Protecting your digital information with

# OnBase Content Services Platform

OnBase®
by Hyland

# ONBASE SECURITY

2017 was the costliest, most substantial year in cybersecurity history. Monumental security breaches hogged headlines while almost 2 billion records worldwide became compromised in just the first half of the year (88 percent of which occurred in the U.S.) according to the “Breach Level Index” by Gemalto. Criminals behind keyboards continue to evolve their methods of security penetration and have broadened their scope of attack to include everyone, especially government organizations.

Security breaches happen even more frequently than you might imagine. In fact, Ponemon Institute, one of the leading cybersecurity research firms, discovered that one out of every four companies will be a victim of a breach. In other words, chances are high that your government organization has or will be a victim of an attack. The scariest part is you could be under attack and not even know it.

OnBase by Hyland provides layers of enterprise security to internally and externally protect the critical and proprietary information your organization works with every day. Natively, the OnBase environment is secure by design. However, there are additional security offerings that address some of the more common and costly security threats, such as ransomware, user error and file server intrusion. And OnBase provides support for key federal security standards and practices like Common Access Card (CAC), Identity Verification (IdV) and FIPs 140-2 compliant deployments.

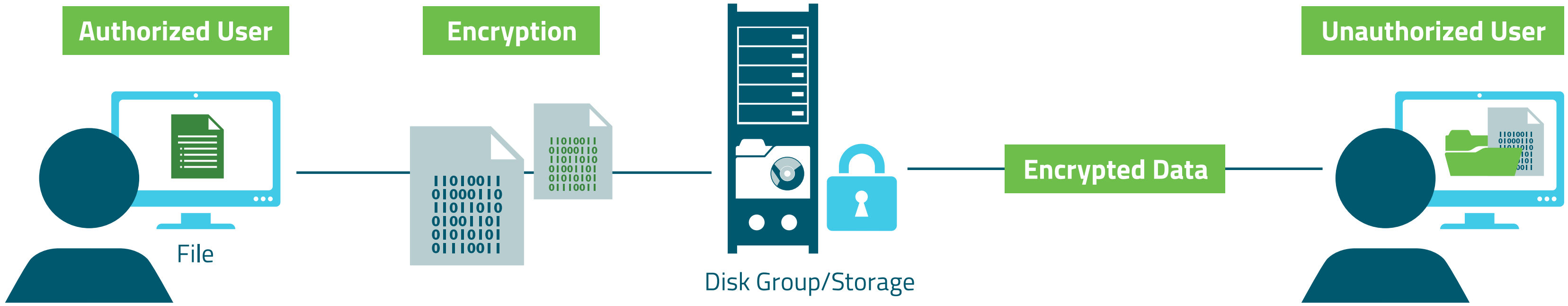
In addition to the federal security standards above, insights from CSO, an IT security thought leader and IDG subsidiary, suggest that using encryption extensively can realize cost savings of $1.4 million a year. This eBook will show you additional ways that OnBase protects your data by leveraging encryption capabilities. Discover how these “must-have” offerings deliver premium data security.

# PART 1

# ENCRYPTED DISK GROUPS

The information you store in your file server – the OnBase Disk Groups – is typically data that, in the private sector, might be subject to protection regulations such as SOX, HIPAA, the Data Protection Act, PCI compliance and more. Whether it's personal information or data that's confidential, classified or sensitive, the consequences of lacking Disk Group protection can be detrimental.

Take the Equifax breach as an example. One of its underlying causes was the lack of protection for information stored in the company's database. Richard Smith, CEO of Equifax, stated in a congressional hearing regarding the breach, "We use many techniques to protect data — encryption, tokenization, masking, encryption in motion, encrypting at rest … To be very specific, this data was not encrypted at rest." As a result, Equifax has already spent $87.5 million in breach remediation expenditures and, to make matters worse, they may incur an additional $100–200 million in legal fees. This is the most severe data breach in history caused by one of the simplest, yet costliest, oversights. Imagine the consequences for a federal or state agency if data is not stored in an encrypted manner and a breach occurs.



Encrypted Disk Groups provide a layer of protection for information at rest in your database using the AES-256 or AES-128 encryption algorithm. If data were stolen or accessed by an unauthorized party, the information would be unreadable to the attacker.

Most enterprises use full-disk encryption to prevent unauthorized access to their database while at rest. However, the problem with relying on full-disk encryption is that it was never intended for machines that host files online, 24 hours a day. In this scenario, there's still a possibility that the machine hosting the files can be compromised and, since it's powered on, the files are decrypted and accessible.

