NETWORK DETECTIVE PRO™

POLICIES AND BELIEFS DON'T EQUAL PROTECTION

Although compliance officers, IT directors and lawyers stress the need for cybersecurity policies, they often fail to focus on equally important compliance procedures and evidence of compliance. Formulating policies is easy because they simply state a requirement, but the hard part is documenting the procedures that need to be implemented to support these policies. Creating this "evidence of compliance" is mandatory to pass an audit or investigation. Unfortunately, most companies assume that just because they have policies in place, everyone follows them. However, that couldn't be further from the truth. It takes "under-the-skin" network scans to lay these assumptions bare and truly reveal what's really going on.

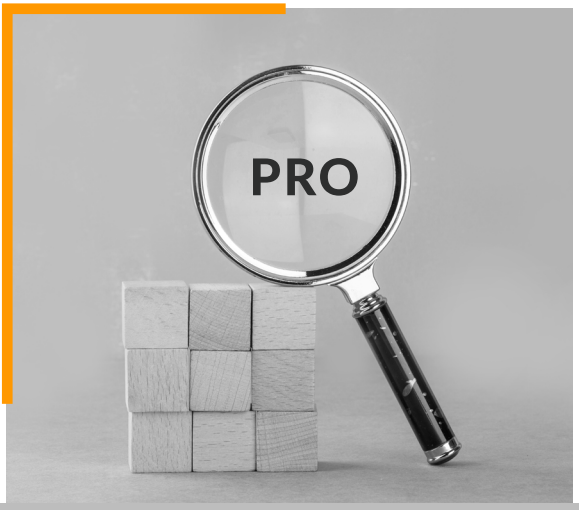
You can always find legally protected data, including Personally Identifiable Information (PII), Protected Health Information (PHI) and business-sensitive data like payroll information, stored on desktops and laptops that often aren't encrypted. Often, the users aren't aware of this, and even worse, the IT team doesn't look for it since they believe the users are following policy and storing data on servers.

Sometimes, IT directors and senior executives are shocked to see that their data is being stored in unexpected locations. They often ask, "We have policies requiring data to be stored on servers, so why aren't our people following our policies?"

Well, the simple answer is that their data storage isn't properly automated, their users aren't properly trained, and worse, they assume their policies are followed to a T, so they never look for evidence of compliance.

HOW NETWORK DETECTIVE PRO HELPS

One way to avoid the pitfalls of not having evidence of compliance is by using RapidFire Tools' Network Detective Pro to perform under-the-skin assessments that dig deep and look for data files. Its Data Breach Liability Report shows you where social security numbers, credit card numbers, driver's license numbers and banking information are stored, even if they are in PDF or .zip files.

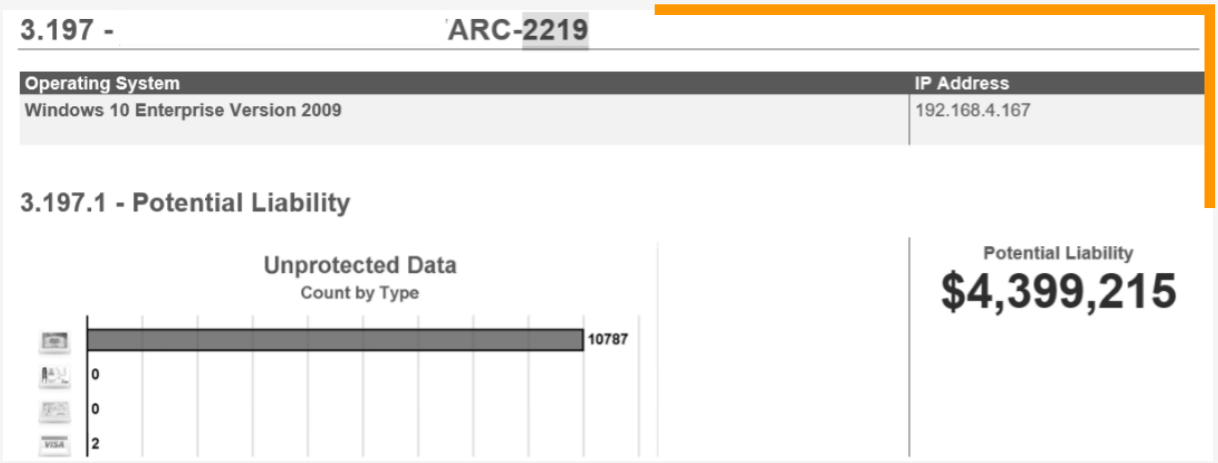


It also calculates the potential liability based on the amount of protected data using the cost per record identified in the respective annual IBM Cost of a Data Breach Report.

Are you having trouble getting clients to invest the right amount in protecting their organizations? Wouldn't it be nice to show them their potential liability based on their own data? Perhaps something like this figure gleaned from a recent assessment performed for a non-profit organization.

Total Potential Liability
$8,579,468

Over half of their potential risks were hiding on an unencrypted desktop computer that contained over 10,000 social security numbers — including those of the executives responsible for funding cybersecurity. All this transpired even though the organization had policies in place forbidding protected information from being stored in an unencrypted manner, requiring users to only store data on server shares for security and to ensure this data is backed up.



You can validate your role as a trusted advisor by basing your cybersecurity recommendations on facts obtained through under-the-skin network scans. This will help you show prospects and clients that what they believe to be true is actually quite the opposite.

Learn how Network Detective Pro helps you validate your role as a trusted advisor using facts obtained through under-the-skin network scans and win new business.

SIGN UP FOR A FREE DEMO NOW