HEAT software

Heat Software

Cloudsec 2016

Ransomware – The New Normal in Malware

Liam Puleo


Lets start with a few stats…

HEAT software

- *"Of the **15%** that reported a security breach in 2015, **42%** have been hit with ransomware, **10%** reported 'significant disruption to systems' and **11%** said they'd lost data"*
  InfoSecurity Magazine Survey, January 2016

- *Fake technical support scams rose by **200%** and crypto-based ransomware attacks grew by **35%***
  BBC April 16

- *CryptoWall Ransomware Cost Users **£225M** in **2015**, Lavasoft November **2015***
  Lavasoft November 2015

- In 2015, there were **9** breaches that exposed more than **10 million** records. By contrast, in 2014 only four breaches were this severe
  BBC April 16

Infosecurity Magazine:

31% of organisations admit paying a ransom

ANATOMY OF A CYBER ATTACK:

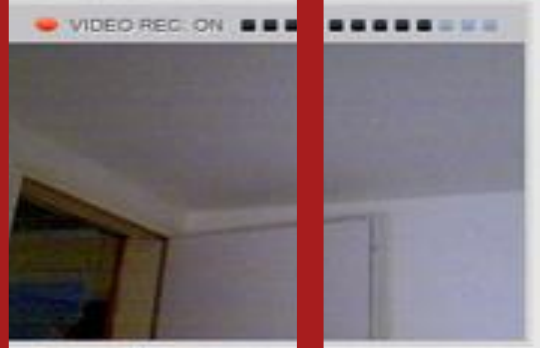
ransomware

METROPOLITAN POLICE

DEPARTMENT OF CYBERCRIME

ATTENTION !

YOUR PC IS BLOCKED DUE TO AT LEAST ONE OF THE REASONS SPECIFIED BELOW



YEAR	DAY	MONTH	TIME	TYPE OF VIOLATION

IP-ADRESSE	ISP	PLACE

Serial number of violations

TC-BZXCCDD/FF

You have been violating Copyright and Related Rights Law (Video, Music, Software) and illegally using or distributing copyrighted content, thus infringing Article 128 of the Criminal Code of Great Britain. Article 128 of the Criminal Code provides for a fine of two to five hundred minimal wages or a deprivation of liberty for two to eight years.

You have been viewing or distributing prohibited Pornographic content (Child Pornography, Pedofilia and etc). Thus violating article 202 of the Criminal Code of Great Britain. Article 202 of the Criminal Code provides for a deprivation of liberty for four to five years.

Illegal access to computer data has been initiated from your PC, or you have been.... Article 208 of the Criminal Code provides for a fine of up to €100,000 and/or a deprivation of liberty for four to nine years.

Illegal access has been initiated from your PC without your knowledge or consent, your PC may be infected by malware, thus you are violating the Law On Neglectful Use of Personal Computer. Article 210 of the Criminal Code provides for a fine of €2,000 to €8,000.

PayPal

Enter your card number *

example: 4444 4444 4444 4444

ukash

Enter your card number *

example: 4444444444444444

paysafecard

Enter your card number *

example: 4444444444444444

Strafe zahlen

Please choose one of methods of payment

Norton by Symantec

AVIA Agip Esso OMV Q1 Westfalen epay

Metropolitan Police Service New Scotland Yard Broadway London SW1H 0BG

Ransomware is a type of malware that holds to ransom an infected computer system in some way, and demands that the user pay a monetary ransom to the malware operators in order to remove the restrictions.

Example of CryptoRansomware

Crypto-Ransomware is an extremely malevolent type of malware that encrypts the infected computer system's data in some way, and demands that the user pay a ransom to the malware operator in order to receive a decryption key.

ANATOMY OF A CYBER ATTACK:

ransomware

1 → 2 → 3 → 4 → 5 → 6 → 7 → 8 → 9

DELIVERY

LEVERAGE A MECHANISM FOR DELIVERY OF RANSOMWARE

PHISHING
Email attachment commonly disguised as ZIP, PDF, or SCR.

EXISTING BOTNET
Uses computers already infected but dormant.

DRIVE-BY DOWNLOAD
Lures victims to questionable or legitimate sites through social engineering.

MOBILE: BAD APPS
Malware built into apps such as games or productivity helpers.

MALVERTISING
Legitimate-looking banner ads on legitimate sites which cause download when clicked.

EXPLOIT

FIND A VULNERABILITY ON VICTIM MACHINE TO EXPLOIT

OPERATING SYSTEM & 3RD PARTY APPS

Typically exploits older vulnerabilities since these need to be coded into the malware kits first.

VULNERABLE BROWSERS

Inadequate security caused by browser vulnerabilities and misconfigurations.

INSTALL

RANSOMWARE INSTALLS ITSELF ON VICTIM MACHINE. TYPICALLY DISGUISES ITSELF AS ANOTHER PROCESS SUCH AS 'EXPLORER.EXE' AND ALSO INJECTS ITSELF INTO OTHER BENIGN PROCESSES SUCH AS 'SVCHOST.EXE'

Disarm

LOWER THE SECURITY POSTURE OF THE VICTIM MACHINE TO CREATE AN ENVIRONMENT WHERE RANSOMWARE CAN SUCCEED

DETECT SHADOW COPIES

Secure deletion of shadow copy files using vssadmin.exe so that file restore operations won't be possible.

