SECURE COLLABORATION – THE IMPOSSIBLE PARADOX

Exploring the impact of collaboration on information security and methods to secure collaboration

archTIS

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Spending on security software is at an all-time high with Gartner cybersecurity experts forecasting an increase in spending on IT security of 8.7%, up $124 billion in 2019.[1] And, at the same time, the number and scale of information breaches, in particular insider breaches, is also at its highest – and still rising. So how is this possible?

Despite best efforts, the security solutions in use today are only partially effective at protecting sensitive data. A new approach is clearly needed. First, we must understand the impact of modern collaboration demands on information security, as we explore a more effective method to secure collaboration.

The Demands of Modern Collaboration

When computers were first used for document creation and collaboration, it involved a handful of documents and a small number of users. Information was always accessed from within the office and so each user had a single risk profile. As a result, protecting information could be achieved by setting access permissions “at-rest” on these documents - then allowing users to interact with them. Since then, the demands on collaboration have significantly increased.

The expectations of a typical user have become unprecedented: work from anywhere, on any device and with any user be they within the same organization or from a different external organization. These expectations are certainly not dampened by the sensitivity of the data to be collaborated on. Today a single user has multiple risk profiles ranging from a “fully trusted” profile when they are in the office on a corporate PC, to more “high risk” situations when they are accessing sensitive data from their own personal device on a public, unsecured connection (e.g. café or airport).

As a result, the requirements and demands placed on corporate IT and security teams has grown exponentially. In the early days, the access requirements of users were limited, requiring only a small number of access permissions to be set ‘at-rest’ on information. Security could be effectively managed using this model hence it became widespread and considered best practice. Since then however, as already highlighted, user access requirements and collaboration expectations have changed dramatically.

INSIDER BREACHES ARE ON THE RISE

A recent report by Cybersecurity Insiders[2] revealed:

- 70% of organizations confirm insider attacks are becoming more frequent
- 68% feel extremely to moderately vulnerable to insider attacks
- 39% identified cloud storage and file sharing apps as the most vulnerable to insider attacks
- 85% of organizations find it moderately difficult to very difficult to determine the actual damage of an insider attack
- 56% believe detecting insider attacks has become significantly to somewhat harder since migrating to the cloud

[1] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019
[2] https://info.nucleuscyber.com/2019-insider-threat-report

THE SECURE COLLABORATION PARADOX

THE SECURE COLLABORATION PARADOX

How do you control and protect information, while also allowing open collaboration?

Today, IT and security teams have been placed in an almost impossible position trying to keep up with user requests. With the use of BYOD and flexible working practices becoming the norm, administration teams are being stretched in order to attempt to implement these security controls. As a result, costs can spiral, response times incur ever increasing latency and system performance can be degraded - simply trying to verify user permissions.

And the penalties for failure have become almost unimaginable. Marriott Hotels and British Airways have both fallen foul of regulators and incurred large fines, and the recent Quest data breach has led to the bankruptcy of the responsible third-party data handling organization.

Adding to the challenge is explosion of collaboration platforms being used since the advent of cloud services. Companies have turned to third party software solutions (including Microsoft) in an effort to better secure their information. But we have reached the point where only compromise and partial implementations are possible. You only have to look at current security recommendations within the administration and user guides to see evidence for that: e.g. guidance to “copy files into new folders/secure containers and set access permissions on those”, “encrypt everything at-rest”. Today, we are faced with either:

- Making a compromise on security by relying on complex permissions and multiple information silos, or;
- Creating dissatisfied users as they struggle to find and easily access the data that they need in order to get their job done.

The result is the Secure Collaboration Paradox: how to control and protect information, while also allowing open collaboration. On the one hand, achieving high information security normally results in tight controls – causing collaboration to be limited and in-effective resulting in the proliferation of rouge clouds. Conversely, full collaboration requires such a varied number of work practices that it often results in significant weaknesses in a corporate security strategy. How can a robust security foundation be effective in an ever-changing dynamic environment?

If asked, most companies would say that they have effectively implemented a strong security policy. However, the number and scale of breaches continue to increase. Why is that? The answer stems from the ways in which data is lost:

1. An outside party breaks through the perimeter defences and steals the information
2. A bad actor discovers how to impersonate a trusted user and accesses information using the compromised credentials
3. A trusted insider maliciously takes information out of the company for their own personal use
4. A trusted insider is negligent with their data handling despite what any user training or written policies state and accidentally shares or loses sensitive information

Traditional Security Practices Are Falling Short

The foundation for data security to date is built on the practice of using access permissions 'at-rest' to stop the wrong people from gaining access. Therefore, the focus of security/IT departments and security software has been to build ever stronger barriers around key information and only allow in those people that have been granted access.

