## Protect your data. Pervasive encryption in action.

0:01 Data is your organization's most valuable resource, and each day you feel more pressure to securely manage it.

0:07 You know the consequences of stolen or compromised data - regulatory and financial penalties, lost trust, and lost customers, all causing irreparable damage to the business.

0:20 But, protecting data at every step of its journey against every possible threat is a daunting challenge.

0:26 Pervasive Encryption on IBM Z is designed to meet that challenge head-on.

0:32 How does Pervasive Encryption keep data safe both in-flight and at rest? Let's see it in action.

0:38 From the moment that the credit card number leaves the reader, it is encrypted at the network level to help protect it from any potential attack while in-flight to the IBM Z system.

0:49 Network encryption of data in-flight is underpinned by transport layer security, or TLS.

0:55 However, the TLS handshake protocol could be a potential point of vulnerability.

1:00 Attackers can attempt to downgrade the TLS cipher in place, to a weaker algorithm that can be easily broken.

1:09 The z/OS encryption readiness technology (zERT) makes it possible to detect the attack.

1:16 zERT system management facility records are produced the moment the connection is made, showing the network encryption protocol, cryptographic algorithms, and key lengths being used to protect the data, and the SMF records can be consumed by IBM QRadar, which produces a report for the security administrator.

1:35 The report enables the admin to find unsecured or weakly secured services and take corrective action.

1:42 A network sniffer attack at this stage could attempt to collect the data, but because the attack is encrypted in-flight, the attack is mitigated.

1:50 The encrypted data is unreadable by the hacker, therefore it is unusable.

1:55 Pervasive Encryption also protects at the data set level, where insider attacks could easily compromise unencrypted data.

2:03 For example, let's say a storage administrator with valid credentials is tempted to access sensitive information.
2:11 She can access the data set itself, but because she doesn't have system authorization facility authority to the key label, she can't access the information within the encrypted data set.

2:21 The encryption keys protecting the database and the data sets are stored in the cryptographic key data set, so if the storage admin attempts to dump the encryption keys in the CKDS, the attack is mitigated because all of these keys are protected by a master key that was loaded by two or more key officers.

2:41 The dumped encryption keys are unusable without the master key, the master keys themselves are stored on a tamper-responding crypto express adapter, so if a data center technician attempts to extract them, the adapter detects the attack and zeroes itself to protect against the intrusion.

2:58 Because we had multiple crypto adapters in our system, the data continues its journey.

3:04 The data is encrypted before it is written to a storage device, so even as it moves across the storage network, it remains encrypted in-flight, and the data remains protected all the way down to the direct access data storage device, or DASD level.

3:20 Pervasive Encryption guards against vulnerabilities like network sniffing attacks, when the data is replicated to a disaster recovery system, the data itself is already encrypted, so even when the data is no longer on the DASD and thus not protected by disk encryption, it remains safe.

3:38 It also guards against vulnerabilities like network sniffing attacks when the data is migrated, even through the process of transparent cloud tiering, as it is copied and transferred from the storage device to the public cloud.

3:52 And once it's in the cloud, the data remains encrypted, so it is useless to attackers in the event of a breach.

3:58 Pervasive Encryption also provides protection for database data in memory.

4:03 Here, attackers often force a database dump in order to access sensitive data in memory.

4:09 Guardium data encryption ensures the safety of the data by encrypting the memory buffers, and when the data from the dump is transmitted off-platform, to IBM or another vendor, the data remains encrypted and secure.

4:24 If someone is able to obtain the database administrator's user ID and password, through a social engineering attack for example, multifactor authentication ensures that the attacker doesn't have all the credentials he needs to log in to the system.

4:38 Pervasive Encryption also provides protection for data shared with other members of the sysplex using the coupling facility.

4:45 Th page containing the credit card data is read into memory within the buffer pool.

4:50 With CF Encryption in place, the buffer pool is encrypted before leaving the host, and remains encrypted in the CF cache structures.

4:59 The encryption keys protecting the CF structures are stored in the Coupling Facility resource manager couple data set.

5:05 So if the Storage Admin attempts to dump the encryption keys, the attack is mitigated because encryption keys are protected by the master key, on the tamper-responding crypto express adapter.

5:19 The dumped encryption keys are unusable without the master key.

5:24 Pervasive Encryption event protects against physical infrastructure attacks.

5:28 If an attacker removes the DASD in attempts to read the data on another computer, the attack is mitigated because 100% of the data residing on the disk is encrypted, including data that could not be encrypted by other methods.

5:42 Pervasive Encryption is the best way to stay one step ahead of cyberthreats, and keep your data safe and secure.

5:50 Encryption at the network level, the data set level, and the data base level, and defense against intrusion and tampering at the disk level - protect your data both in-flight and at rest wherever it lives.

6:03 IBM Z Pervasive Encryption - learn more.