nullafi

White Paper

Avoid Data Breaches and Data Loss by Quickly and Easily Controlling Who Sees What Data

How to Detect and Redact Sensitive Data in Transit and the Critical Reasons Why You Should

Introduction

Access to data is a mess. Data that has never been more sensitive has never had more people than ever able to see it. While companies have secured much of the user workflow (e.g., protecting endpoints, networks, and application access), there hasn't been an easy way to control the visibility of the data itself within the applications themselves.

The result? Unfettered, unwarranted, and over-privileged access, leading to a precipitous rise in data loss. In fact, Gartner estimates that inadequate management of identities, access, and privileges will account for 75% of security incidents by 2023.

Between remote work, app updates, and even simple mistakes, organizations can expose data to the wrong users. From there, it's often out of your hands what they do with it.

Understanding why controlling access to data is so difficult can help you take back that control. Here are three significant areas of complexity:

1 The Selection of Access Control Models

There are different access control models, and every company has a game plan around who gets access to what. But as your company grows and collects more data, that playbook may shift — and you'll often need to rely on outside help.

CSO highlights four leading access control models organizations tend to use:

- **Discretionary Access Control (DAC):** The data owner decides who can access it.
- **Mandatory Access Control (MAC):** A central authority determines access rights; if people have information clearance, they can access the data.
- **Role-Based Access Control (RBAC):** Building on key strategies such as the "principle of least privilege," users receive access to data that's relevant to the job they need to do.
- **Attribute-Based Access Control (ABAC):** Taking RBAC to the next level, ABAC determines a series of attributes and characteristics for users and information. These attributes consider roles, responsibilities, and factors such as the user's location and time of day.

This decision isn't always an easy choice, nor is it a static one. You may still be determining the best path forward, but one thing is clear: as your organization evolves, the calculus for choosing the most appropriate model will shift along with it, so even though access control will always be an essential component of your company's security architecture, you'll need to regularly evaluate which model makes the most sense.

2 Remote Work Means More Ways to Share Data

When everyone worked from one office, it was easier to understand where data was coming from and going to; your IT team was never too far from company computers, and employees tended to use company phones for business only.

However, when the pandemic accelerated work-from-home capabilities, a floodgate of personal device usage opened up. You might find your employees' personal devices accessing anywhere between 80 and 250 SaaS and SaaS-like applications transferring information from and to all over the world. Pair this with a cultural shift toward fast data transfers and the notion of productivity above all else and you can see why creating and maintaining effective controls is nearly impossible.

Even if there's no ill intent, remote workers might send a file to their personal email accounts. Maybe they're headed to the airport and want to read from their phone. Or perhaps they'll back up a few folders to a personal hard drive, unaware that those folders contain sensitive data. Once an employee has made that move, it's nearly impossible to control that information.

3 Too Much to Manage Across the Board

In addition to the almost-overwhelming (and ever-increasing) number of applications for which to manage access, companies also have to manage the complexity and myriad challenges in mitigating security, compliance, privacy, and regulatory risks. This gets even more complicated as workers change roles, store/edit data, and even send data to outside parties.

In other words, companies aren't just trying to control access to data, but also managing risk, unknown data exposures, and unauthorized data access (inadvertent or otherwise). It's almost too much to manage, which creates a huge opportunity for human error.

In fact, Help Net Security highlights a new study from Egress that show respondents' top security concerns are the result of human-activated risks, such as accidental data loss and malicious data exfiltration. In response, we often see companies restricting access to entire apps and databases, but that often disrupts workers and encourages them to seek workarounds.

While it's clear that companies need to be more strategic about ways to keep their data secure, some organizations opt for convenience over security. That decision can lead to troubling scenarios — here are three common ways companies allow employees too much access to data:

Not Updating Security Practices During Company Growth

When your company is in its early stages, there's typically a skeleton IT team. Sometimes, it may just be one person managing all user accounts while also serving as support staff for any security issues that arise.

To save time and frustration, the IT team might offer the same access to everyone in the organization. After all, people in startup-phase companies often chip in on multiple roles, and they need to stay agile as the company grows.

However, once the company gets larger and job roles are more clearly defined, IT departments don't always go back and make the necessary changes to keep data secure. They use the same onboarding framework for new hires as they did for the early staff, and they don't adjust for the shifting roles of current employees.

That combination can lead to the majority of the company having over-privileged access, which is a poor security practice.

Granting Additional Permissions After a Breach – And Then Not Resetting Them

Even if you've done an excellent job limiting the amount of data new hires can access, a breach will likely still occur at some point.

Handling a breach often requires several people working together, typically needing high-level access to ensure a thorough response. To promptly address these major incidents, organizations often grant additional permissions to specific people on the IT team or even throughout the company.