In terms of the four data loss scenarios outlined above, this "strong barrier / guard the doors" approach only addresses the first scenario above(1). Think of it as a bank vault – you place all the company gems into a strong room for protection. Over time, add more and more layers of perimeter protection and additional methods for the user to prove who they are. However, once you are through the door, you can access all the gems and take them outside the vault – whether you should or not.

Addressing Data Loss with Dynamic Protection

So, what else could be done? With the four most common types of data loss in mind, a better solution would be to extend the bank vault analogy to include protecting the corporate gems as they are being picked up and used by the user – adding a new layer of protection that travels with the gems. So, as a user tries to use the gems in the vault, new security rules would provide extra protection:

- Hide the gems from sight for certain visitors to the vault
- If someone can remove the gems and then leave the vault:
- Wrap the gem in its own personalized locked box only accessible by the user (and their current companions) - or
- Only allow them to take an image of the gem with them if their need is only to be able to view it for reference purposes - or
- Prevent them from removing the gem but provide them with an invitation to come back to the vault to access the gem as needed – or
- Replace individual gems within a crown leaving only the less important gems in place

With the addition of "in-use" protection, we start to see how all types of data loss could be addressed. So, does this mean we need to rip up the traditional security mechanisms and start again? Not necessarily.

We still need users to prove who they are by authenticating themselves and so be allowed to access documents and information (the corporate gems). So, there is no need to replace this aspect of the current security implementations. All we are looking to do is add an additional security layer to manage the fine-grained access controls and allow the dynamic work practices.

To perform "in-use" protection, security would need to be applied for each action performed by a user. The best way to do this is to employ a proxy or access broker technology. However, simply using only the traditional security identifiers and groups (the basis of at-rest protection) would not be scalable or efficient enough to support all the possible user scenarios. A new "security by metadata" paradigm would be needed.

Documents and users already have metadata (properties, claims or whatever label you prefer). Document properties can be set manually by users or automatically using classification engines (e.g. Microsoft AIP, or other third-party solutions such as NC Protect). Users are already given properties by their identity providers, by their network/internet connection and their devices. So, the building blocks are pretty much already there with usually only a few tweaks required.

THE 4 MOST COMMON WAYS DATA IS BREACHED

- An outside party breaks through the perimeter defences and steals the information
- A bad actor discovers how to impersonate a trusted user and accesses information using the compromised credentials
- A trusted insider maliciously takes information out of the company for their own personal use
- A trusted insider is negligent with their data handling despite what any user training or written policies state and accidentally shares or loses sensitive information

A security management system would be needed that combines these properties to use as part of access rules. With these rules evaluated every time a user interacts with a document; the security model can accommodate the changing environment in real time.

A Data-centric Approach for Secure Collaboration

A data-centric approach respects the security boundaries and capabilities of the data repository. But it also recognizes that protection must also be applied when a file is in motion during the collaboration and sharing process as the risk profile changes. Furthermore, this must be achieved without negatively impacting a user's ability to get their job done.

When the sensitivity of the content changes over time the protection must identify when this occurs and dynamically adapt the access or usage rights accordingly. The same is true for users. The policies and systems must recognize that users need access across a variety of devices and locations. The protection mechanisms must once again be dynamic enough to recognize the context of the user and make the appropriate security adjustments to the data "in-use" not only "at-rest".

With this approach, different users will be allowed different usage rights:

- Some will be allowed full control to edit the file and share it as they see fit; while others may only be allowed to view the file.
- The same file being accessed by the same user can also have different protection based on their circumstances, such as device being used or location:
- In the office, allow the file to be fully opened on the local machine in Word, Excel, etc.;
- But while in the local coffee shop or from a mobile device only allow the file to be viewed within a secure browser or not at all depending on its sensitivity level.

In summary, the traditional location-based access controls, that only provide a binary allow or block-all access to information, do not fit with how users need to work and collaborate in the modern workplace. Equally, securing your sensitive information by beefing up perimeter security alone will unfortunately not be enough to guarantee protection from accidental data loss or malicious insider threats. Only adopting a data-centric approach that utilizes both file content and user context will provide dynamic access and protection to the level of information security that is needed for secure collaboration.

