PKWARE®

PKWARE, Inc.

Forrest Ratliff
Sr. Solutions Engineer

Thieves, Snoops, & Idiots
Smartcrypt Overview & Demo

Agenda

- State of Information Security
- The Problem: Thieves, Snoops and Idiots
- What happens if you don't take action
- Smartcrypt Overview and Demo
- How you can get started

State of Information Security 2016

2015 Data Breach Stats

"Data security events increased by 38%"

"Intellectual property theft increased 56%"

2016 Global State of InfoSec Survey Price Waterhouse Cooper

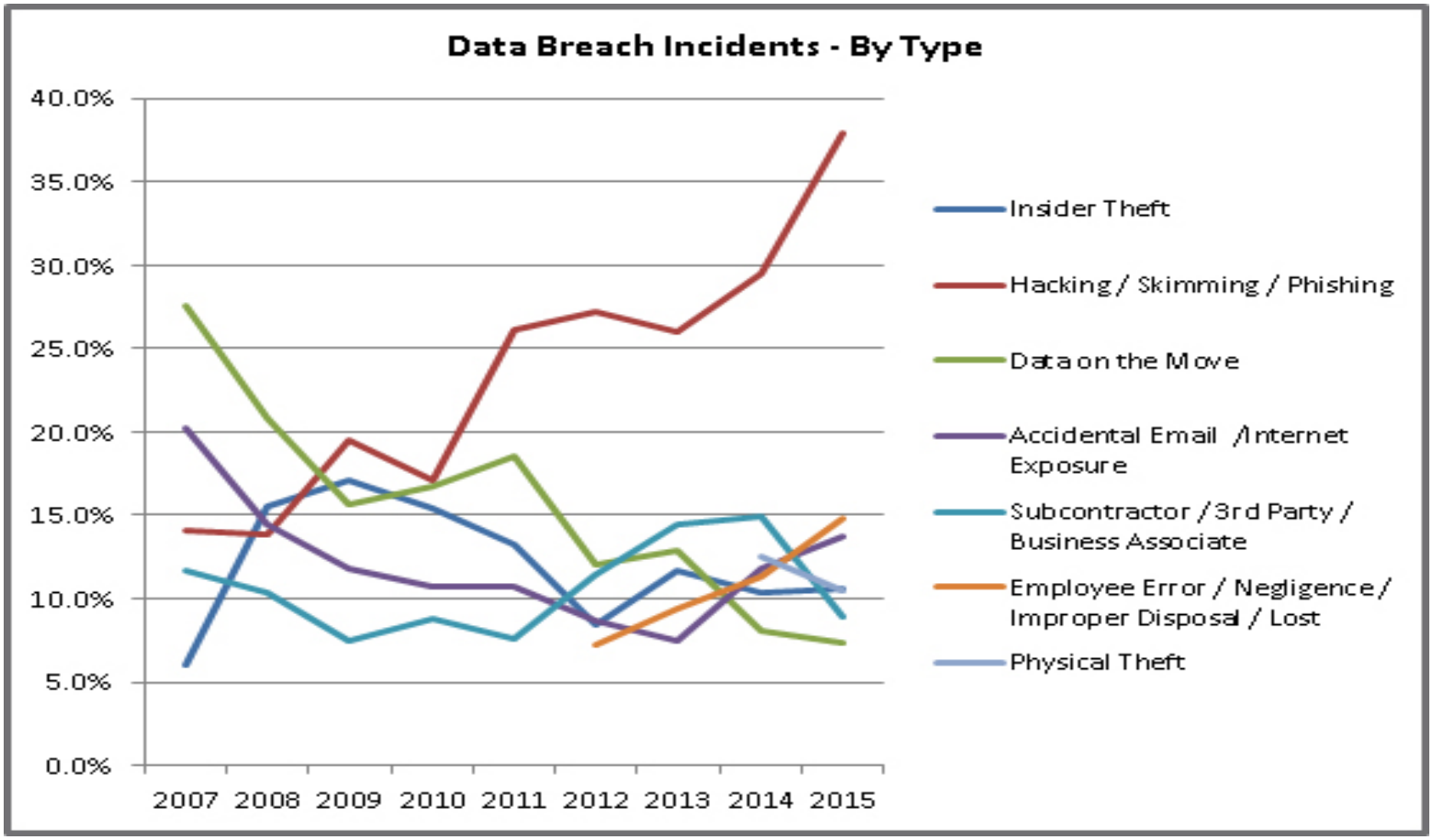
"$400 Million – estimated losses from 700 million compromised records"