DISABLE WARNINGS

Disable warnings to victim about non-secure network/browser connections.

ALTER PROXY INFO

Change or clear any proxy information.

OCCUPY

ESTABLISH COMMUNICATIONS TO COMMAND AND CONTROL SERVER

MAKE A CONNECTION

Depending on the variant, could use hard-coded or dynamically generated URLs on the web, Tor URLs, or I2P network servers.

'SEE' THE VICTIM

Victim machine communicates certain identifiers for that machine to the server.

CUSTOMIZE THE ENVIRONMENT

Server responds with data about the machine's location, language-appropriate UI elements for the user interface, a unique payment portal URL for that machine and possibly a unique encryption key for that machine.

TAKE HOSTAGES

Ransomware does not typically encrypt files prior to establishing contact with the server—with the exception of CTB-Locker (Critroni.A) which encrypts the files before contacting server to avoid early detection.

encrypt

ENCRYPT DOCUMENTS, IMAGES, AND MEDIA ACCESSIBLE TO THE VICTIM'S MACHINE

HARDCODED EXTENSIONS

Selectively uses a hardcoded list of extensions in order to keep the OS and ransomware running. The list has grown from 44 extensions in 2005 to over 230 in 2014.

NO BACKTRACKS

Proceeds alphabetically or reverse alphabetically through folder names and files within the folder, processing one folder at a time. Doesn't backtrack.

EVEN REMOVABLES UNSAFE

Also encrypts files on network locations and removable storage which have been assigned a drive letter.

ENCRYPTION KEY STRENGTH

Encryption key strength has risen from 660 bytes in early GPCode to a claimed 3072 byte key in CTB-Locker.

demand ransom

THE RANSOMWARE DISPLAYS A MESSAGE TO THE VICTIM INFORMING THEM THAT THEIR IMPORTANT FILES HAVE BEEN ENCRYPTED. THE MESSAGE LETS THEM KNOW HOW MUCH TO PAY, HOW LONG THEY HAVE TO PAY IT, WHAT PAYMENT METHODS ARE ACCEPTED, AND WHERE TO DIRECT THEIR PAYMENT. BITCOIN IS THE PREFERRED PAYMENT METHOD. BITCOIN IS DIFFICULT TO TRACE AND BTC LAUNDERING SERVICES ARE COMMON.

negotiate

IN SOME CASES, ANECDOTALLY, VICTIMS HAVE BEEN ABLE TO NEGOTIATE A LOWER RANSOM BASED ON THEIR STATUS AS A CHARITY, STUDENT, OR INABILITY TO PAY THE FULL RANSOM.

CUSTOMER SUPPORT

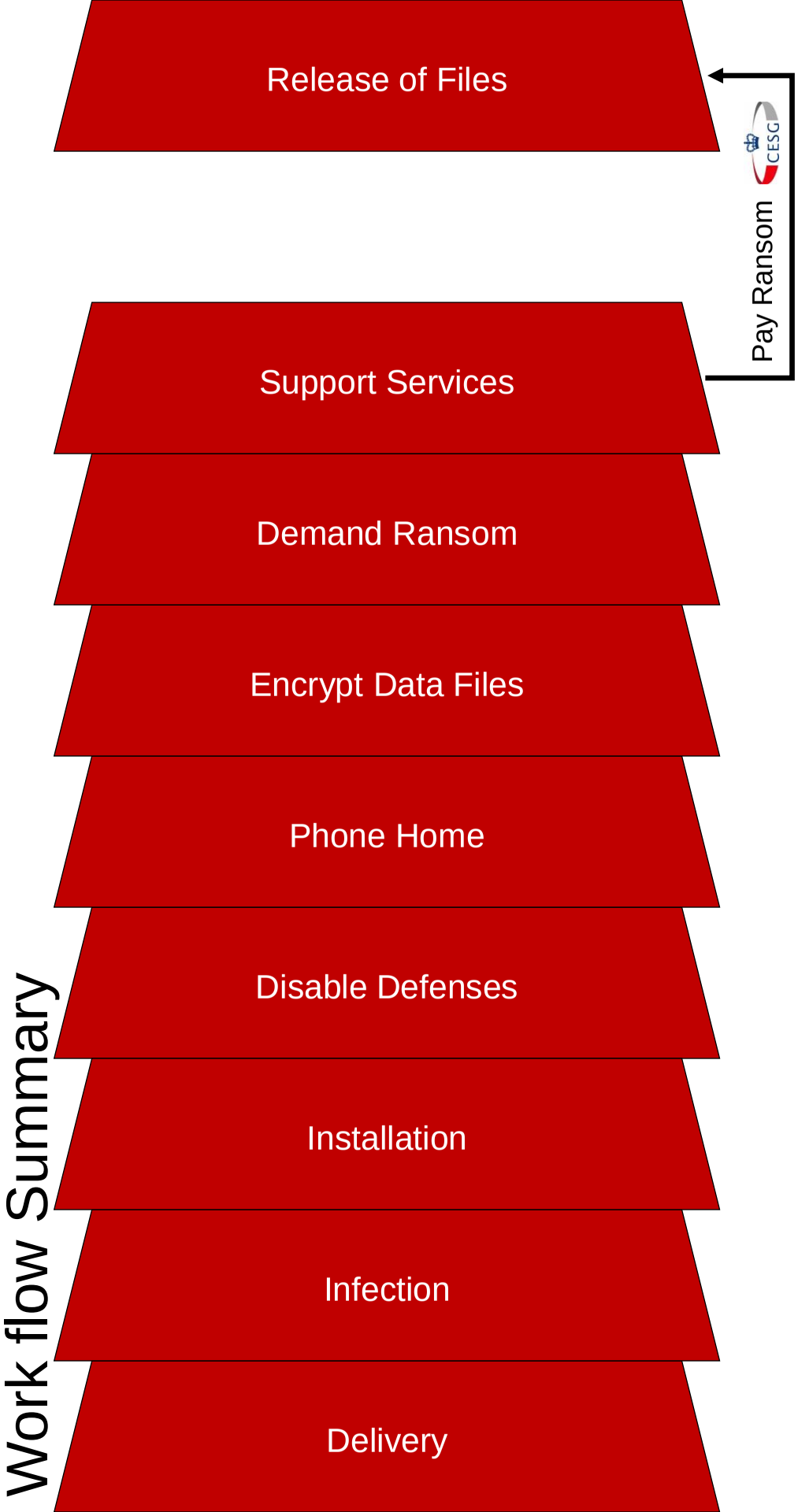
Some ransomers provide forums for support. Victims can get advice on installing Tor, buying Bitcoins, etc.

