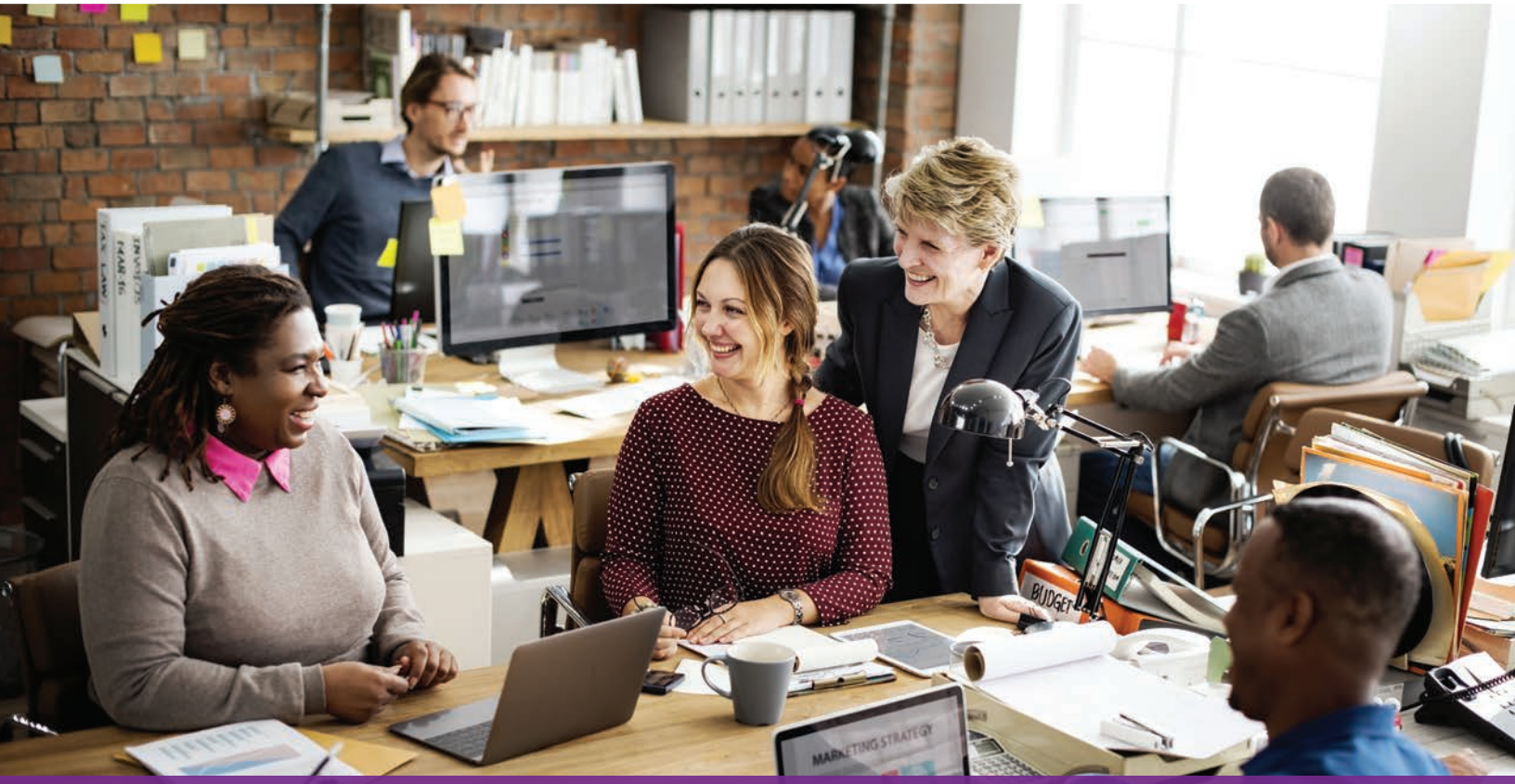

SECURE SSO TO OFFICE 365 & OTHER CLOUD APPLICATIONS WITH A CLOUD-BASED AUTHENTICATION SOLUTION

ADVICE FOR SIMPLIFYING & SECURING YOUR DEPLOYMENT

Evan O'Regan, Director of Product Management for Authentication

Entrust Datacard™

SECURING OFFICE 365 AND OTHER CLOUD SERVICES

Microsoft® Office 365™ continues to lengthen its lead as the world's top enterprise cloud service. Nearly one-in-four employees in Fortune 500 companies are active on Office 365 — and more than 90% of those large enterprises currently have more than 100 active users. Users are clearly becoming more reliant on Office 365, as usage grew at a rate of more than 300% in 2016.

