ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Preventing a Data Disaster

Understanding threats, why you're a target and how to deal with them

Audience

- Covering topics for people with entry level IT skills up to a standard IT admin
- Written to address security at a higher level
- Hopefully, give you the tools to address Data Loss Prevention (DLP) in your organisation
- Some of this data has been taken from the Symantec Internet Threat Analysis Report (ITAR) 2016

https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Background

EMT Distribution

- Based in Adelaide
- Focus on the Australian Signals Directorate Top 35
- Provide a wide selection of security software to Australia and New Zealand
- Working closely with ConnectingUp to help bring security solutions to NFP's
- Security is important for everybody

Adam Hack

- Also from Adelaide!
- Pre-Sales/Solutions Engineer
- Also handle technical support
- Been working in IT for 10 years
- Started at Adam Internet (now TPG)
- Yes that's my real last name

Why take it seriously?

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Breaches in 2015

- 429 million identities were exposed
  - A rise of 23 percent from 2014

- Of just the reported breaches, 113 did not give a figure of identities taken
  - Taken into account, the final number would be more than 500 million

That's over 17 x AU & NZ combined!

Source, ITAR 2016 pg53

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Bureau of Meteorology

- ‘Major Cyber Attack’ in 2015
- Targeted their supercomputer
- But why?
  - Openly display their information
  - Easily accessible, not hiding data

It wasn’t the BoM that was the goal, it was who they had access to

Australian Government
Austrade

Australian Government
Department of Defence

You are a target

- It may not be your own data, but it easily could be data of who you do business with, partnerships, joint-efforts etc.

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

What is a threat?

Simple look at what you're up against

Vectors

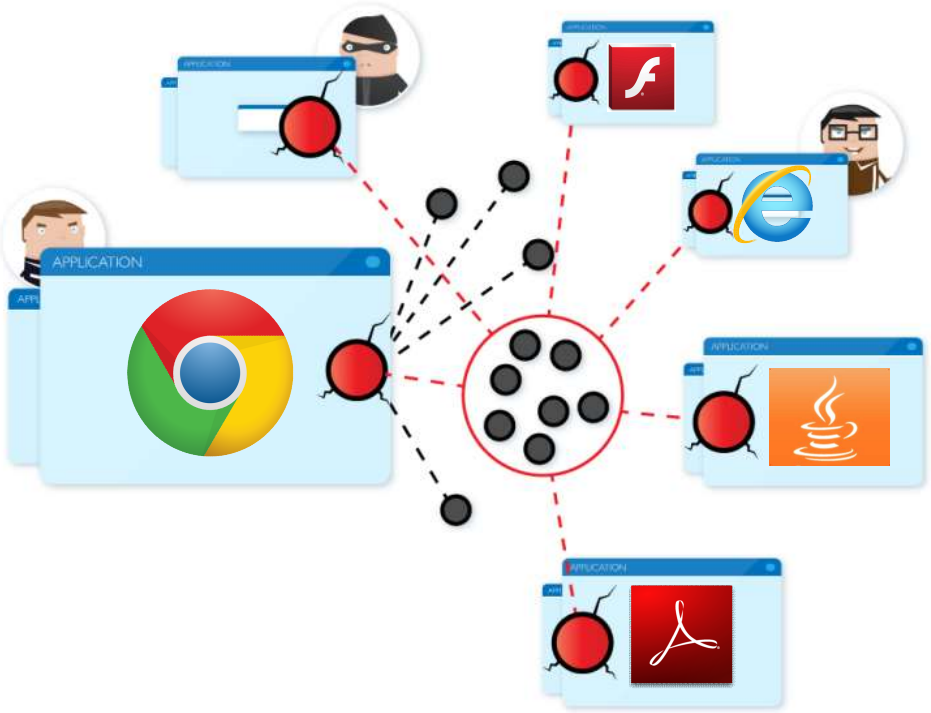
- ’Typical’ virus, trojan or worm
- *New* ransomware
- APT’s
  - (A talk for another day)
- **Data-exfiltration**
  - **Maliciously, innocently, by an employee or by anybody**

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Typical Virus, Ransomware etc

Software vulnerabilities – Flaws in the way an application is written



- Flaws in the code:
  - Security risk
  - Functionality issues
- Where are those applications?
  - Servers
  - PCs, laptops
  - Mobile devices
  - Printers, switches, routers
  - Business and domestic appliances!