2015 Verizon Data Breach Report

"Data Breaches in Healthcare totaled over 112 million records in 2015"

Forbes

Threat Landscape Evolution



Identity Theft Resource Center

The Problem:
Thieves, Snoops and Idiots

Thieves

- External Attackers
  - Competitors
  - Script Kiddies
  - Nation States (OPM breach)
  - Lexis Nexis Breach
- Rogue Administrators
  - Snowden
- Internal Bad Actors
  - Espionage

Snoops

- Privileged Administrators
- Credential compromise
- Sony Attackers

Idiots


I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

Idiots

- Users
  - Make mistakes (lose devices)
  - Have poor security education (password=123456)
- Developers / Vendors
  - Lenovo
  - Fortinet
- Administrators
  - Sony
  - AT&T
  - Dropbox

Thieves, Snoops and Idiots

Thieves, Snoops and Idiots exploit gaps in enterprise information security every day. PKWARE's Smart Encryption armors data, eliminating vulnerabilities everywhere it is used, shared or stored. Smart Encryption is easily embedded and managed without changing the way people work. Integrated across all enterprise systems, platforms and languages, Smart Encryption fortifies information security inside and outside the organization.

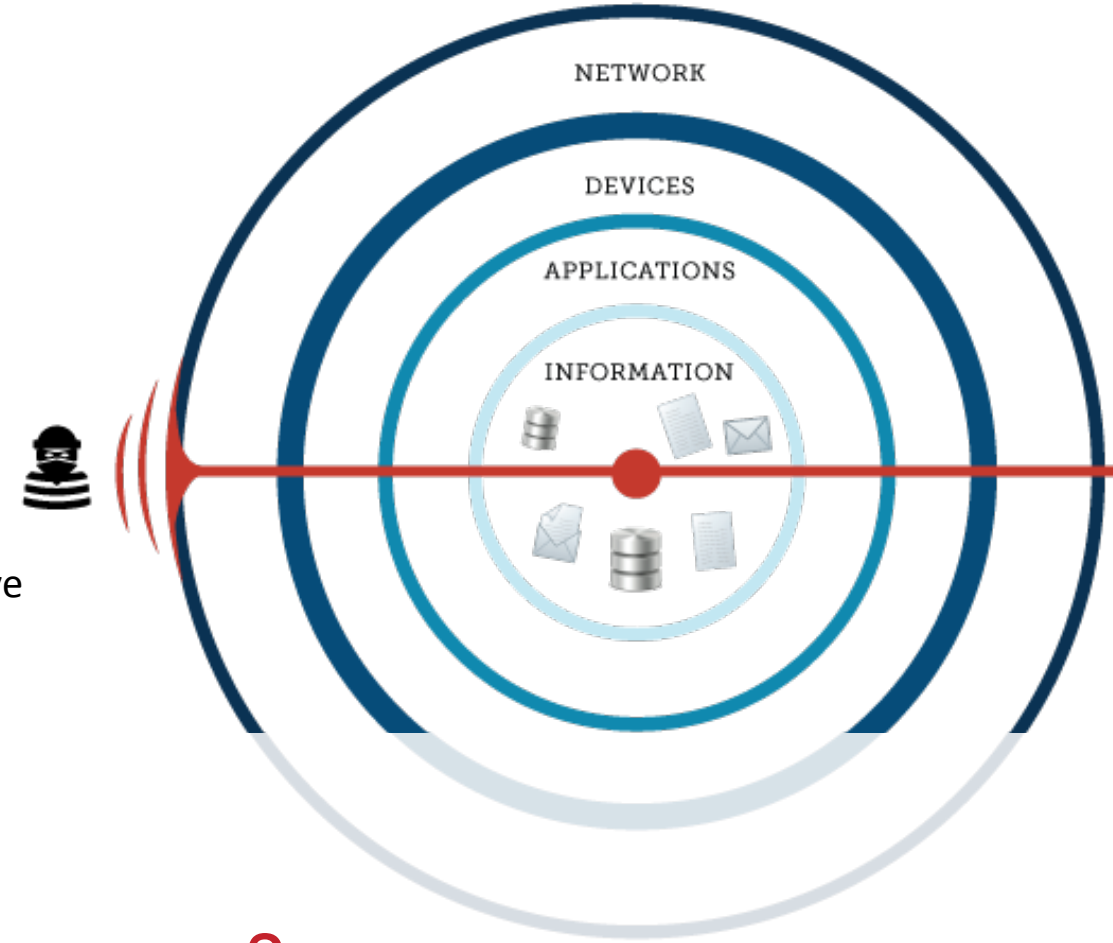
What Happens if we don't take action:

The Risks

Risks: $$$$$

- Thieves represent the highest cost in terms of dollars lost and money spent
- Snoops represent the lowest cost in terms of dollars lost but have the potential to heavily damage reputation and brand
- Idiots represent mistakes made by everyone that results in sensitive information exposure
- Risks:
  - Financial penalties
  - Brand reputation
  - Customer confidence
  - Intellectual property

The Three Elements of a Breach



1

They have to get in

2 They have to gain access to information

3

They have to get it out

Persistent data level encryption

- You must have at minimum 3 layers assuming that two will fail
- No defense in depth strategy is complete without a data-centric security solution

Smartcrypt Overview
PKWARE Smart Encryption Platform

What PKWARE Smart Encryption Provides

The Smartcrypt Application

- End-to-End, client side encryption for existing processes
- Available for every major operating system

Manager

- Policy and Control, Visibility
- Encryption Key Management

SDK

- Application Layer Encryption
- Alternative to Tokenization
- Secure sensitive information in files and databases
- Available for every major language

Total Enterprise Support

ENTERPRISE DATA CENTER INFRASTRUCTURE

- IBM System z / Linux for z
- IBM i
- IBM PureSystems
- IBM PowerSystems
- IBM AIX
- VMware
- HP UX (Integrity)
- Oracle Solaris
- Linux (RedHat, SuSE)
- X86 Servers (IBM x, Windows, ProLiant)