When the OnBase environment is configured to use Encrypted Disk Groups, individual files are automatically encrypted using the AES-256 or AES-128 algorithm as they are imported into OnBase, becoming indecipherable when retrieved outside of the system. Even within OnBase while a machine is powered on, these files are accessible only to permissioned users, further decreasing the risk of exposure. If a user without permissions for the file were to somehow locate where the Disk Groups are stored on the file system, they still would not be able to open or view any documents.

Encrypted Disk Groups give you additional peace of mind that the sensitive information in your database is safely guarded whether a machine is powered on or off. You can also further support compliance with your industry's information protection regulations.

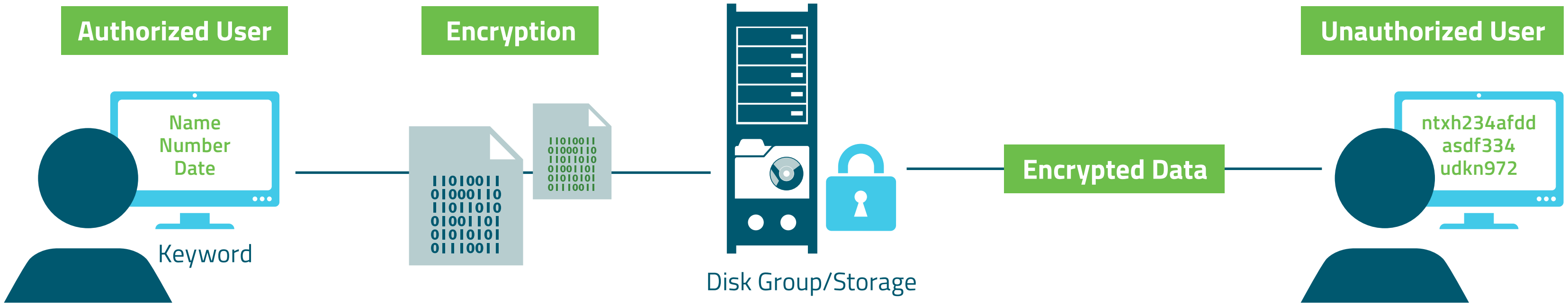
**Individual files are automatically encrypted using the AES-256 or AES-128 algorithm as they are imported into OnBase**

PART 2

# ENCRYPTED ALPHANUMERIC KEYWORDS

There’s more to data confidentiality than creating restricted work areas and encrypting data storage. Some programs, services and missions require employees to interface with documents containing highly sensitive information like medical files, Social Security numbers, bank accounts, credit card numbers or sensitive data. That, in itself, creates the risk of internal security threats, ranging from accidental user error to intentional misconduct. Some of these values are critical to retrieve the information stored in OnBase, but should only be accessible to permissioned users.

One way to address these risks is to secure the specific keywords associated with the sensitive data users interface with. Using the AES-256 or AES-128 encryption algorithm, Encrypted Alphanumeric Keywords can be configured so that if an unauthorized employee or attacker were to gain access to the OnBase database, the encrypted keyword values will be unreadable.



>>> When handling sensitive information, executing the "principle of least privilege" is a security best practice. Configuring a database to grant users access to only what they need to do their job – and nothing more – is the embodiment of this practice.

The level and ease of which organizations can configure the database to encrypt keywords is just as important. With Encrypted alpha keywords, you can quickly grant or restrict access to files by keyword value at an individual or user group level. The selected encrypted keywords will have partial or completely unreadable values to those who are not granted viewing rights.

Encrypted Alphanumeric Keywords also offer the ability to perform keyword masking, where sensitive keyword values are replaced with a masking character in the event a user shouldn't see that particular value but needs access to other information on the file (like a payroll record containing a Social Security number). This is different and more secure than redaction, which covers keyword values and, in certain instances, can be overridden.