As we mentioned earlier, the problem with this approach is that organizations might not revert to original access levels once the issue gets resolved. Now, multiple people within the company have more access than needed, potentially compromising sensitive information.

Workers Leaving the Company – And Taking Data with Them

Ghost employees are employees who are no longer with your organization. Yet they can leave a lasting impact. For example, Security Magazine reports that a former employee of Fintech giant Block (previously known as Square) caused a data breach that affected 8.2 million users, when they downloaded reports from Cash App.

It's imperative to quickly delete any company accounts former employees once had, including SaaS apps covering CRM, analytics, accounting, and other business-critical functions.

Dragging your feet in removing those accounts increases the likelihood of a data leak. A malicious actor can take advantage of an unused but active account. And if an employee leaves the organization on bad terms, they might become the bad actor and take a spiteful approach with those accounts and company data.

This scenario is further complicated by remote work. Remote workers might send themselves files with sensitive data to their personal email accounts. When the employee leaves the company, any work files saved in a personal account, on a personal device, or backed up to a personal hard drive, remain with the employee. Suddenly, PII or other company data is more vulnerable, as it's unprotected outside company walls.

What Can You Do?

While too much data access can quickly bring a company down, what if you could actually control access to the data within the applications themselves? That fundamentally solves the problem of data security and data privacy. Imagine if your organization could:

- Automatically detect and redact sensitive data in transit, before it reaches the user's device
- Secure data with intuitive controls that use natural language so even less-technical managers can quickly govern data access at the most granular levels
- Control access to data across any number of users, endpoints, and applications, inside or outside of your organization, and without excessive costs – or slow, complex deployments or application integrations...

...all by just changing one configuration file in your network? Nullafi makes all that, and more, possible. We're dedicated to protecting sensitive data within any application so that your users see only the data they need to see, giving your organization unprecedented control over data access.

The Difference Between Data Masking and Data Obfuscation

Can your company control who can see specific data in all of your applications? To do that, some companies deploy a complex blanket defense that limits what people can see; others restrict apps entirely. Both of these approaches introduce key pain points: they're difficult to implement, and they're not foolproof—any data that's not labeled properly won't be addressed correctly.

Some better options include data masking and other types of data obfuscation. People often use these terms interchangeably, and they're both methods companies use for data access control and user privacy. They're not quite the same, though, and knowing the distinction can help you make better decisions for your company.

Data obfuscation is the blanket term for transforming data into a different form to protect it. There are three main types of data obfuscation: data masking, tokenization, and encryption.

Data masking creates a substitute version of a dataset. The data values are changed, but the format remains the same. Because of this, an organization can run tests or training sessions as if it were using the real data without actually compromising that user information.

Nullafi uses data masking to obfuscate sensitive data, preferable to restricting access to entire apps and databases, which disrupts worker productivity and can spur them to try and get into those apps and databases in less secure ways.

How It Works

Nullafi's proprietary data security software sits between applications and endpoints, tying in with your existing network technology in order to detect and redact sensitive data across applications. Because our software runs in your environment, you don't have to worry about latency, third-party data risk, or downtime.

Nullafi intelligently recognizes and obfuscates sensitive data in transit, before it gets to the user's device – no matter where it originates, what field it's in, or how it's labeled. You get simple-yet-powerful controls to granularly manage, monitor, and block data access for any user in any application.

