bonafeyed
privacy in plain sight

Adopting A Data-Defined Approach to Cybersecurity

There is an opening scene in Independence Day where Will Smith and Harry Connick Jr. lead an intrepid band of resolute jet pilots on a mission to attack one huge mother of an alien spacecraft. “They must have some kind of protective shield”, Will Smith exclaimed as they watch their sidewinder missiles explode harmlessly in the air. The realization is that this is how most cybersecurity technology operates -- a sophisticated perimeter that attempts to guard or keep attackers out while everything on the inside remains safe and sound.

This method has been effective for a long time because the perimeter is a well-defined and understood boundary. But with the addition of BYOD, IoT, smartphones and cloud services, all of that has changed because the perimeter is no longer fixed. The way we view security needs to change, as sufficiently fortifying the perimeter is not only impossible, but most feel it is no longer worth the effort.

Today, the emphasis on data protection must shift from a perimeter-based solution to a data-defined approach because there are too many user access-points, and too much data to manage. Protecting individual data elements, PII and PHI, while seemingly unfeasible for most companies to consider, has never been more necessary.

According to Accenture and Ponemon Institute’s Cost of Cybercrime Study, breaches are growing by 27.4 percent per year even with the cost of cyber security growing by almost the same rate. Recent Gartner research states that enterprises and governments failed to protect approximately 75 percent of sensitive data in 2020. The 2019 Thales Data Threat Report revealed approximately 6 million records succumb to data breaches worldwide daily. Throwing money at trying to fortify the perimeter is no longer (although it never has been) 100 percent effective.

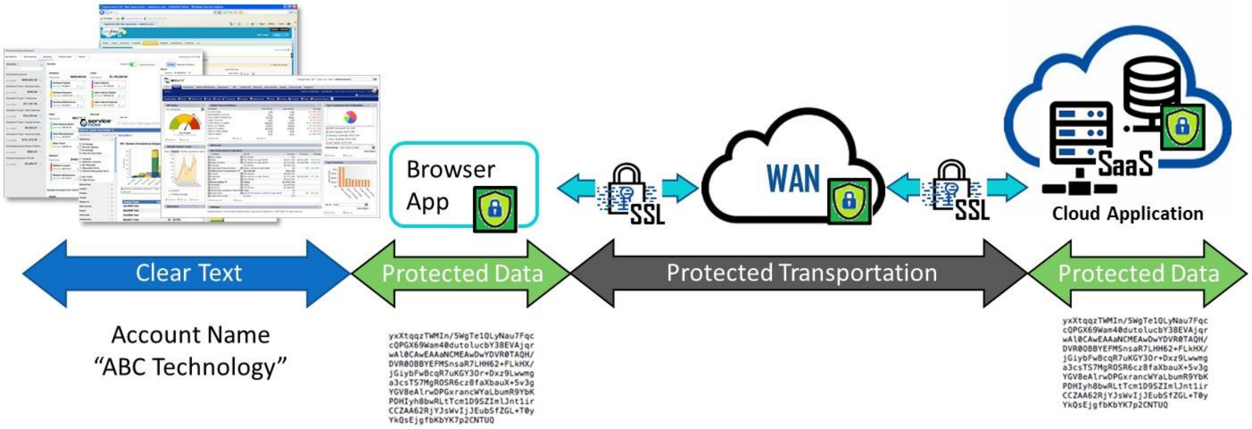
While we have already mentioned two facets of data security that must change - the first being moving from a systems approach to a data-defined approach, and the second being the need to acknowledge that the perimeter remains vulnerable as evident of the ongoing mega breaches, there is a third condition that needs adoption, and that is the necessity to move from manual human interactions to active, automated, authorizations and protection.

To illustrate the difference between manual implementation and active authorizations, let’s use Public Key Encryption (PKE) as an example. Public Key models work for the occasional message if the user is willing to do the prep work themselves. The users must exchange Public Keys with the intended recipients and do it in a way that they are confident as to the owner of the corresponding Private Key. And while this does work, at its core, it is a manual process which opens PKE to lack of adoption. When humans are involved, procedures will be forgotten or implemented incorrectly at some point.

Some may be thinking, “I am already doing data level encryption with application-layer encryption or per application file passwording”, but this is not at the data element level, it is at the file level. File level protection has one main weakness, it requires exposing the password to share files, and as the hierarchical complexity increases, (as more people or groups are added) users may stop using encryption, reuse existing passwords, or create common passwords to speed up the process.

At this point you may be feeling that data level protection may seem too complex, time consuming, or expensive to implement. Or you may be in the camp who is "hoping" data-at-rest encryption or transport protection (SSL or TLS) is good enough for data protection. However, anytime data is shared, when it leaves your domain and is placed or sent to another, that data is no longer protected. The right approach is to encrypt data at the source before it is placed in a database or at the end-point device before it’s shared. This is when a data-defined approach becomes a game changer and can protect data shared by an application or cloud service.

Now imagine a technology that can operate in the background, invisibly such that all data is encrypted just before leaving your device (any device) en route to either websites, cloud applications but remains encrypted in the receiving database holding your PII or PHI information. If we assume for a moment that the unencrypted data is pure gold, once it is automatically encrypted, it becomes as worthless as a rock as it travels to recipients. At any point when the data resides on intermediate locations such as 3rd party SaaS services, or any database backed application data remains protected. When recipients receive the encrypted data and the user is authorized, it is unencrypted and turned back into its golden state without the recipient having to run separate security software or lookups or ask for passwords from the sender to gain access to the data or communications. The ‘clear’ data is made available within the application or displayed in web browser for the user.


Browser App
SSL
WAN
SSL
SaaS
Cloud Application
Clear Text
Protected Data
Protected Transportation
Protected Data
Account Name
“ABC Technology”
yxXtqqzTWMIn/5WgTe1QLyNau7Fqc
cQPGX69Wam40dutolucbY38EVAjqr
wAl0CAwEAAaNCMEAwDwYDVR0TAQH/
DVR0OBBYEFMSnsaR7LHH62+FLkHX/
jGiybFwBcqR7uKGY3Or+Dxz9Lwwmg
a3csTS7MgROSR6cz8faXbauX+5v3g
YGV8eAlrwDPGxrancWYaLbumR9YbK
PDHIyh8bwRLtTcm1D9SZImlJnt1ir
CCZAA62RjYJsWvIjJEubSfZGL+T0y
YkQsEjgfbKbYK7p2CNTUQ
yxXtqqzTWMIn/5WgTe1QLyNau7Fqc
cQPGX69Wam40dutolucbY38EVAjqr
wAl0CAwEAAaNCMEAwDwYDVR0TAQH/
DVR0OBBYEFMSnsaR7LHH62+FLkHX/
jGiybFwBcqR7uKGY3Or+Dxz9Lwwmg
a3csTS7MgROSR6cz8faXbauX+5v3g
YGV8eAlrwDPGxrancWYaLbumR9YbK
PDHIyh8bwRLtTcm1D9SZImlJnt1ir
CCZAA62RjYJsWvIjJEubSfZGL+T0y
YkQsEjgfbKbYK7p2CNTUQ

Eliminating the arduous task of data encryption now ensures that all data is protected when shared with others and its security remains in the control of the sender or data owner. When protected data is lost, stolen, abandoned, or forgotten, it remains secure and becomes permanently inaccessible and demonetized once access is removed or retired, ensuring that cybercriminals, non-authorized users and even the occasional alien, only obtain unintelligible data - nothing more than a pile of worthless rocks!

Contact us at info@bonafeyed.com for a demonstration or visit us at www.bonafeyed.com.