FREE SAMPLES

Some ransomers allow for the decryption of one or more files for free as proof that the ransomer can restore the files once the ransom has been paid.

Decrypt

ONCE THE RANSOM HAS BEEN PAID, THE FILES ON THE VICTIM MACHINE ARE TYPICALLY DECRYPTED. THERE ARE NO HARD STATS, BUT ANECDOTAL REPORTS OF PAYING AND NOT HAVING FILES DECRYPTED ARE FEW. THE VICTIM MAY RECEIVE A DECRYPTION KEY TO TYPE INTO THE RANSOMWARE ON THEIR COMPUTER. OTHERS MAY DOWNLOAD A DECRYPTION UTILITY FROM THE PAYMENT PORTAL OR OTHER UNIQUE URL GIVEN TO THEM THROUGH THE RANSOMWARE UI. ONCE THE DECRYPTION UTILITY RUNS, THE FILES ARE RESTORED. HOWEVER – THE RANSOMWARE IS NOT NECESSARILY REMOVED, AND THE SECURITY SETTINGS COMPROMISED IN STEP 4 ABOVE ARE NOT RESTORED.

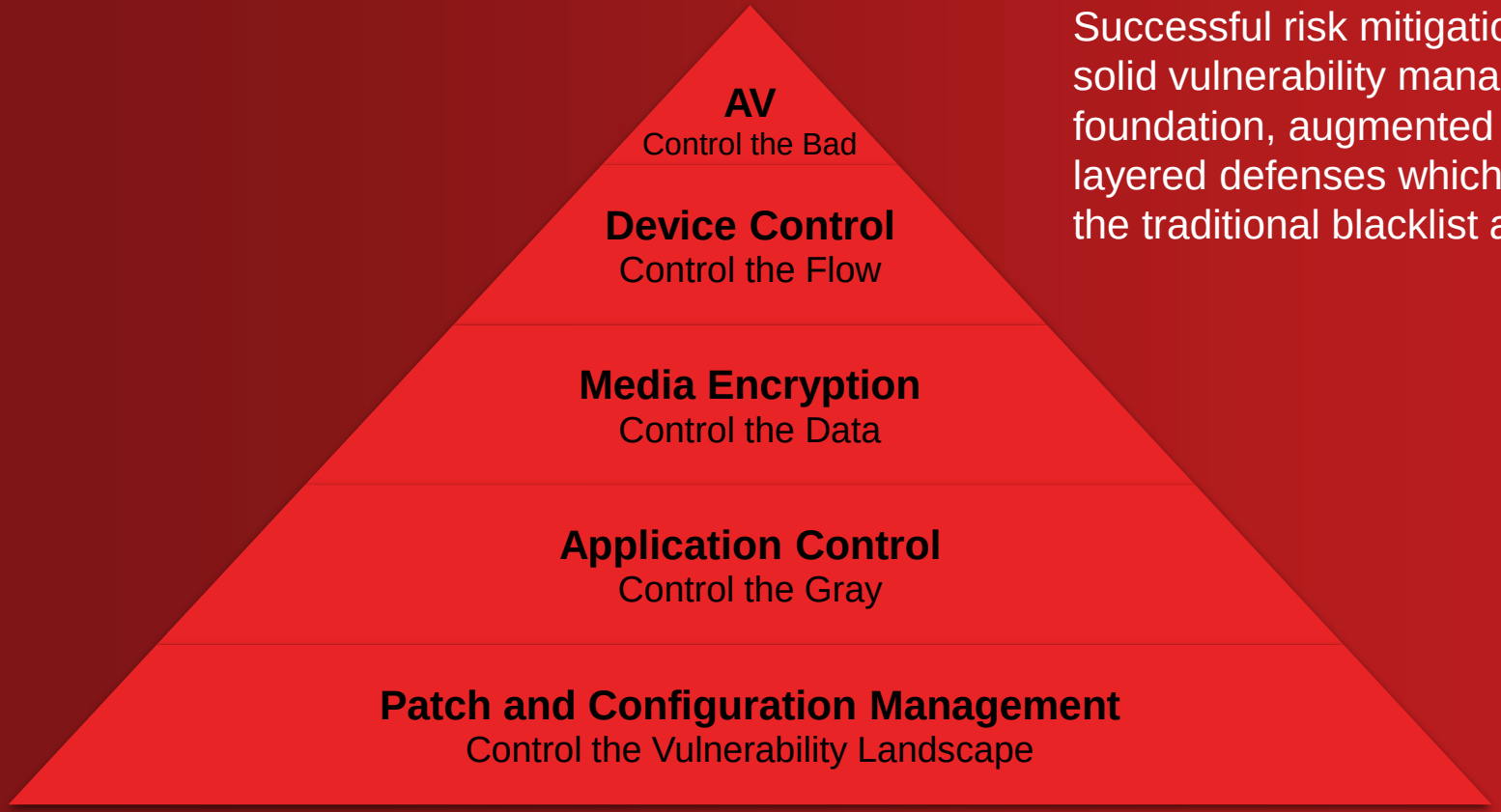

Release of Files
Pay Ransom
Support Services
Demand Ransom
Encrypt Data Files
Phone Home
Disable Defenses
Installation
Infection
Delivery
Work flow Summary

Are your ransomware defences ready?