Most ransomware takes advantage of these flaws to drop the file onto your machine


VV 0
Your personal files are encrypted!
Your private key will be destroyed on:
4/13/2015
Time left: 00:00
Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site
and follow the instruction.
in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.42k2bu15.com
https://34r6hq26q2h4jkzj.tor2web.blutmagie.de
Use your Bitcoin address to enter the site:
1MQrnrWHRo52jt32eUzpNcarSJM
Click to copy address to clipboard
if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address 34r6hq26q2h4jkzj.onion
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.
Click for Free Decryption on site
Show files
Enter Decrypt Key

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Things to ponder

- If your organisation was hit tomorrow with one of the ‘lockers’, would you lose your data?
- What would it cost you to recover?
- Would you pay the ransom?
  - Are you sure you would get your data back?

And what's more, is paying the ransom actually funding crime?

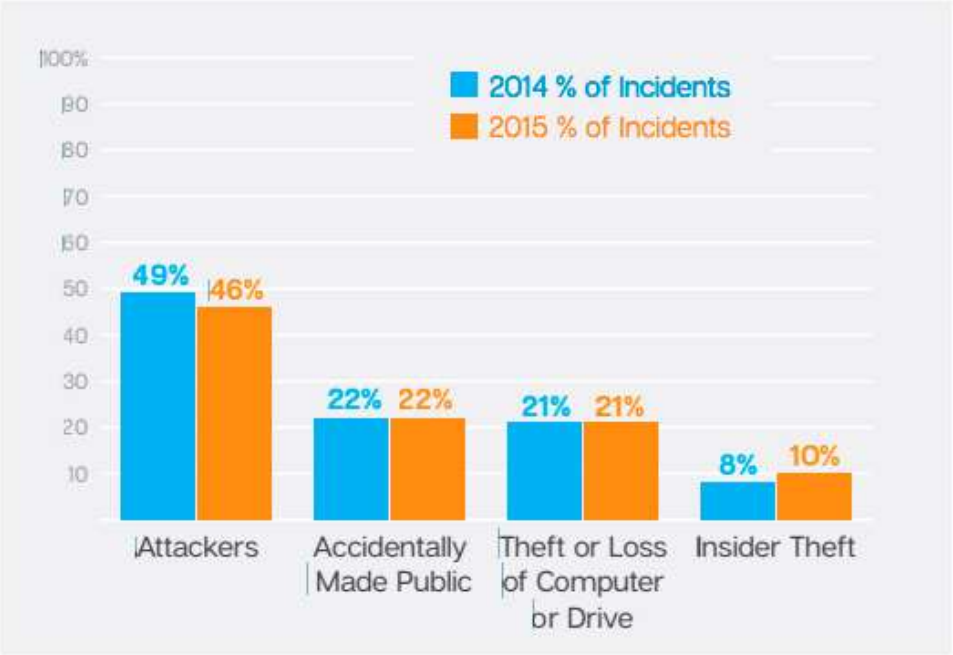
ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Data Exfiltration

Data Exfiltration

- The “unauthorised transfer of sensitive information”

