Cryptzone™

DATASHEET

Dynamic Data Security for SharePoint and Office 365

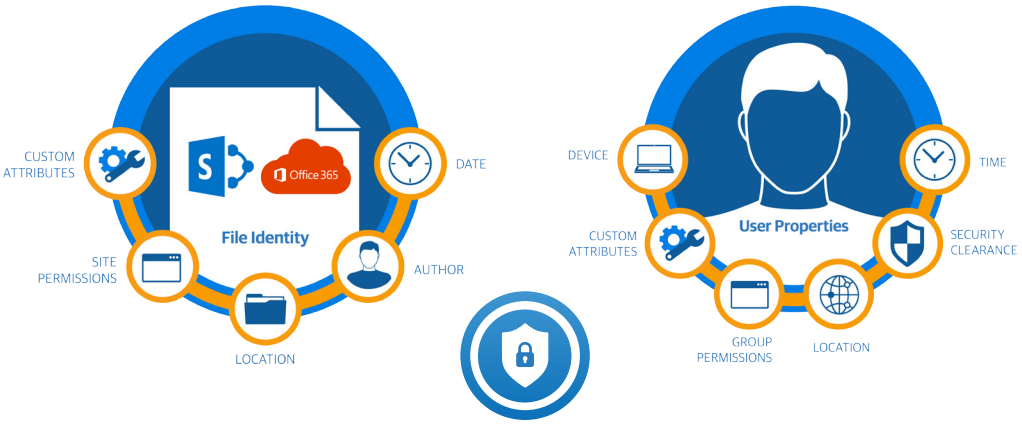
Perimeter file security is obsolete - Balance data security with user experience

EXECUTIVE SUMMARY

Security Sheriff™ dynamically adjusts file security based on real-time comparison of user and file context to make sure that users view, use and share files according to your business's regulations and policies. Security Sheriff secures files at rest without the overhead of complex user permissions and encryption, ensuring that the data is protected at the time it is used or shared. It restricts usage and visualization of data based on the file's classification and the user's current location, device and security clearance, automatically encrypting it when the data leaves the safety of the corporate file system.

KEY BENEFITS

- Individualized restriction that changes when the context changes
- Dynamically restrict ribbon rules by user / file context in all MS Office apps
- Restricted view of all files and properties so users can't discover security policies
- Automatically encrypt individual files only when the situation requires
- Adjust security based on file and user context – including email recipients
- Automatically apply business policies to files as they move between people



Real-Time Authentication Determines

What a user sees when viewing and searching for files	Whether a user can open, export or copy a file	What actions are enabled in the Microsoft ribbon	If a file is encrypted when saved, copied or emailed	If a file should be emailed to a particular recipient	If a user must view the file Securely

What You Don't Know Can Hurt You

Do you know where your unstructured content in your organization is being created, shared and stored? Are you sure that your sensitive information is secure and only available to the appropriate individuals?

Locate and classify all data on-premises and in the cloud, encrypt or quarantine when required and report status to stakeholders. Cryptzone has helped public and private sector organizations around the globe assess and control content residing in SharePoint® and Office 365®. We can help you do the same.

Dynamic, Content-Aware Security and Compliance

Security Sheriff complements the powerful content publishing and collaborative features in SharePoint and Office 365 by enabling users to monitor content at rest and restrict content in motion to protect against data loss and misuse.

Security Sheriff works natively within Microsoft's products to dynamically restrict the functions a user can access through the ribbon and to automatically apply RMS protection when required. Trusted users can collaborate on any device and in any location, knowing that all data is secure, even when it leaves the company.

Manage Content Security and Permissions

With Security Sheriff, IT administrators can manage user access without creating more security groups, more sites, libraries or folders. Instead, IT administrators define user claims and access rules efficiently and dynamically control access and user actions.

In Security Sheriff, policies and permissions are managed by the people who know the regulations, the users and the data, reducing cost and frustration.

PERIMETER DATA SECURITY DOESN'T WORK ANYMORE

With migration to cloud services, users can access data from an alarming number of new locations. Between Azure and Office 365, businesses are adopting new technologies faster than ever and data loss prevention methodology needs to keep up. The data security policy must be firm enough to accommodate the adoption of new cloud services – or understandable enough to determine which must be blocked.

REAL-TIME AUTHENTICATION FOR THE EXPANDED ATTACK SURFACE

Real-time authentication is bolstered by the unique identity a file builds over time. It starts the moment the file is first saved, with its content, name, who created it and date stamps. And then when it is checked into SharePoint, it adds some more transient context such as the file location or site and classification levels.

Real-time authentication reflects the user's current context, blending traditional user permissions with granular business information such as security level or project team. And then Security Sheriff considers even more transient context such as IP address, device, browser or time of day. Security Sheriff takes your data security policies and pushes them out to each and every user and device, completely invisible to the end user.

Gold
Microsoft
Partner

Microsoft

Secure Data At Rest

Security Sheriff locates and classifies all data on premises and in the cloud, encrypting or quarantining when required, and it reports status and compliance violations to stakeholders. It automatically inspect, classifies, and restricts data according to industry regulations and your business policies.

Secure Data In Use & In Transit

Security Sheriff leverages dynamic access, deny rules and a secure viewer to help ensure that only the right users can access the right content and help you keep confidential information in SharePoint and Office 365. Security rules can be applied centrally or locally, ensuring user education and compliance, while enabling content experts to fine-tune rules.

Lower Cost of Ownership

Security Sheriff works natively with Microsoft products, restricting usage of Microsoft functionality, including the SharePoint ribbon, all Microsoft methods of viewing files, RMS encryption and emailed attachments through Exchange Email. Security Sheriff requires no additional client side application, reducing the overhead and risks involved in implementing new cloud services or BYOD policies.

Encrypt When Neccessary

Microsoft RMS encryption is automatically applied when necessary, and read/write privileges are automatically manipulated, so the user can concentrate on the content rather than the policies governing collaboration. Data is automatically secured even after it leaves the business.

Dynamic, Content-Aware Security, Data Protection and Compliance

About Cryptzone

Cryptzone reduces the enterprise attack surface by 99% with its secure network access solutions. Using a distributed, scalable and highly available Software-Defined Perimeter model, Cryptzone protects applications and content from internal and external threats while significantly lowering costs. In cloud environments including AWS and Azure, Cryptzone provides user access control, increases operational agility and improves the ability to meet regulatory and compliance standards. More than 450 companies rely on Cryptzone to secure their network and data.
For more information visit www.cryptzone.com.

Cryptzone™

Americas +1 888 272 2484 | **EMEA & APAC** +44 118 900 1236 | www.cryptzone.com | sales@cryptzone.com