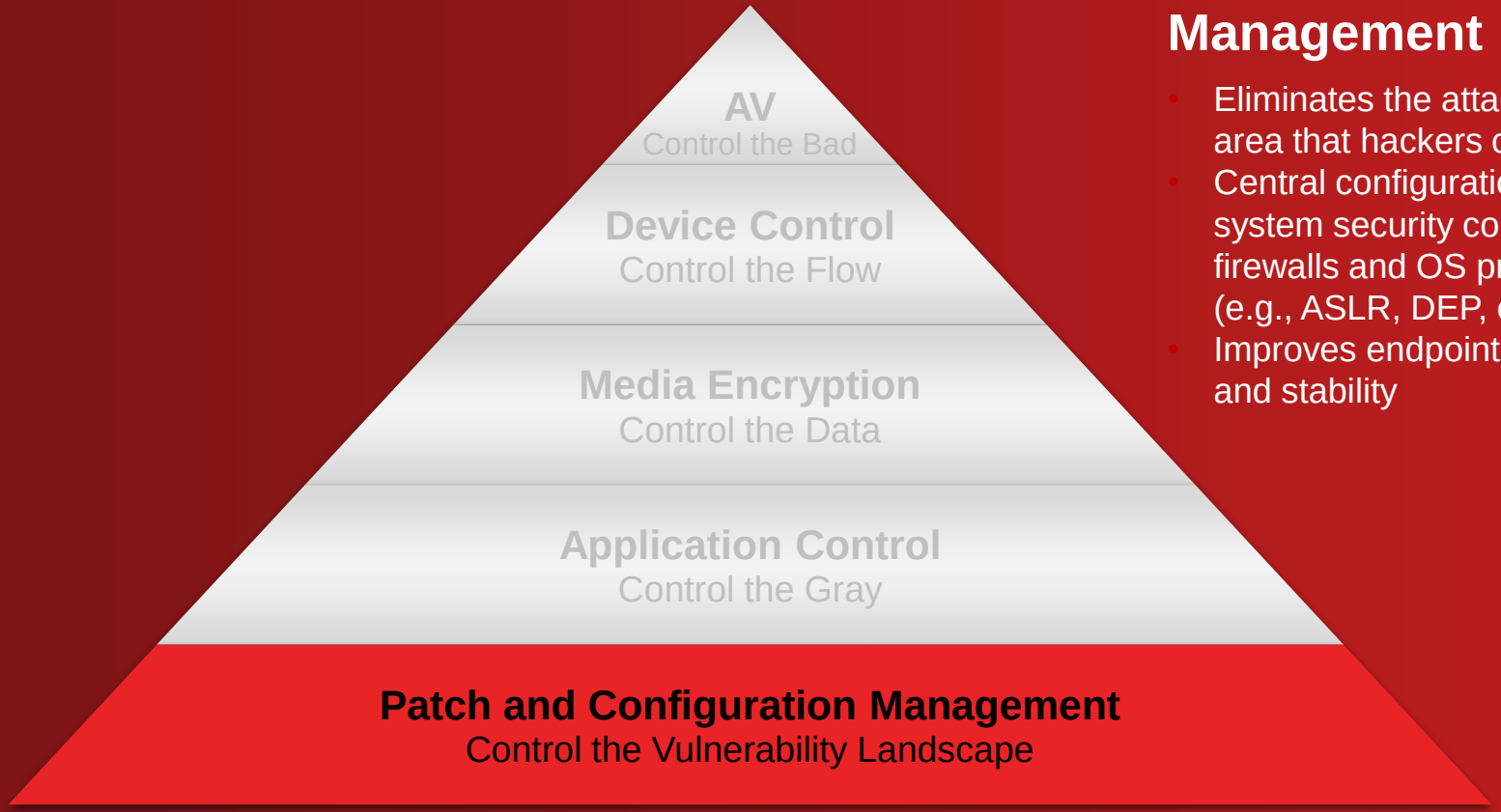
Recommendations

Endpoint Defense-in-Depth

Successful risk mitigation starts with a solid vulnerability management foundation, augmented by additional layered defenses which go beyond the traditional blacklist approach.



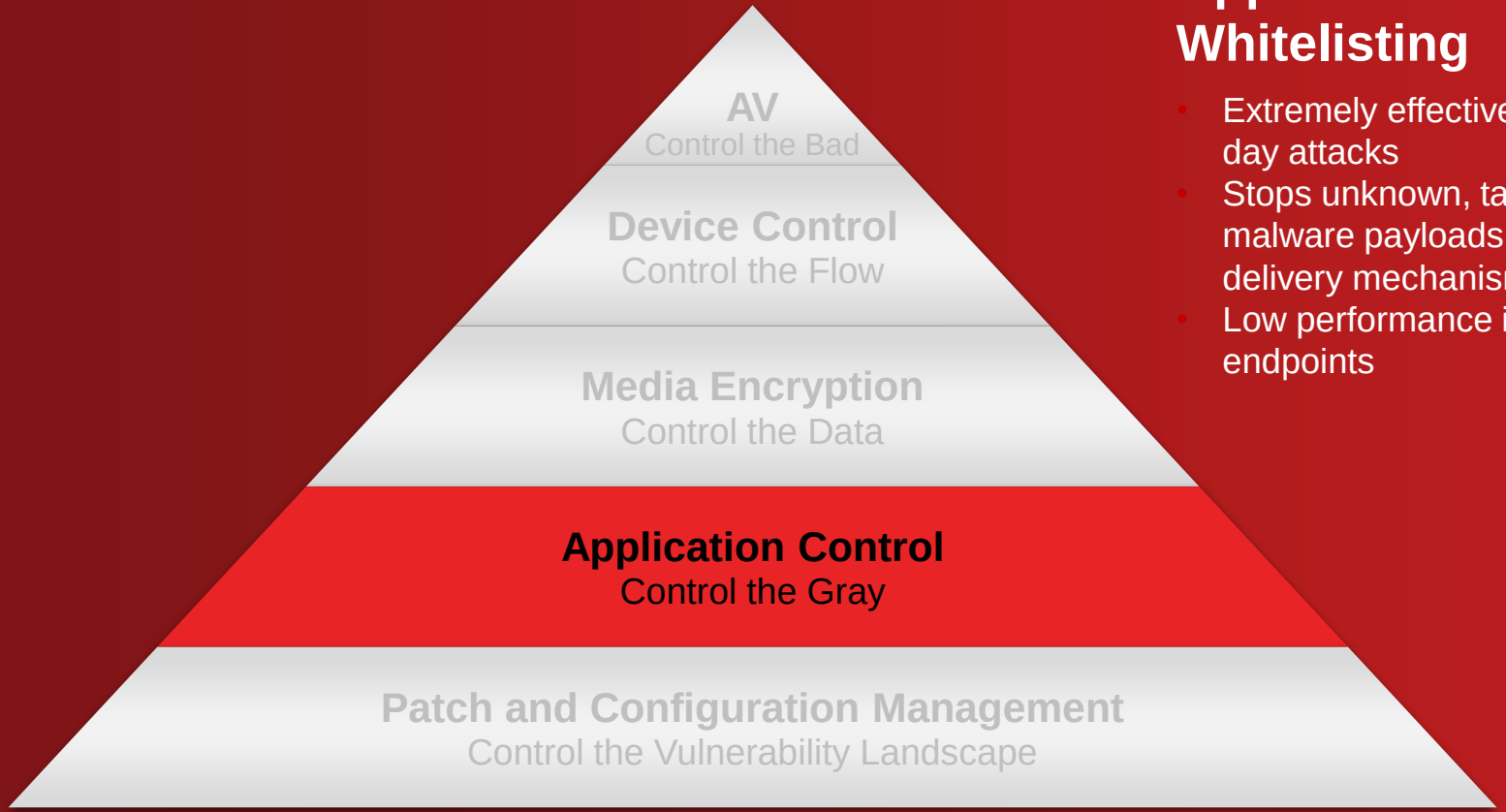
Recommendations



Patch & Configuration Management

- Eliminates the attackable surface area that hackers can target
- Central configuration of native system security controls such as firewalls and OS protections (e.g., ASLR, DEP, etc.)
- Improves endpoint performance and stability