SMALL-PLATFORM & MOBILE INFRASTRUCTURE

- Windows Desktops
- Mac
- iOS
- Android

IBM zSeries

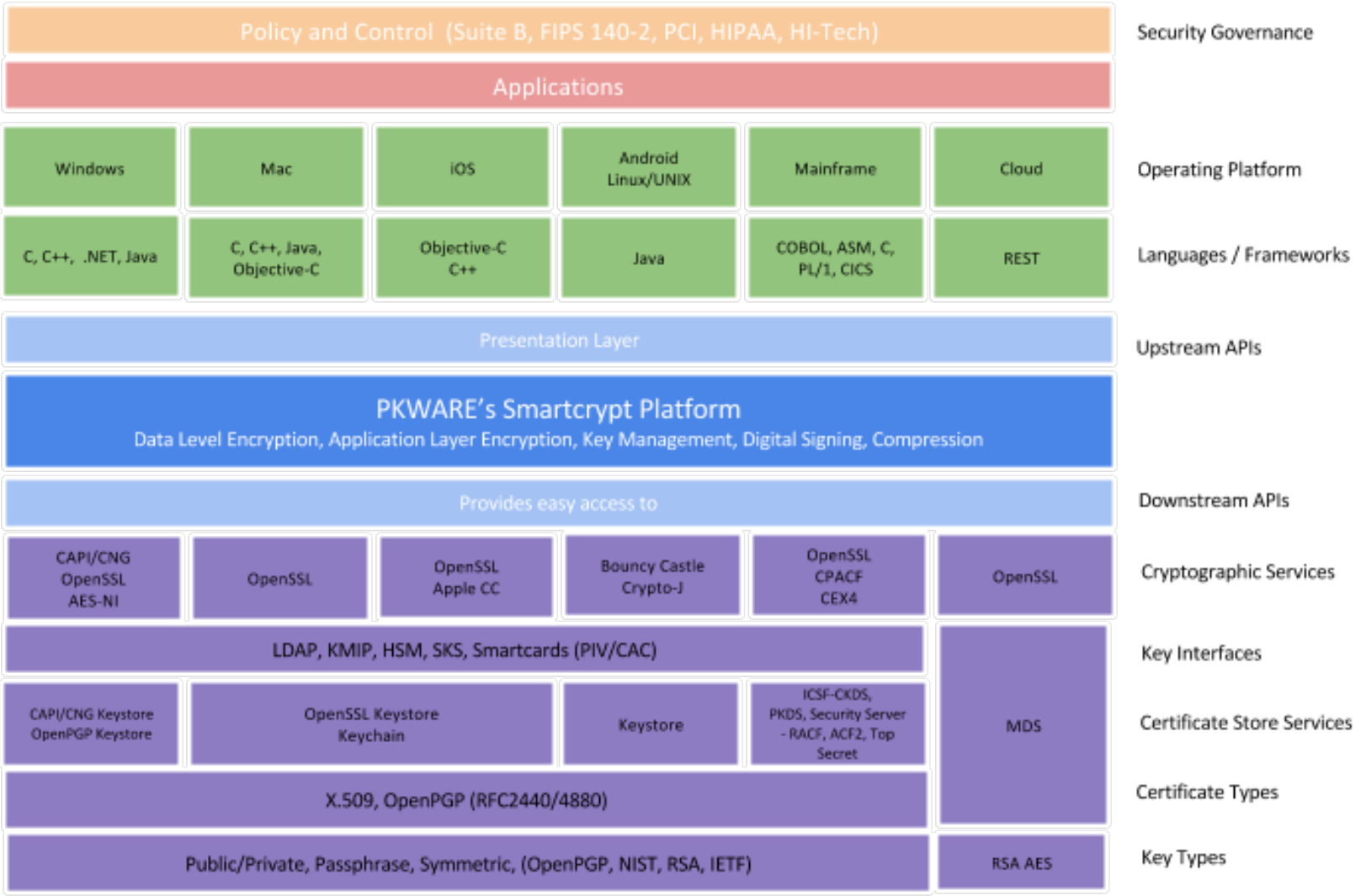
IBM i Series

Server

Desktop

Mobile – iOS & Android

Smart Encryption Platform



PKWARE®

Smartcrypt

- Provides persistent encryption for sensitive files
- Takes the complexity out of key management through “Smartkeys”
- Maintains a record of who is manipulating sensitive information
- Components:
  - Smartcrypt Application / Manager
  - SDK