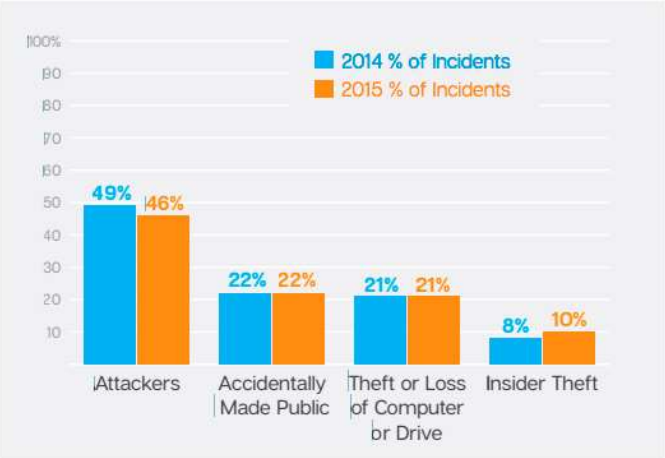


Top Causes of Data Breach by Incidents

46% attributed to attackers
53% attributed to **employees**

Source, ITAR 2016 pg53

Data Exfiltration



Top Causes of Data Breach by Incidents

- Accidently made public?
  - Sent to the wrong person
  - Uploaded to websites
  - Public folders
- Loss of a drive
  - USB falls out of a pocket
  - Accidently left behind
- Insider Theft
  - Disgruntled employee
  - Paid data theft

It happens, and it happens all the way up the corporate tree!

Source, ITAR 2016 pg53

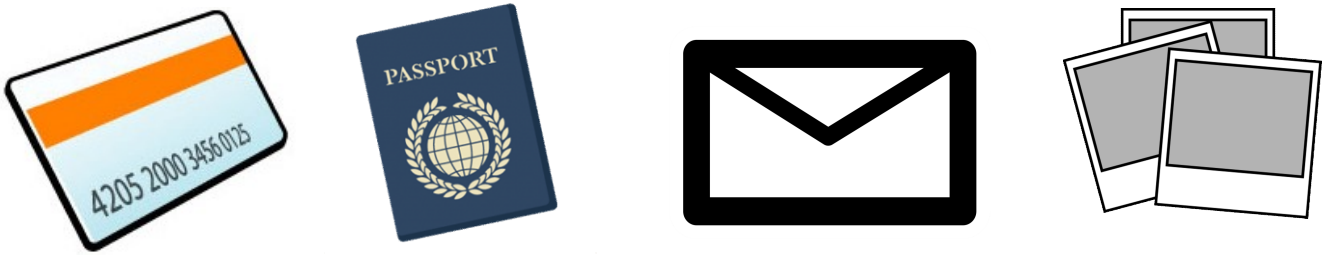
ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Data Exfiltration

- The challenge?
  - Balance out securing data while giving enough control to work day to day
  - It's easy to lock down everything, but if this gets in the way of legitimate organisation workflows users will push back

The first step is to establish what you are wanting to protect



So what do we do?

Let’s have a look at the first steps

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Device Control vs Content Control

Controlling based on which devices are plugged into the network

vs

Controlling what content is being transferred, regardless of which device

Or a combination of both?

Examples of what you can see

Device Control

USB Flash Drive being copied to:

File Read	CBRWKS1	FLASH_DISK	Administrator	USB Storage Device	E:/IPH.PH
File Write	CBRWKS1	FLASH_DISK	Administrator	USB Storage Device	E:/IPH - Copy.PH
File Copy	CBRWKS1	FLASH_DISK	Administrator	USB Storage Device	E:/IPH.PH -> E:/IPH - Copy.PH
File Copy	CBRWKS1	FLASH_DISK	Administrator	USB Storage Device	C:/IPH.PH -> E:/IPH.PH
File Read	CBRWKS1	FLASH_DISK	Administrator	USB Storage Device	E:/EasyLock.exe