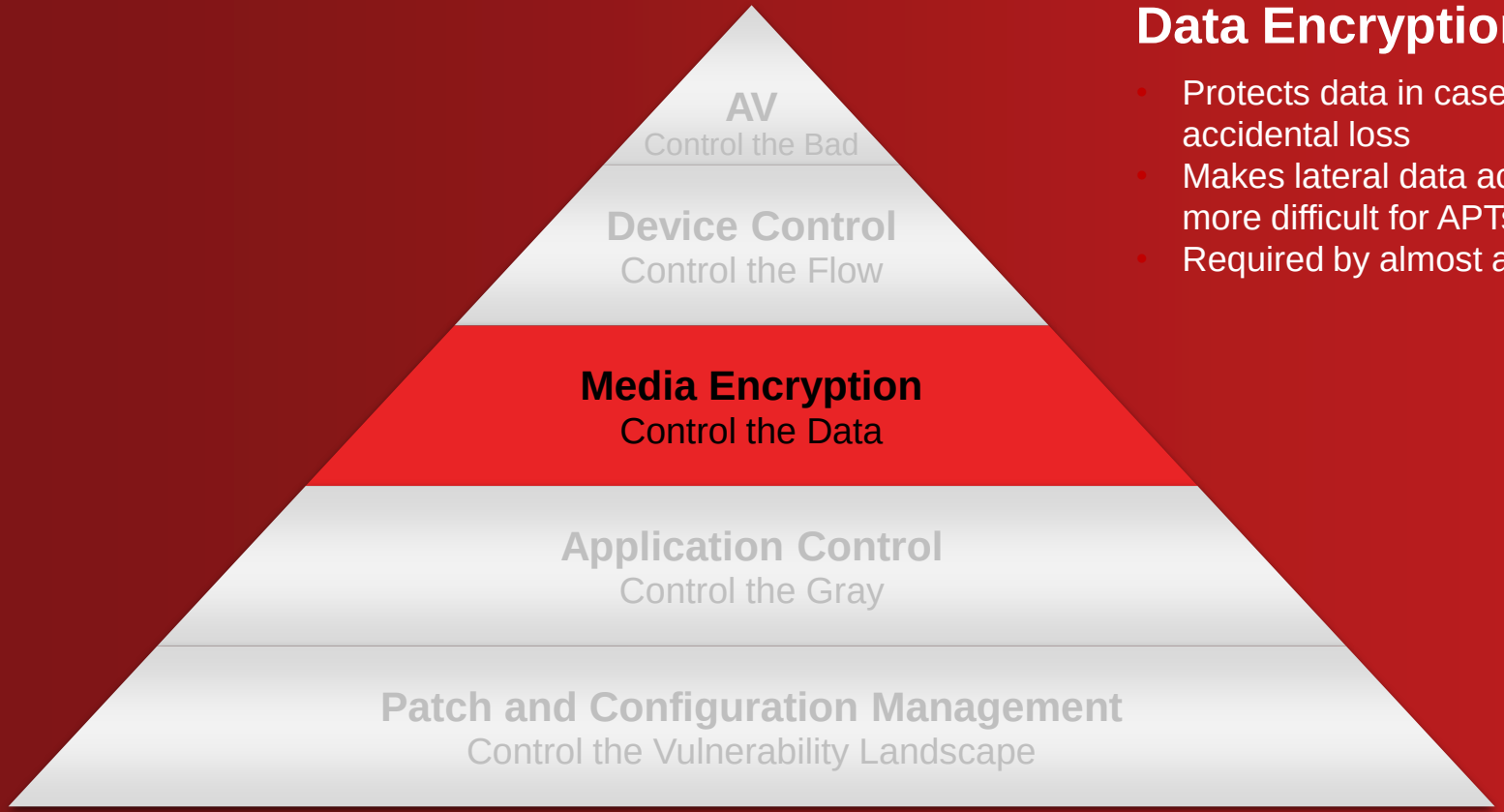
Recommendations



Application Whitelisting

- Extremely effective against zero-day attacks
- Stops unknown, targeted malware payloads, regardless of delivery mechanism
- Low performance impact on endpoints