Encryption + Key Management

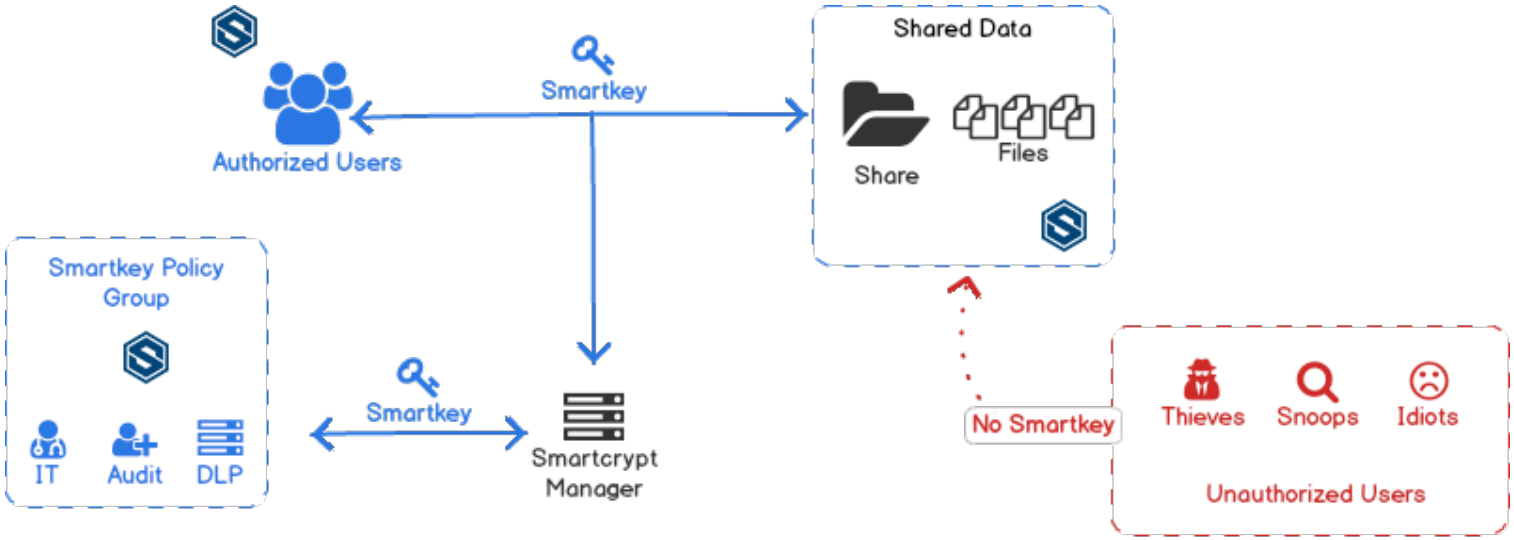
- Built to use the most well vetted cryptographic services available on each platform.
- Keys are accessed in place through existing key service layers and stores
- A variety of key formats and cryptosystems are supported
- If no PKI is in place, PKWARE can provide key management solving for
  - Uncontrolled encryption
  - Private key transfer amongst authenticated devices
  - Public key exchange for secure data exchange operations

Smartkeys

- Combine multiple symmetric keys with public keys for encryption and distribution
  - A unique session key is used to encrypt the data
  - An Asset key encrypts the session key
  - Asset keys are encrypted for Public Key of recipients
  - Recipients are managed via ACL
- Solves the re-encryption problem
- The access control travels with the data