Content Aware

JPEG blocked from being emailed

Content Threat Blocked	CBRWKS11	hbirdman	Disable Picture Files	E-mail	Mozilla Thunderbird	C:/Documents and Settings/All Users/Documents/My Pictures/Sa...	image/jpeg
Content Threat Blocked	CBRWKS11	hbirdman	Disable Picture Files	E-mail	Mozilla Thunderbird	C:/Documents and Settings/All Users/Documents/My Pictures/Sa...	image/jpeg
Content Threat Blocked	CBRWKS11	hbirdman	Disable Picture Files	E-mail	Mozilla Thunderbird	C:/Documents and Settings/All Users/Documents/My Pictures/Sa...	image/jpeg
Content Threat Blocked	CBRWKS11	hbirdman	Disable Picture Files	E-mail	Mozilla Thunderbird	C:/Documents and Settings/All Users/Documents/My Pictures/Sa...	image/jpeg

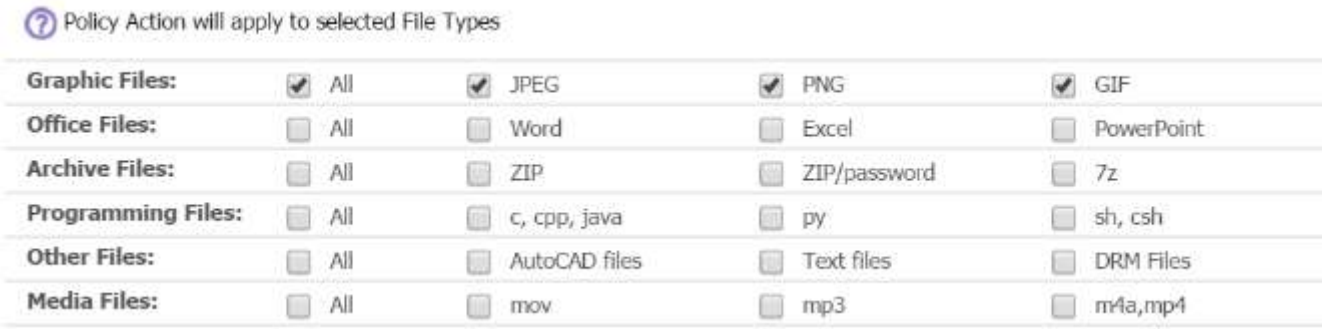
From CoSoSys Endpoint Protector 4

Deciding what's important

- What is critical to the organisation?
  - Financial Records
  - Personal Data
  - Credit Cards
  - Bank Details
  - Images/Photos

Going granular

- Do you want to block based on the actual file?
  - JPEG, PNG, GIF
  - Word, Excel, Powerpoint, PDF
  - Zip, RAR, 7z
  - Programming files (c, py etc)
  - Media (.mov, .mp3, .mp4)