The rapid adoption of Office 365 means that work created using the Microsoft product contains a large amount of the business world's sensitive information. In fact, in most enterprises using Office 365, more than half of that highly valuable information — including business plans, sales data, product designs, M&A details and financial forecasts — is contained within Excel, PowerPoint, Word, Outlook and other Microsoft software.

Salesforce.com, Box and Slack are also gaining market share and moving quickly in this competitive market. But Office 365 is clearly the mostly commonly deployed cloud service from a market share perspective, so securing the information created with its products has emerged as a primary concern for CSOs, CIOs, IT departments and other C-level executives.

THE EVOLVING COMPLEXITY OF SECURITY AND ENABLEMENT

Despite the best efforts of leading cloud service providers, including Microsoft, Salesforce.com, Box and Slack, enterprises building out digital business infrastructures are under continuous attack from an increasing number of internal, external and self-propagating threats. Ransomware worms, evolving phishing schemes, sophisticated IoT hacks and dark web "attack-as-a-service" capabilities challenge the often held notion that high-assurance security isn't a business imperative.

TRANSITIONING TO THE CLOUD

A COMPETITIVE NECESSITY

"By 2019, **40% of IDaaS IMPLEMENTATIONS** will replace on-premises IAM implementations, **up from 10% today.**[1]"

75% of **U.S. and EMEA manufacturers** have developed **intelligent products**[2]

More than **65%** of **C-level execs** view **digital transformation** as a **matter of survival**[3]

Nearly 9-in-10 CEOs view **cloud-based infrastructure** as the **key to growth**[2]

Enterprises also face threats from bad internal behaviors, ranging from excessive provisioning to employees taking data with them as they leave to join competitors. Also, as more customers and partners are connected to enterprise ecosystems, and as more core business assets and processes are transferred from legacy or on-premises servers to the cloud, the sheer number of endpoints elevates every enterprise into the high-assurance security space.

From an enablement perspective, deploying Office 365 is moving well beyond the goal of end-user satisfaction. Because Office 365 offers content sharing tools, calendars, email and other apps that connect authorized users, it is becoming foundational for the lifeblood of the enterprise brand: collaboration and innovation. As more and more enterprises deploy digital business infrastructures, market share threats from both traditional and unexpected competitors make it critical that users not only leverage cloud-based apps, but that they engage them with proficiency and gain measurable competitive advantages.

MANAGING IDENTITIES BEYOND OFFICE 365

Most enterprises deploying Office 365 have on-premises applications and use Active Directory to manage identities. One approach is to synchronize identity between your on-premises server and Azure Active Directory. This allows the user to continue with on-premises management while user accounts and passwords get synchronized in the cloud. However, it does not give you the advantages of single sign-on (SSO), which is clearly a driver of user adoption and productivity.

Achieving SSO requires federating your identities. Office 365 promotes Active Directory Federated Services (ADFS) as the answer, but it only creates another silo of identities. Without SSO, this breaks down the moment you introduce any other cloud-based app into the enterprise.

Clearly, getting the most value out of your Office 365 investment is dependent on it running well with all your other enterprise apps. Also, nearly every enterprise will be supporting a long list of on-prem apps that will require a flexible authentication approach. These apps' focus on solving their own authentication challenges – not uniting your enterprise ecosystem or improving your user experience. Since it is not realistic to expect that all apps will be cloud based or part of the Office 365 suite, a more effective path is to choose a third-party cloud-based authentication solution that can support Office 365 and additional cloud-based apps.