Smartkeys

- Data is encrypted with a Smartkey(s)
- Policy driven for IT and Audit

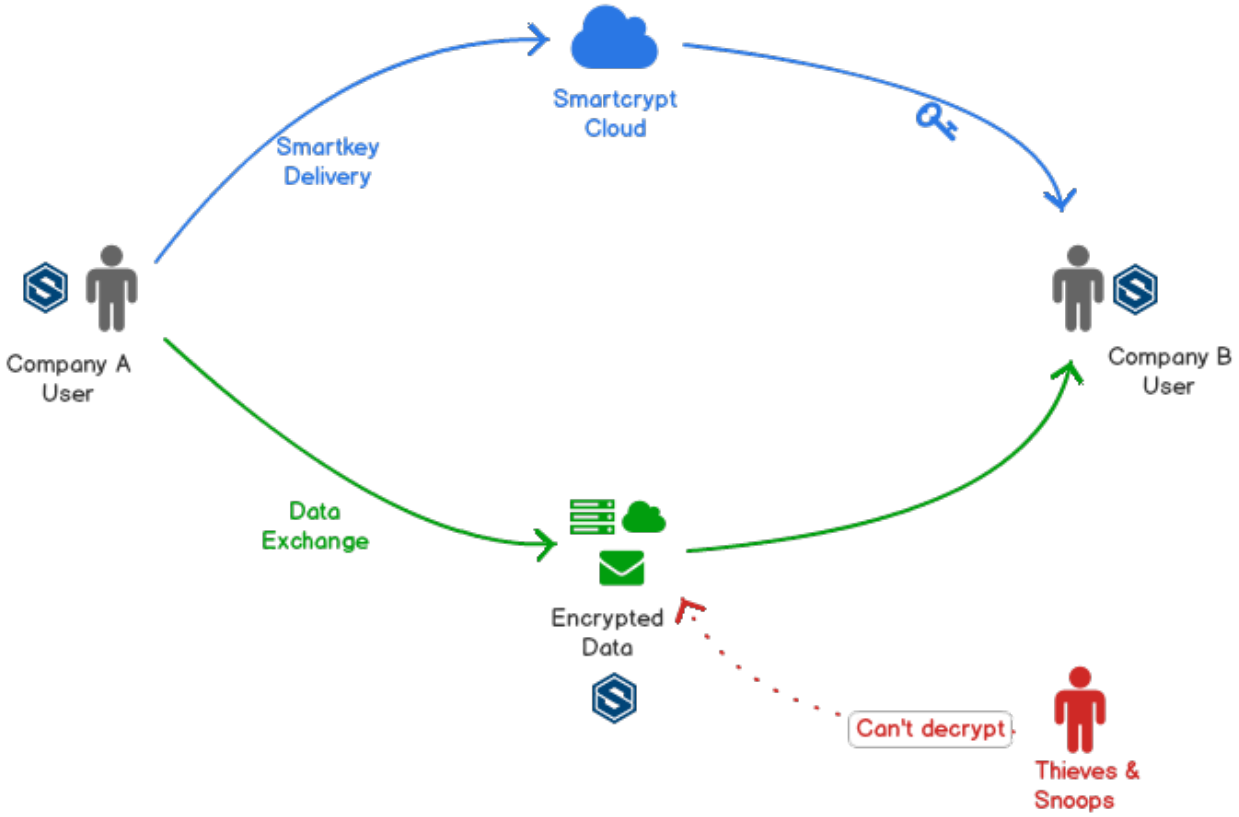


Smartkeys

- Private keys generated client side
- Synced through Smartcrypt Manager to your devices

Smartkeys

- Smartcrypt Cloud performs key exchange
- Data follows normal paths



Data Security Intelligence

Compliance reporting to ensure security mandates and regulation are being met

- What was encrypted? When? Who did it?
- When was it accessed?
- Where were these operations performed? (IP Address, User Device)
- How was it protected? (Smartkey, Passphrase, PGP, X.509, etc.)
- Where did it go? (Email, EFSS, removable media, custom)
- Focus on GRC (PII, PHI, PCI, SOX, etc.)

Smartcrypt Manager

SMARTCRYPT Actions Basics Advanced Reporting Event Log Help Log out

First Day: 12/28/2015 Last Day: Get Events Just Problems Show Help

Events

Show 10 entries Search:

Time	Level	Tags	Event	Message
1/27/2016 10:05:41 PM	Info	Account, Access	Issue Access Token	Successful Issue Access Token - device 66:mkemac-ratliff - user Forrest Ratliff(Forrest.Ratliff@pkware.com)
1/27/2016 10:05:37 PM	Info	Account, Access	Login	Successful Login - user Forrest Ratliff(Forrest.Ratliff@pkware.com)
1/27/2016 9:43:56 PM	Info	Account, Access	Issue Access Token	Successful Issue Access Token - device 73:FORRPC - user Forrest Ratliff(Forrest.Ratliff@pkware.com)
1/27/2016 9:41:13 PM	Info	Account, Access	Issue Access Token	Successful Issue Access Token - device 7:MKEWKS-CORPDEV5 - user Joe Sturonas(joe.sturonas@pkware.com)
1/27/2016 9:40:40 PM	Info	Archive,Extract,Encrypted	Smartcrypt Decrypt	Decrypt Document1.docx Archive=C:\Users\matt_l\Desktop\Document1.zip - device 2:MKEWIN-LITTLE10 - user Matt Little(matt.little@pkware.com)
1/27/2016 9:40:34 PM	Info	Archive,Add,Encrypted	Smartcrypt Encrypt	Encrypt Document1.docx Archive=C:\Users\matt_l\Desktop\Document1.zip - device 2:MKEWIN-LITTLE10 - user Matt Little(matt.little@pkware.com)
1/27/2016 9:40:15 PM	Info	Account, Access	Issue Access Token	Successful Issue Access Token - device 59:mkemac-little - user Matt Little(matt.little@pkware.com)
1/27/2016 9:40:14 PM	Info	Asset, Membership	Allow	Allow Joe Sturonas(joe.sturonas@pkware.com) access to "Demo-Key1" (id=7): by user Matt Little(matt.little@pkware.com)
1/27/2016 9:37:35 PM	Info	Archive,Extract,Encrypted	Smartcrypt Decrypt	Decrypt Document1.docx Archive=C:\Users\matt_l\Desktop\Document1\Document1.zip - device 2:MKEWIN-LITTLE10 - user Matt Little(matt.little@pkware.com)
1/27/2016 9:37:27 PM	Info	Archive,Add,Encrypted	Smartcrypt Encrypt	Encrypt Document1.docx Archive=C:\Users\matt_l\Desktop\Document1\Document1.zip - device 2:MKEWIN-LITTLE10 - user Matt Little(matt.little@pkware.com)