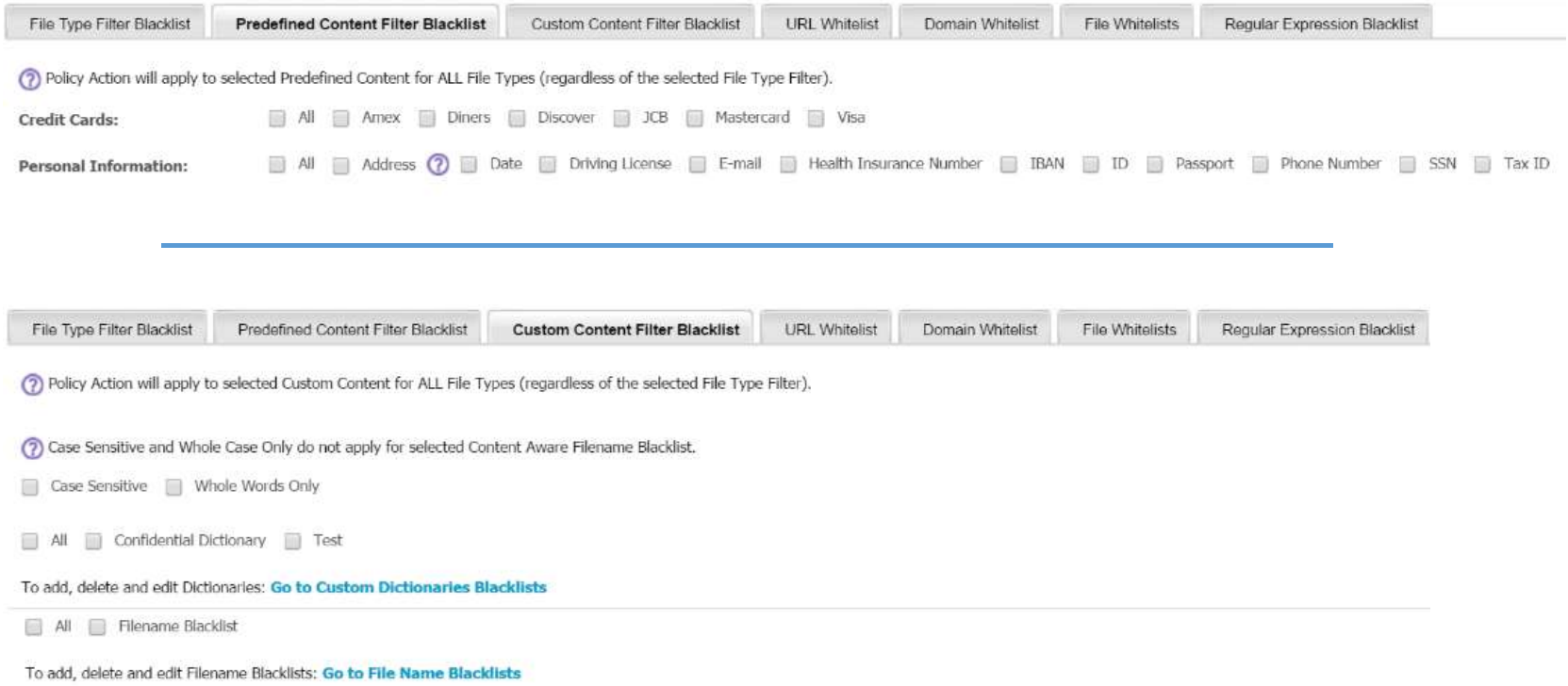
From CoSoSys Endpoint Protector 4

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Going granular part 2

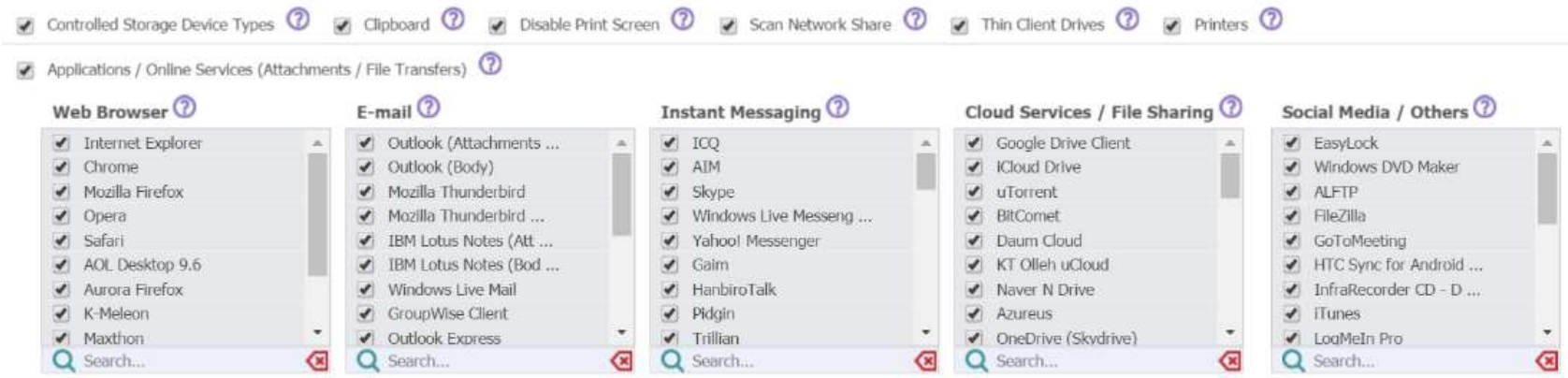
Content Filters



From CoSoSys Endpoint Protector 4

You've established what, now where

- USB isn't the only way to get data off the network
  - Google Drive
  - Dropbox
  - Skype
  - Outlook