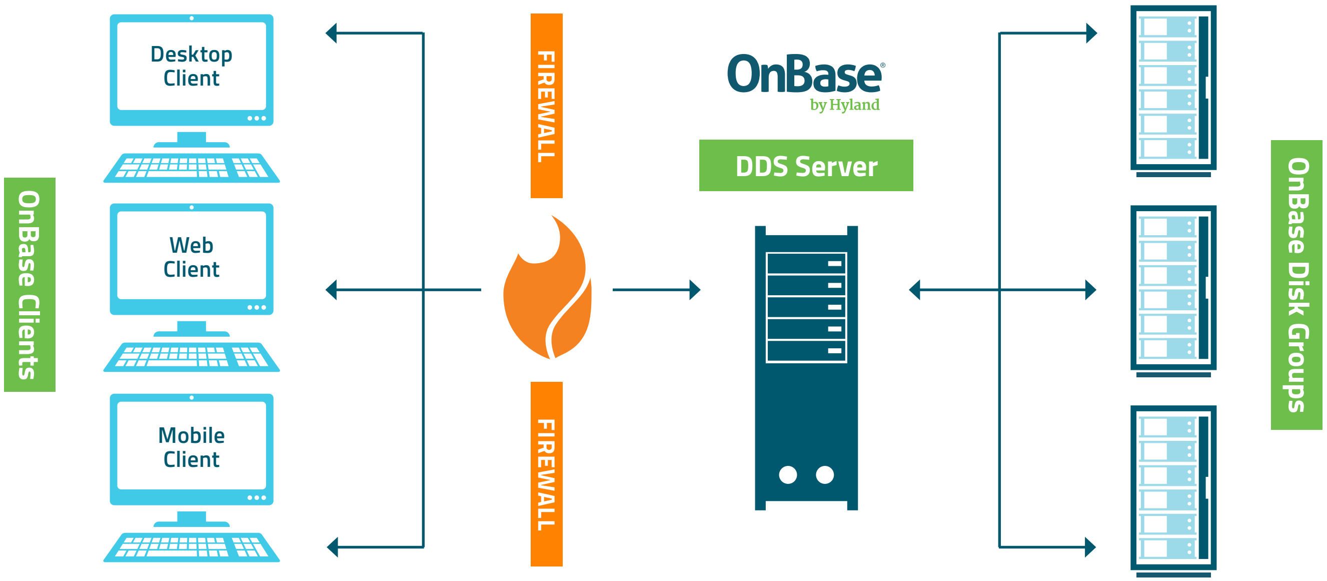
Having an additional layer of protection like Encrypted Alphanumeric Keywords can be the difference between peace of mind and a costly breach. OnBase provides invaluable ease and speed of configuring encrypted alphanumeric keywords where system administrators have the agility to meet the ever-changing security needs of their database.

**OnBase provides invaluable ease and speed of configuring Encrypted Alphanumeric Keywords**

PART 3

# DISTRIBUTED DISK SERVICES

According to Ponemon, "Only 27 percent of respondents are confident their current antivirus software will protect their company from ransomware." Antivirus software isn't enough. Distributed Disk Services (DDS) is an additional layer of in-transit protection for data. It prevents unauthorized access to files by forcing OnBase clients to authenticate with the DDS server before files can be retrieved from the Disk Groups. Traffic between the DDS Server and the Disk Groups is encrypted so that even if it is intercepted by an attacker, it will be unreadable and unusable.



>>> A properly configured DDS environment is a valid mitigation against ransomware attacks. Ransomware is a malicious software designed to block access to a device or data until a ransom is paid. This attack is typically deployed in the form of a deceptive email attachment or download.

One of the first things ransomware tries to do is find backup data. If you're storing files on a local network, chances are ransomware will find them. When you have DDS in place, all of the files related to OnBase data and documents are stored on a Disk Group server that's accessed only by the DDS server. This means only DDS knows where to retrieve the files, making it significantly more difficult for ransomware to find hostage files by adding another level of complexity to the system network.

As discussed in Ponemon's research, "Fifty-two percent of respondents did not pay the ransom because they had full backup." However, "Fifty-five percent of respondents say with certainty or that it was likely that the ransomware exfiltrated data from the compromised device(s). On average organization spent 42 hours dealing with and containing the ransomware incident."

Refusing to pay ransom doesn't solve the problem that the attacker has gained access, control and, perhaps, possession of your files and information. Most companies are reactive and replace the hostage files from a backup. DDS is a proactive protection against ransomware that makes it significantly more difficult to obtain control over the files initially.

**When you have DDS in place, all of the files related to OnBase documents are stored on a Disk Group server that's accessed only by the DDS server**

# CONCLUSION

Your organization's information is a valuable asset and government agencies have a responsibility to protect its systems, processes and data. Abiding by checklists recommending baseline security installations won't be sufficient in today's cyber environment. Your organization needs multiple layers of security to safeguard your mission. Enterprise information and content services platforms like OnBase offer several safeguards inherent to the solution's design that provide security that isn't just about whether a breach happens. Experts believe breaches will continue to happen and users may make errors or try to gain unauthorized data access. With federal standards like CAC, IdV and FIPS 140-2, OnBase supports some key tools. And with Encrypted Disk groups, Encrypted Alphanumeric Keywords and Distributed Disk Services, data breaches find only unreadable data. Bolster your agency's security and reap the benefits of a content services solution that can transform and modernize your agency and be ready for today's security challenges.

Learn more at **OnBase.com/Government ››**

For more information on OnBase security modules and how you can elevate your solution, **visit the Hyland Community or contact your first line of support.**

OnBase®
by Hyland