VERA VS. MICROSOFT AZURE INFORMATION PROTECTION

Microsoft DRM has been around for decades but still can't meet the most basic requirements of enterprise security teams. We know. Here are five ways Microsoft rights management fails enterprise teams (and five reasons Vera's got your back).

1. PAINFUL, CLUNKY EXTERNAL COLLABORATION

MICROSOFT

To access secure files, Microsoft Azure Information Protection (AIP) forces external collaborators outside your organization to download the Microsoft RMS application on their local device and create a Microsoft account. The experience is confusing for business users and requires frequent IT intervention.

VERA

We believe sharing should be a simple, secure experience. With Vera, your recipients can easily access secure content directly from a browser without needing to install any apps or sign up for yet another account. No friction, no headaches, no reason not to share securely.

The Vera Advantage - Vera's got your back with simple security that scales: It's a fact: tools like Microsoft AIP that introduce friction into your team's collaboration process quickly lead to employee workarounds and risky behavior. We built Vera with the employee experience in mind to power secure collaboration and ensure adoption across the company.

Gartner predicts that by 2018, 40% of Microsoft Office 365 deployments will be forced to rely on third-party tools like Vera to fill significant gaps in security and compliance. That's 3x more than today.

2. ZERO AUTOMATION EQUALS ZERO SECURITY

MICROSOFT

Microsoft relies on every user to manually secure content in OneDrive and SharePoint. This requires your security team to continually train and monitor adoption in the hopes of slowing data loss. And, common collaboration tools outside the Microsoft ecosystem, including Box, Dropbox and SMB drives are also not supported.

VERA

Vera automates data security with a simple drag and drop interface. Content uploaded to OneDrive and SharePoint is automatically and invisibly secured with Vera and permissions remain with your files even after they're downloaded or copied. Leverage Vera's smart rules engine to automatically secure all email attachments too.

The Vera Advantage - Vera secures SharePoint, OneDrive, and beyond, automatically: The last thing you need is to worry about whether employees are following the prescribed "steps" to secure sensitive content. Whether you're using OneDrive, SharePoint, Box, Dropbox local drives, or a mix of them all, Vera provides simple, automated data security that gives you peace of mind and ensures your end-users get it right.

3. LIMITED FILE TYPES MEANS LIMITED SECURITY

MICROSOFT

Microsoft AIP only protects a limited number of Microsoft-created file types. Have any non-Office content? Forget collaboration - anything that doesn't fit within Microsoft's walled garden is flattened into a proprietary PDF-like format that requires special software to view.

VERA

Your business is too dynamic to rely on only five file types. That's why Vera is content agnostic and can secure, track, and revoke access to any file type, including Office documents, audio, video and image files, 3D PDFs, CAD drawings, and more. Secure files open seamlessly in their native apps. No file format plug-ins or proprietary viewers required. How nice is that?

The Vera Advantage - Don't limit yourself. Or your employees. Collaborate with confidence (and Vera): Teams generate data in all forms and bring new data types into their organizations (think Slack). Your security platform must scale to natively incorporate and secure these new file types without triggering additional file format plug-ins.

4. STATIC FILES LEAD TO STATIC PERMISSIONS

MICROSOFT

With Microsoft, once you set permissions on a file, updating security policies after-the-fact is onerous and burdensome. To cite just one example: to revoke access to a specific user, you need to lock down the entire file. Imagine doing that on a project with 10 collaborators.

VERA

With Vera, users can 'unsend' files by instantly revoking access from any user, device, or organization. Unlike Microsoft AIP, Vera allows IT to update and revoke access to individual users without locking down the entire file, making a working "kill switch" for enterprise data a practical reality. Even better - Vera's approach means that keys and content are never kept in the same place.

The Vera Advantage - If it doesn't scale, it's not a practical solution: Collaboration is a messy process - don't put hurdles and roadblocks in the way. Imagine an everyday scenario with Microsoft: You need to share a highly confidential file with the 20 people on a project. If one team member leaves, to ensure she no longer has access to the data, Microsoft requires you kill the file for everyone and reissue a new file for the remaining 19. Not practical! Vera can show you a better way.

5. THERE'S NO ONE PLACE TO STORE YOUR FILES

MICROSOFT

Like most Microsoft products, AIP is limited in its scope, and assumes your whole business is run on Microsoft. But, as your employees, customers, and partners adopt new tools and applications, AIP has no way to support these new workflows.

VERA

While OneDrive and SharePoint might be your team's preferred storage platform, Vera's content-agnostic solution future-proofs your collaboration strategy, giving you the flexibility to protect content shared through other collaboration tools (e.g., local folders and shared drives, Dropbox, Box, etc.) without sacrificing security or control.

The Vera Advantage - Future-proof collaboration that changes with your business: Gartner predicts that by 2018, 40% of Microsoft Office 365 deployments will rely on third-party tools like Vera to fill gaps in security and compliance, a major increase from less than 10% in 2016. Security can't operate in silos or work exclusively in an island. It must weave itself seamlessly into your entire ecosystem.