From CoSoSys Endpoint Protector 4

Encryption

- Copying data to USB but keeping it protected
- Can enforce it on any USB, or particular approved ones
- Encryption can be as basic as a program you run on the USB, to special hardware with a fingerprint scanner
- Most DLP solutions should be able to natively work with an encryption solution

Mobile Device Management

- **In 2015 more than 1.4 billion smartphones were bought**
- Remember, these devices are effectively an extremely mobile, small, powerful computer
  - They still need to be protected
  - Be aware of what data they can access
  - A phone without a password/code is an accident waiting to happen

https://gaspull-geeksaresexytech.netdna-ssl.com/wp-content/uploads/2013/01/nasa-smartphone.jpg

Auditing vs Enforcing

- Do you want to just watch and audit, or do you want to enforce restrictions on the user base?

Auditing		Enforcing	
Pro's	Con's	Pro's	Con's
• No user restrictions • Quietly watch users • Log everything without impeding	• Can't stop data being removed	• Protect data from being removed • Also able log users behaviour • Proper data loss prevention	• Policies need to be set correctly

The most important thing is not to just say "it's too hard" and fail to do it at all

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

How does it look?

What should the end user expect to see?

Endpoint Protector 4

Tray Icon

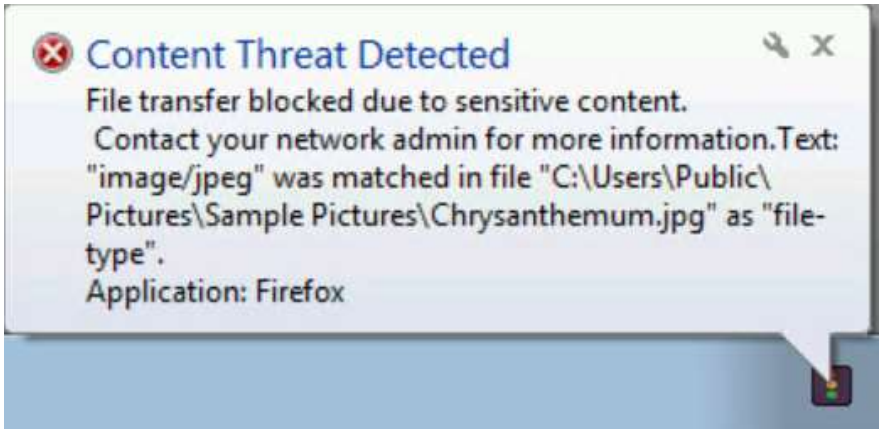
Application

In this case, the only reason you would need to open the application would be to over-ride an existing setting

From CoSoSys Endpoint Protector 4

Something being blocked:

Trying to upload a picture via Firefox

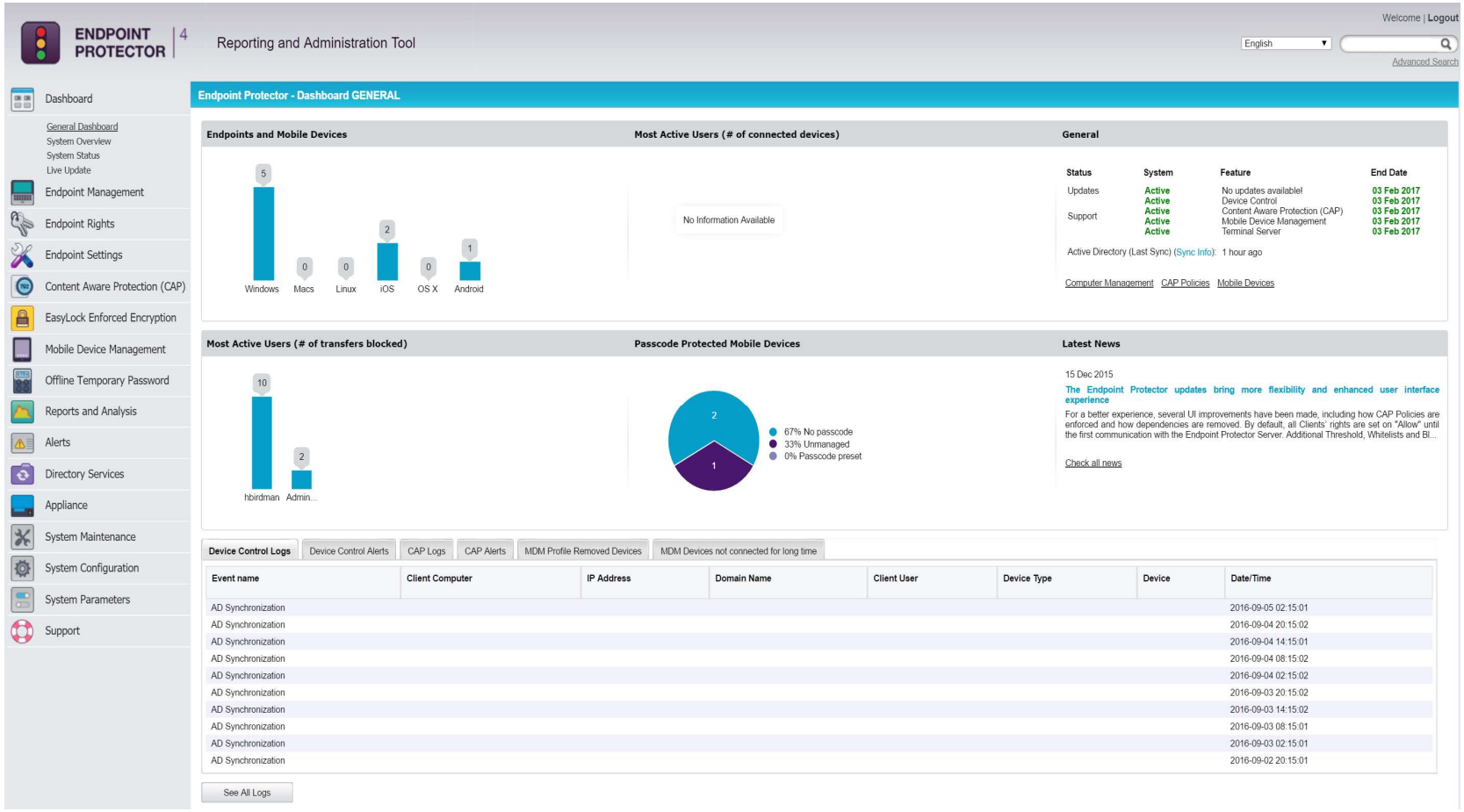


In this case the policy was to block all picture files from being transferred, because the machine was trying to upload a file via Firefox it was blocked.

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

How about the admin?



From CoSoSys Endpoint Protector 4

ENDPOINT PROTECTOR | by CoSoSys

emt | TECHNOLOGY DISTRIBUTION

Conclusion

Conclusion

- It’s not difficult to implement a good solution
- Planning is key
- As an organisation you need to know what is worth protecting
- Correctly set-up a good solution will look after itself, be low touch and minimal end user contact
- Remember:
  - **You are a target**
  - Reporting will eventually become mandatory
  - Implement solutions early and save yourself the headache later on

Questions?

Always feel free to contact me

adam.hack@emtdist.com