multi Factor Authentication (MFA) can and should be used to more securely authenticate a person (or thing), the underlying technology that supports enterprise-class authentication and subsequent access rights to IT resources (i.e., authorization) is more often than not Microsoft Active Directory (AD) – whether on- premise or running as Azure Active Directory (AAD) in the Microsoft cloud. Understanding that Microsoft Windows and Active Directory are deployed as the IAM, network operating system and directory infrastructure for most organizations around the globe, we can determine that AD/AAD is trusted authentication and authorization platform most ubiquitously able to support the Zero Trust framework.

Furthermore, Microsoft has established Azure as its global cloud platform and strongly encourages its customers to migrate their on-premise deployments of Active Directory (AD), Office 365, SharePoint, etc., to Azure. In the past few years, most of its customers have migrated to Azure (or are in the process of doing so) and this major shift to its multi-tenant Azure cloud continues at a rapid pace. Coupled with this, Microsoft has begun to move towards a 'passwordless' future, investing substantially in the development and deployment of MFA across its Azure-centric customer base.

With this momentum well underway, now is the perfect time to deploy ActiveCypher encryption capabilities with AD and Azure AD because the solution was designed to completely leverage AD/AAD security groups. This is key, because there is virtually no additional administrative overhead and governance required to enable consistent, secure and fully recoverable file encryption using Active Cypher – it simply extends file encryption to the AD/AAD IAM infrastructure you already have in place. Recoverability is simple and error-proof because key management functions are deployed in the client's Azure Cloud Subscription with all the oversight, auditing, scaling and continuity planning that is available to your own subscription. Furthermore, Active Cypher's 'AC Detect' tool facilitates migration from on-premise AD to Azure AD by helping identify security groups for integrated file encryption. This means an existing AD environment doesn't have to be pristine or previously re-architected for Azure AD migration.

The current regulatory compliance and intellectual property protection requirements remain front-and-center for all of us. As the traditional enterprise security barriers continue to morph into perimeter-less, zero trust models, the elegance and effectiveness of Active Cypher's file encryption solution becomes the best way augment your AD- centric IAM environment with fully integrated file encryption.