DATA-CENTRIC SECURITY

A data-centric approach respects the security boundaries and capabilities of the data repository. But it also recognizes that protection must also be applied when a file is in motion during the collaboration and sharing process as the risk profile changes. Furthermore, this must be achieved without negatively impacting a user's ability to get their job done.

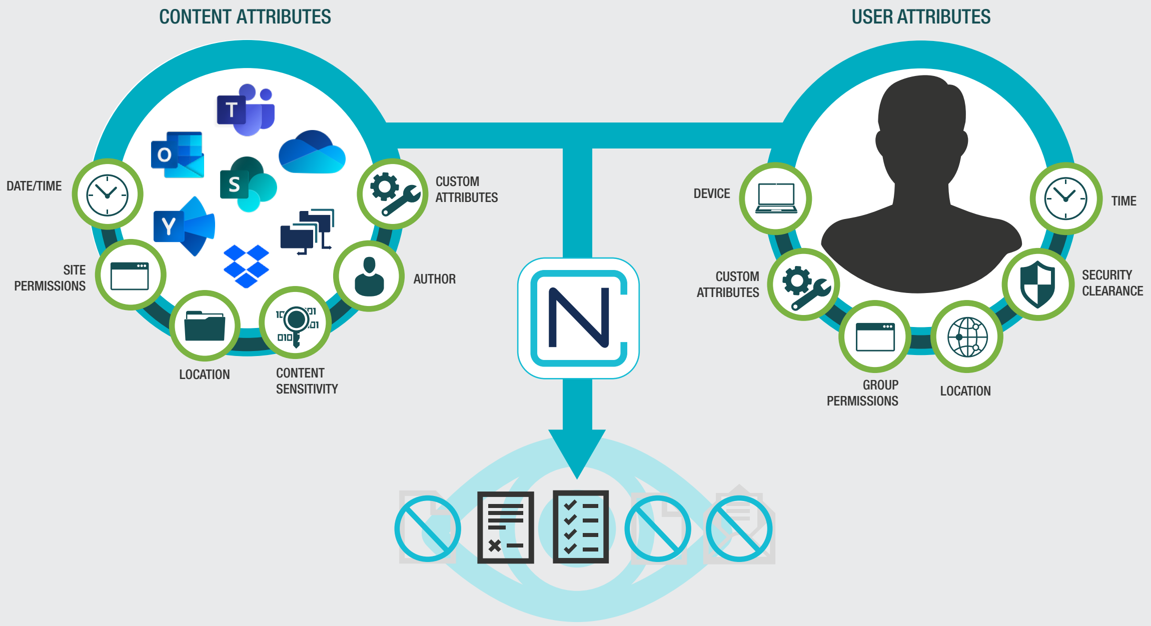
EMPOWER USERS TO COLLABORATE FREELY - WITHOUT RISKING SENSITIVE DATA

archTIS provides a way to leverage data-centric security that dynamically provides granular control over your organization's IP and information without restricting the collaboration freedom that your users demand or risking the high cost of being too open with your sensitive data.

NC Protect from archTIS solves the secure collaboration paradigm with dynamic data-centric security based on real-time comparison of file and user attributes. It provides dynamic, granular data security and governance that leverages and enhances an organization's existing infrastructure investments.

NC Protect is both content and context aware to automatically find, classify and secure unstructured data on-premises, in the cloud and in hybrid environments. The platform protects against insider threats including breaches, sensitive data misuse and unauthorized file access enabling enterprises to fully take advantage of collaboration without the risk.

GET REAL TIME, ATTRIBUTE-BASED ACCESS & SHARING CONTROL WITH NC PROTECT



START DYNAMICALLY SECURING YOUR COLLABORATION

Discover how NC Protect solves the secure collaboration paradigm with dynamic data-centric security based on real-time comparison of file and user attributes.

For more information or a product demo, **contact us and let us know how we can help.**

ABOUT ARCHTIS LIMITED

archTIS Limited (ASX:AR9) is a provider of innovative software solutions for the secure collaboration of sensitive information. The company's award-winning data-centric information security solutions protect the world's most sensitive content in government, defence, supply chain, enterprises and regulated industries through attribute based access and control (ABAC) policies. archTIS products include Kojensi, a multi-government certified platform for the secure access, sharing and collaboration of sensitive and classified information; and NC Protect for enhanced information protection for file access and sharing, messaging and emailing of sensitive and classified content across Microsoft 365 apps, Dropbox, Nutanix Files and Windows file shares. For more information visit archtis.com. Follow us on twitter @arch_tis

archTIS

archTIS.com | info@archtis.com

Australia | United States | United Kingdom