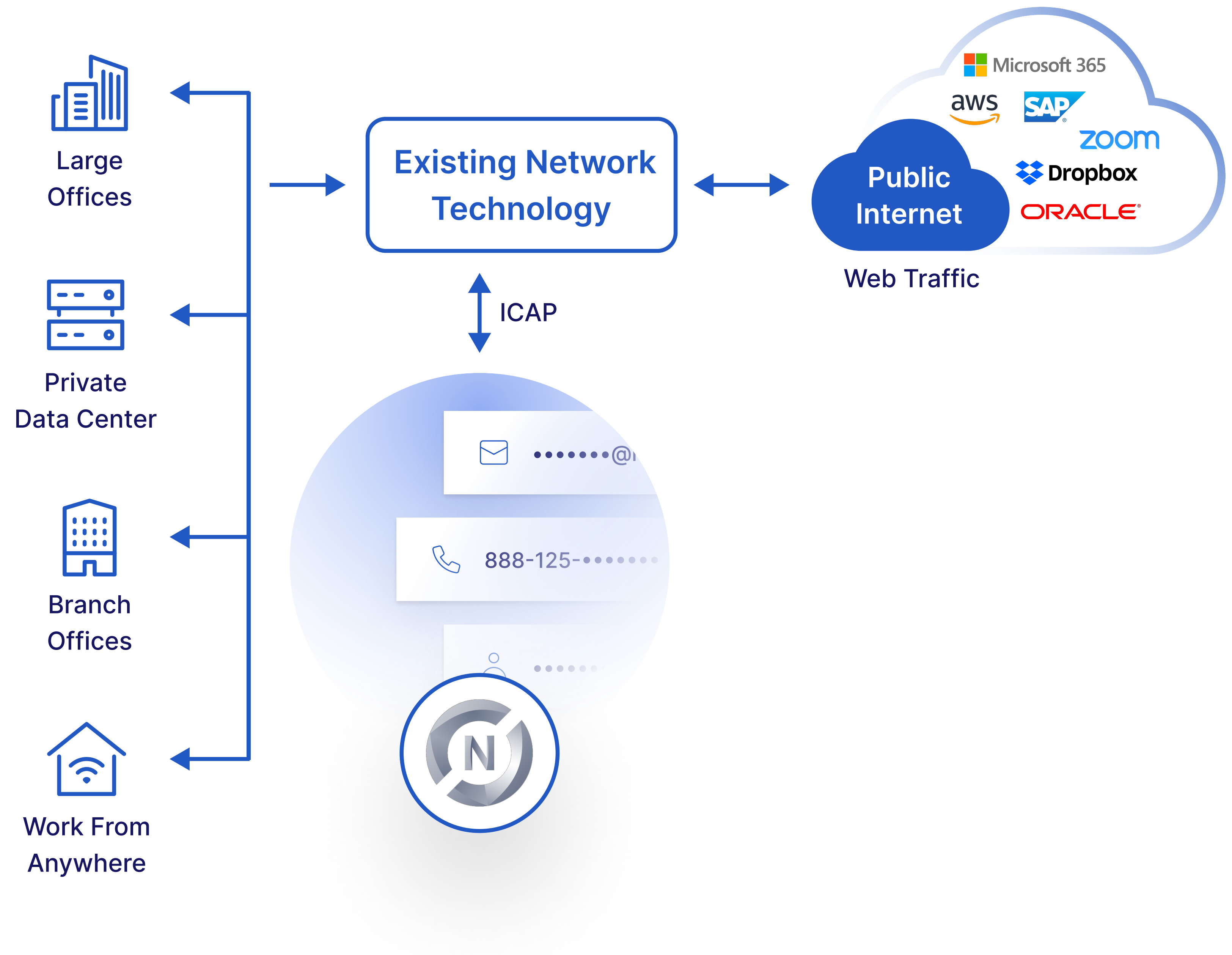

Figure 1: Nullafi Shield sits between applications and endpoints and simply "ties in" with existing network technology to obfuscate individual data elements according to the user's identity, before they get to the user's device.

In fact, because Nullafi intercepts data at the network level, it works with any application, any data, anytime, anywhere, with no application integrations necessary, providing you with a data safety net for the entire suite of corporate applications. With less than a 15-minute setup just by changing a single configuration file in your network, you're able to detect and redact sensitive data to solve data privacy, security, and access challenges. Imagine easily mitigating third-party data risk, insider threat, improper data exposure, and related compliance headaches.

Our agentless approach is invisible to end users and is a fast, easy way to protect sensitive data, automate policy enforcement, and eliminate risks such as data leakage, inadvertent access, and improper downloading – all while allowing business to continue without interruption. With Nullafi, your users see only the data they need to see, giving your organization unprecedented control over data access.

There's no need to install extensive, complex software, deploy app updates, or go through hours of confusing training. Nullafi software is delivered as a containerized service. Deploy it with a simple script and use our controls to manage, monitor, and block data access for any user in any application.

If you’d like to:

- **Automatically protect sensitive data** in transit before it reaches a user’s device
- **Secure data with intuitive controls** that use natural language, allowing even less-technical managers to quickly govern data access at the most granular levels
- **Control access to data** across any number of users, endpoints, and applications, inside and outside of your organization
- **Eliminate slow, complex deployments** or application integrations...

...we urge you to consider Nullafi. To learn more, schedule a demo today.

About Nullafi

Nullafi is a fast-growing provider of data security software that helps customers quickly, easily, and comprehensively detect and redact sensitive data, automate policy enforcement, and eliminate risks such as data leakage, inadvertent access, and improper downloading – all while allowing business to continue without interruption. With Nullafi, users see only the data they need to see, giving organizations unprecedented control. The company serves primarily mid-market companies, technology resellers, and application developers in North America. With rave reviews from analysts, multiple patents granted, and key partnerships already established, Nullafi is well-positioned to transform data security as we know it. For more information, visit www.nullafi.com.