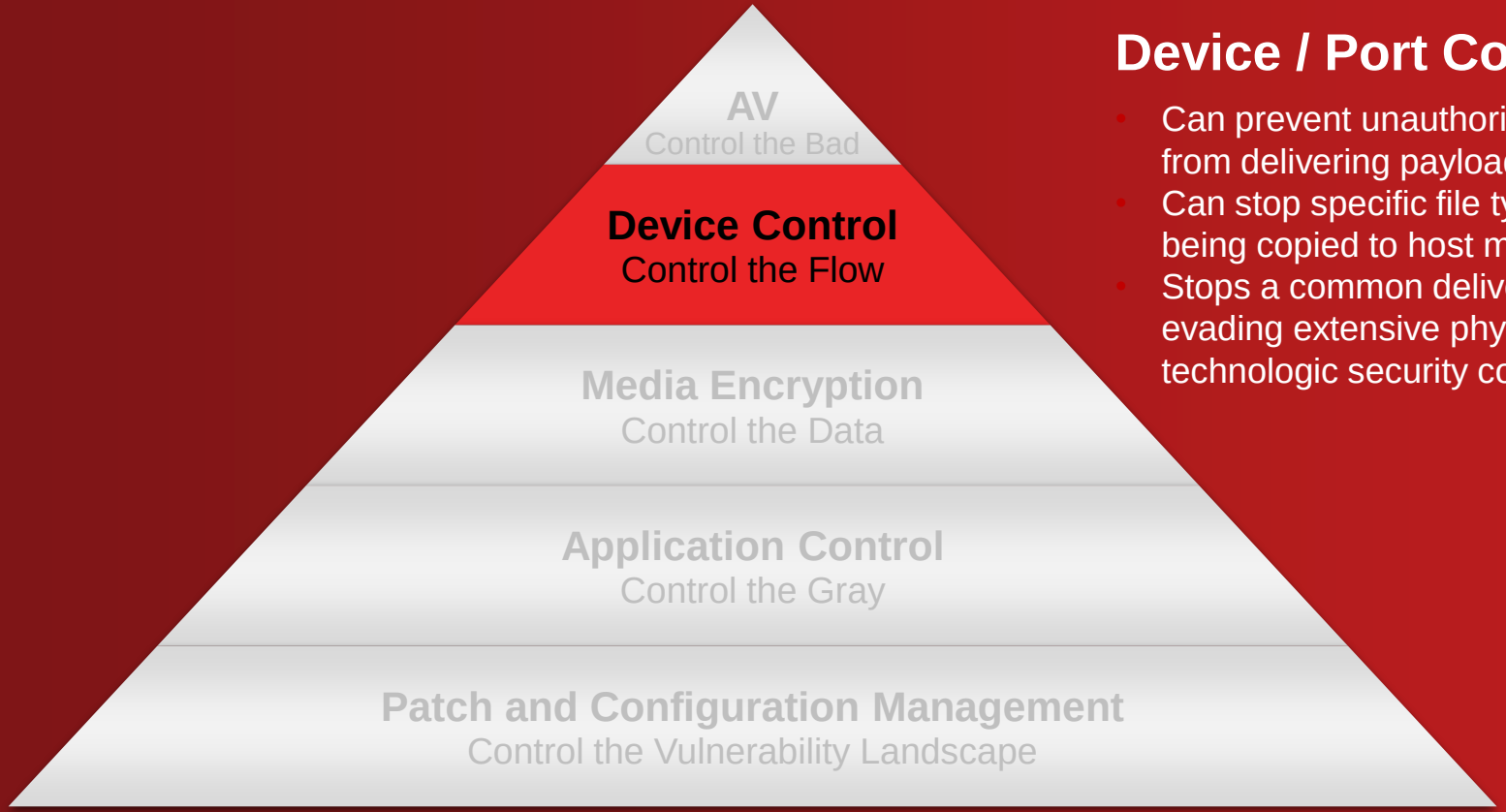
Recommendations



Data Encryption

- Protects data in cases of theft or accidental loss
- Makes lateral data acquisition more difficult for APTs
- Required by almost all regulations