RECOMMENDATIONS FOR DEPLOYING CLOUD-BASED AUTHENTICATION

ACHIEVING SUCCESS: USING SSO FOR AUTHENTICATION

User experience is key to success. Empowering your authorized users to fully leverage Office 365 and other cloud services requires simplicity. For Office 365 in particular, this can be an overwhelming challenge simply because of the volume of clients included — with desktop versions of Word, PowerPoint, Excel, Outlook and more. There are also web-based versions of most clients to accommodate. Deployments also have to consider web and native apps for iOS, Android, Windows and other mobile environments. Enabling secure yet frictionless experiences across all of these environments presents a formidable challenge. A flexible authentication service with true SSO capabilities is essential. Improving user experience with office 365 depends on getting these points right:

Highly Efficient Provisioning

Choosing an authentication cloud service that simplifies the Office 365 provisioning process is critical. Well-designed solutions allow IT administrators to set up new users automatically if they already exist in Active Directory (AD) or a Lightweight Directory Access Protocol (LDAP) store. With the right cloud service, users can simply try to log in for the first time to Office 365, and the authentication cloud service will automatically check user credentials against AD or LDAP. The new user profile is created automatically and access is granted immediately. The most efficient authentication cloud services will also automate downstream access to other apps using this same process.

A Complete Approach to Deprovisioning

The right authentication cloud solution will enable single-step deprovisioning when employees leave the organization or are denied access to Office 365 clients for other reasons. It should be possible for passwords to be changed or deleted with one click. However, effective deprovisioning includes remotely wiping the user's devices, granting mailbox access to authorized administrators, and searching mailboxes and other folders for relevant documents that should be retained by the enterprise.

Robust Adaptive Authentication Options

Whether it's for the deployment of Office 365 or any other cloud service, be sure to look for authentication cloud services that offer evolving adaptive authentication capabilities. While Office 365 may work for some companies today, your auth solution should be ready to evolve with the needs of your users. The right solution will integrate contextual data from all of the user's devices, collect current and historical location data and analyze a wide range of user behaviors. Users will be prompted for authentication and challenged only when necessary. Most often, this process will go unnoticed by authorized users.

Streamline BYOD Provisioning

Mobile employees expect to be able to load their calendars and email onto their own smartphones and tablets. And most enterprises are allowing this BYOD environment because it makes mobile employees happier and more productive. With the wrong authentication approach, synching Exchange Online to users' phones and devices will place a heavy burden on IT. Be sure to choose an authentication cloud service that offers reliable self-service installation of native Office 365 applications and automatic configuration of email, calendars and contacts. Also, be sure the authentication cloud service you choose offers the ability to check that employee devices are secure, trusted and configured properly before they are provisioned — and that devices are properly configured after the self-provisioning process.

SIMPLIFY THE NOW, PREPARE FOR THE FUTURE

Choosing the right authentication cloud service for Office 365 requires a strategic look into the future. Evolving threats and the increasing complexity of your digital business infrastructure will almost certainly create a need for high-assurance capabilities. Simple, lightweight services may work well for an initial launch of Office 365, but as your digital environment evolves, you'll likely find that the increasing number of endpoints that live and work outside your traditional perimeter truly present a need for high-assurance security.

Also, as employees, customers, partners and other users become increasingly mobile and more digitally savvy, they are going to expect increasingly invisible security. Any cloud solution should offer a clear roadmap that includes machine learning, behavioral biometrics, artificial intelligence and other emerging technologies. Choosing a partner with the proven history of investing in an identity platform and providing serious security and bold enablement at the enterprise level will be critical.

CLOUD & MOBILE RESHAPING THE ENTERPRISE

Workers use an average of **3 DEVICES EVERY DAY** to do their work[4]

The number of devices enterprises manage **grows more than 70% ANNUALLY**[4]

3-in-5 enterprise employees regularly work outside the office[5]

ABOUT ENTRUST DATACARD

Employees, citizens and consumers increasingly expect anywhere-anytime experiences — whether they are logging on to corporate networks, crossing borders, accessing e-gov services or making purchases. They also expect the ecosystems that allow this freedom and flexibility to be entirely reliable and secure. Entrust Datacard offers the trusted identity and secure transaction technologies that make these ecosystems possible. Our 45+ years of industry-leading expertise and experience spans the globe, with more than 2,000 employees serving customers in 150 countries worldwide. For more information, visit www.entrustdatacard.com

Entrust Datacard

Contact Your Trusted Advisor Today

Phone: +1 952 933 1223
www.entrustdatacard.com
info@entrustdatacard.com

[1] Gartner's Top 10 Security Predictions, 2016
[2] Forbes Insights 2016 Study, "How to Win at Digital Transformation: Five Steps Digital Transformation Leaders are Taking"
[3] Frost & Sullivan 2013 Journal Article, "Transforming the Relationship Between Products and Services"
[4] Citric Mobility Statistics, 2015
[5] IDC Mobile Worker Forecast, 2015