CUBESYS

CUBESYS DISCUSSION SERIES

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

Today's Discussion Format

The discussion is being recorded.

Please use the chat window to ask your questions.

We have our experts on hand to answer your questions.

The video and content will be sent via email post event.

Panel of Speakers

Kenny Singh
Director Cyber Security & Privacy
Microsoft

Alex Raso
Sales Engineer
SkyKick

Chris Hailes
Senior Cloud Consultant
cubesys

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

Essential Eight

Relative Security Effectiveness Rating	Mitigation Strategy	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Mitigation Strategies to Prevent Malware Delivery and Execution				
Essential	Application Whitelisting	Medium	High	Medium
Essential	Patch Applications	Low	High	High
Essential	Configure Microsoft Office macro settings	Medium	Medium	Medium
Essential	User Application Hardening	Medium	Medium	Medium
Mitigation Strategies to Limit the Extent of Cyber Security Incidents				
Essential	Restrict Administrative Privileges	Medium	High	Medium
Essential	Patch Operating Systems	Low	Medium	Medium
Essential	Multi-factor Authentication	High	High	Medium
Mitigation Strategies to Recover Data and System Availability				
Essential	Daily Backups	Low	High	High

The Essential Eight Maturity Model

Maturity Level	Description
Maturity Level 1	Partly aligned with the intent of the mitigation strategy
Maturity Level 2	Mostly aligned with the intent of the mitigation strategy
Maturity Level 3	Fully aligned with the intent of the mitigation strategy

"Once organisations have implemented their desired mitigation strategies to an initial level, they should focus on increasing the maturity of their implementation such that they eventually reach full alignment with the intent of each mitigation strategy."

Reference - https://www.cyber.gov.au/publications/essential-eight-explained (April 2019)

NIST Alignment

	Microsoft 365	Advanced Threat Protection (Huntress & ThreatLocker)	Cloud Backup (SkyKick)	Password Management	Cyber Awareness Training	Microsoft Defender
Identify	✓	✓				
Protect	✓	✓	✓	✓	✓	✓
Detect		✓				✓
Respond		✓				✓
Recover			✓			

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

The Eight Controls

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

Application Whitelisting

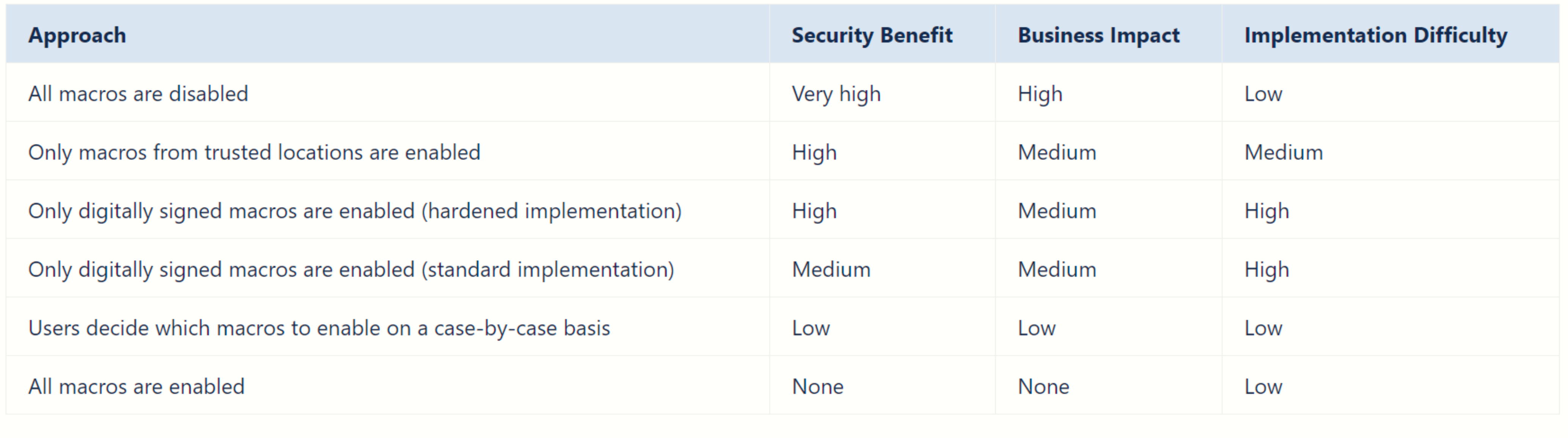
What application whitelisting is	What application whitelisting is not
Application whitelisting is a security approach designed to protect against malicious code (also known as malware) executing on systems. When implemented properly it ensures that only approved applications (e.g. executables, software libraries, scripts and installers) can be executed. While application whitelisting is **primarily designed to prevent the execution and spread of malicious code**, it can also prevent the installation or use of unapproved applications.	**The following approaches are not considered to be application whitelisting**: • providing a portal or other means of installation for approved applications • using web or email content filters to prevent users from downloading applications from the internet • checking the reputation of an application using a cloud-based service before it is executed • using a next-generation firewall to identify whether network traffic is generated by an approved application.

Patch Applications

Relative Security Effectiveness Rating	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Essential	Low	High	High

UNLOCKING COMPLIANCE WITH ESSENTIAL EIGHT

Configure Microsoft Office Macro Settings



Approach	Security Benefit	Business Impact	Implementation Difficulty
All macros are disabled	Very high	High	Low
Only macros from trusted locations are enabled	High	Medium	Medium
Only digitally signed macros are enabled (hardened implementation)	High	Medium	High
Only digitally signed macros are enabled (standard implementation)	Medium	Medium	High
Users decide which macros to enable on a case-by-case basis	Low	Low	Low
All macros are enabled	None	None	Low

UNLOCKING COMPLIANCE WITH ESSENTIAL EIGHT

User Application Hardening

Relative Security Effectiveness Rating	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Essential	Medium	Medium	Medium

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

Restrict Administrative Privileges

Relative Security Effectiveness Rating	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Essential	Medium	High	Medium

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

Patch Operating System

Relative Security Effectiveness Rating	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Essential	Low	Medium	Medium

UNLOCKING COMPLIANCE WITH ESSENTIAL EIGHT

Multi-Factor Authentication

Relative Security Effectiveness Rating	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Essential	Medium	High	Medium

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

Daily Backups

Relative Security Effectiveness Rating	Potential User Resistance	Upfront Cost (staff, software and hardware)	Ongoing Maintenance Cost
Essential	Low	High	High

UNLOCKING COMPLIANCE WITH ESSENTIAL EIGHT

Q & A

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT

cubesys Partners

CLOUDCLARITY

GOT MORE QUESTIONS?

Chris Hailes
chris.hailes@cubesys.com.au
in chailes

CUBESYS

CUBESYS DISCUSSION SERIES

Thank you

UNLOCKING COMPLIANCE EXCELLENCE WITH ESSENTIAL EIGHT