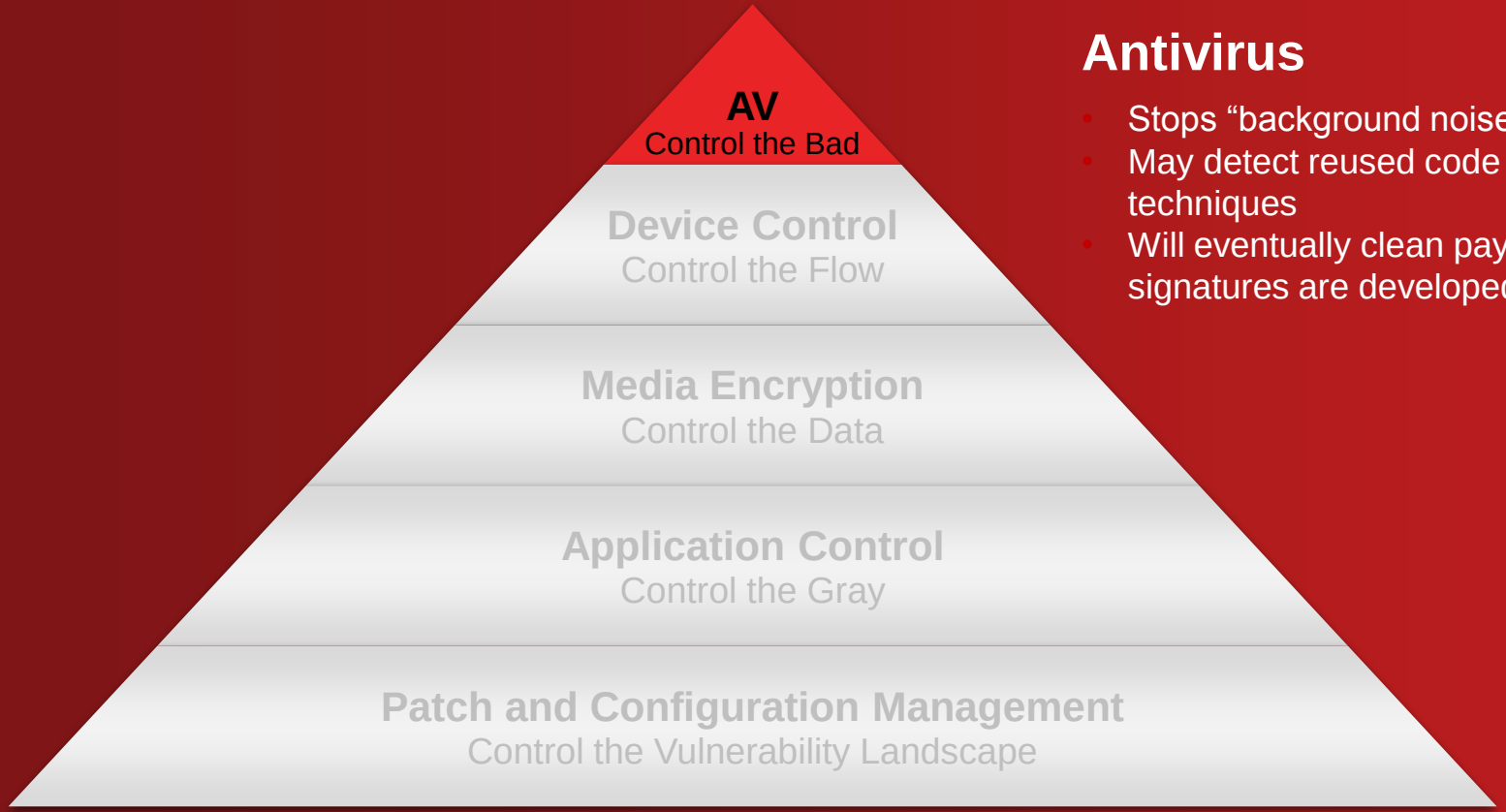
Recommendations



Device / Port Control

- Can prevent unauthorized devices from delivering payloads
- Can stop specific file types from being copied to host machines
- Stops a common delivery vector for evading extensive physical and technologic security controls

Recommendations



Antivirus

- Stops “background noise” malware
- May detect reused code and evasion techniques
- Will eventually clean payloads after signatures are developed

Ransomware Preparedness Checklist

- [x] **User Education**
  It all starts with users. Make them aware of the prevalence of ransomware. Share information about suspect emails, safe browsing practices, and malvertising.

- [x] **Security Reporting System**
  Leverage your ITSM system to create a way for your users to report, and learn about, phishing attempts that might lead to ransomware attack.

- [x] **Incident Response Plan**
  Update your IR plan to cover a ransomware attack, and practice it from detection to recovery to ensure all components of the procedure work

- [x] **Data Backup Plan**
  Implement a 3-2-1 Data Backup Plan. 3 copies of every file – the original and 2 backups. Backups should be on 2 different media, and 1 copy must be kept offsite

Ransomware Preparedness Checklist – Contd.

Application Control
In a whitelisted environment, unapproved and untrusted programmes such as ransomware are not able to execute from a file on a disk

Memory Injection Protection
Some ransomware variants inject themselves into legitimate processes without using a file on a disk. Memory Injection Protection monitors legitimate processes for such suspicious activity, and terminates the process when it has been compromised

Centralised Patch Management
Operating systems, native and third-party applications, plug-ins and add-ons all need to be patched to current levels. Ransomware needs a vulnerability to exploit. The fewer available which exist in your environment, the more secure it is

Secure Browser Settings
Enforce a restrictive but reasonable browser configuration for Internet Explorer, Chrome, Firefox, Safari and any other browsers in your environment.

Recommendations

Network Defences

Endpoint Defense-in-Depth

- ✓ Patch and Configuration Management
- ✓ Application Whitelisting
- ✓ Data Encryption
- ✓ Device Control
- ✓ Antivirus

Preparation

- ✓ Back-ups
- ✓ Staff Training
- ✓ User Training

Post Event

- ✓ Configuration Restoration
- ✓ Forensics
- ✓ Infrastructure Changes

HEAT Software Endpoint Security CESG CPA version

Communications Electronics Security Group – Commercial Product Assurance

CESG

HEAT software

Thank You

www.heatsoftware.com
@HEAT_Software