Showing 1 to 10 of 17,743 entries (filtered from 41,303 total entries) Previous 1 2 3 4 5 ... 1775 Next

Event Details

App	MDS
Asset Id	7
Event	Allow
Level	3
Participant Id	7
Tags	Asset, Membership
Text	Allow Joe Sturonas(joe.sturonas@pkware.com) access to "Demo-Key1" (id=7): by user Matt Little(matt.little@pkware.com)
Time	1/28/2016 3:40:14 AM
User Id	3

Time Stored:Today at 21:40:14

SIEM

Event Details

Action	Add
App	Smartcrypt
Archive	C:\Users\matt_l\Desktop\Document1.zip
Category	step
Command	C:\Windows\Explorer.EXE
Contingency Keys	[]
Crl	none
Current Working Directory	C:\Windows\system32
Device Id	2
Encryption Access	Passphrase
Encryption Kms Data	{"assets":[{"smartcrypt-eFW0l9UpKxvT5+uq2RTVZEDkqL,gQXUR-MA_4_DuqCvGIKYOIXJJHeQwsyTtbrdZZej3wnU7ZelgBWWQo=:1":"245fc7c3590a5e92f443b92475071cf81f31d267505feaf1a548596709f6d4b33d6b78dd5b0af7dc45211de389a6fbb9de08502d16adbf1067beb5075453b638"}],"homeServer":"SAT_Qr,dsxzpUjLx8n,Xs0MCR5pFS2McpW,,69JLYXT0Oek=","owner":"MA_4_DuqCvGIKYOIXJJHeQwsyTtbrdZZej3wnU7ZelgBWWQo="}
Encryption Kms Provider	Smartcrypt
Encryption Method	AES (256-bit)
Event	Smartcrypt Encrypt
Fips	False
Fne	False
Host	mkewin-little10.pkware.com
Item	Document1.docx
Level	3
Modified	1/28/2016 3:32:17 AM
Session Id	6244678155309286373
Size	11285
Split Size	auto
Status Code	0
Status Description	OK
Tags	Archive,Add,Encrypted
Task Id	6244678154062526978
Text	Encrypt Document1.docx Archive=C:\Users\matt_l\Desktop\Document1.zip - device 2:MKEWIN-LITTLE10 - user Matt Little(matt.little@pkware.com)
Time	1/28/2016 3:40:34 AM
User	matt_l
User Id	3

Time Stored:Today at 21:40:37

Our Points of Differentiation

- Data level encryption (not device or network)
- Software defined (no hardware/appliances)
- Open standards-based, non-proprietary crypto
- Persistent protection for structured & unstructured data
- Files compressed and encrypted in one step
- Prevents against uncontrolled encryption

How can you get started?

Jason Ramirez
(913) 205-8715
Jason.ramirez@pkware.com