Trend Micro Best Practice Guide ENDPOINT SOLUTION

WORRY-FREE SERVICES



SCAN SETTINGS

- Enable Real Time Scan
- Enable IntelliTrap
- Enable Quarantine Malware variants detected in memory
- Enable Scan compressed files =



BEHAVIOR MONITORING

- Enable Malware Behavior Blocking
- Enable 4 Ransomware Protection feature
- Enable Anti-Exploit Protection
- Enable Event Monitoring

PREDICTIVE MACHINE LEARNING

- Enable Predictive Machine Learning
- Detection Settings
- File = Quar Process =

WEB THREAT PROTECTION



- Enable Web Reputation
- Security Level = Mediur
- Enable Untested URLs
- Enable Browser Exploit Prevention
- Enable URL Filtering Security Level = Mediun



THREAT INTELLIGENCE

- Enable Endpoint Sensor
- Enable Sample Submission



DATA PROTECTION

- Enable **Device Control**
- Enable "Block the AutoRun Function"



OTHER SCAN SETTINGS

- Enable Scheduled scan
- Frequency = \
- File to scan = A
- Scan compressed files = Max Enable IntelliTrap
- Enable Scan boot area



PRIVILEGES AND OTHER SETTINGS

- Other Settings
- Enable Security Agent Self-Protection

GLOBAL SECURITY POLICY

- Security Settings
- Enable HTTPS Web Threat Protection
- Enable Prompt users for newly encountered programs
- Agent Control
- Enable Uninstallation password Enable Exit / Unlock password



TWO FACTOR AUTHENTICATION

- Enable **2FA Authentication**
- DUO Security
- Google Authenticator

Trend Micro Best Practice Guide ENDPOINT SOLUTION

WORRY-FREE ON-PREMISE



SCAN SETTINGS

- Enable Real Time Scan
- Enable IntelliTrap
- Enable Quarantine Malware variants detected in memory
- Enable Scan compressed files =



BEHAVIOR MONITORING

- Enable Malware Behavior Blocking
- Enable Prompt users for newly encountered programs
- Enable 4 Ransomware Protection feature
- Enable Anti-Exploit Protection

PREDICTIVE MACHINE LEARNING

- Enable Predictive Machine Learning
- Detection Settings
- File = 0
- Process =

WEB THREAT PROTECTION

- Enable Web Reputation
 - Security Level = Mo Enable Browser Exploit Prevention
 - Enable URL Filtering

Security Level = M



UPDATES/PATCHES

 Install latest Security Server Patches Enable Auto-product update downloads Action = D



DATA PROTECTION

- Enable **Device Control**
- Enable "USB Autorun Prevention"



OTHER SCAN SETTINGS

- Enable **Scheduled scan**
- Frequency =
- File to scan = A
- Scan compressed files = Max 4 layer
- Enable IntelliTrap
- Enable Scan boot area



AGENT PRIVILEGES

- Other Settings
 - Enable Security Agent Self-Protection

GLOBAL SECURITY POLICY

- - Desktop/Server Enable HTTPS Web Threat Protection
 - Enable Uninstallation password
 - Enable Exit / Unlock password

Trend Micro Best Practice Guide

CLOUD APPLICATION SOLUTION

CLOUD APP SECURITY



GENERAL SETTING

Enable Real Time Scan



ANTI-SPAM PROTECTION

 Apply to: All messages Detection Level = Medium

MALWARE SCANNING

- Rules Apply to: All messages
- Set Scan to all files
- Enable Predictive Machine Learning • Enable **Scan message body**
- Enable IntelliTrap



WEB THREAT PROTECTION

- Enable **Web Reputation**
 - Apply to: **All messages** Security level = Medium
 - Enable Scan message attachment content for suspicious



VIRTUAL ANALYZER

 Enable Virtual Analyzer Apply to: All messages



BUSINESS EMAIL COMPROMISE

Enable Writing style analysis



TWO FACTOR AUTHENTICATION

• Enable **2FA Authentication** DUO Security

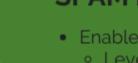
Google Authenticator

Trend Micro Best Practice Guide EMAIL SECURITY SOLUTION

TREND MICRO **EMAIL SECURITY**

VIRUS POLICY

- Enable Malware and malicious code
- Enable With and without mass mailing behavior
- Enable Predictive Machine Learning
- Enable **Virtual Analyzer** (for Advanced license) • Include MACRO, JSE, VBE scam



SPAM PROTECTION

- Level = Moderately High
- Enable **Business Email Compromise**
- Detected as BEC attacks by Antispam Engine Detected as BEC attacks by writing style analysis (writing style BEC threat policy)





• Enable **Web Reputation**

- Security level = Moderately High Detect URLs not tested by Trend Micro
- Enable Virtual Analyzer (for Advanced license) • Enable Time-of-Click Apply to all URLs not tested by Trend Micro
- Enable Social engineering attack



C WWW

IP REPUTATION SETTINGS Dynamic IP Reputation

- Enable the all Standard IP Reputation Setting Known Spam Source (RBL) Dynamically Assigned IP (DUL)

Emerging Threat List (ETL)

DOMAIN-BASED AUTHENTICATION

- Enable SPF checking Enable **DMARC** checking Enable **DKIM SIGNATURE** checking



OTHER POLICY SETTINGS

- Enable Transport Layer Security (TLS) for trusted domains Security level = Mandatory
- Enable Recipient filter
- Enable Password Analysis
- Enable Sender IP match



OUTBOUND MAIL PROTECTION

- Enable Malware or malicious code
- Enable Transport Layer Security (TLS) for trusted domains Security level = Mandatory
- Enable DKIM Signing

Add SPF record



TWO FACTOR AUTHENTICATION

TXT: v=spf1 include:spf.tmes.trendmicro.com

• Enable **2FA Authentication** DUO Security

Google Authenticator

Trend Micro Best Practice Guide EMAIL SECURITY SOLUTION -----

TREND MICRO HOSTED EMAIL SECURITY

VIRUS POLICY

Enable Malware and malicious code

- Enable With and without mass mailing behavior
- Enable Predictive Machine Learning
- Enable Virtual Analyzer Include MACRO, JSE, VBE scam



SPAM PROTECTION

• Enable Spam

Enable Phishing

- Level = Moderately High • Enable Business Email Compromise
- Category:
 - Analyzed Probable (probable BEC threat policy)
- Enable Graymail Include: Marketing, Social Network and Forum
 - Enable Web Reputation Security level = Moderately High
 - Detect URLs not tested by Trend Micro Enable Time-of-Click
- Apply to all URLs not tested by Trend Micro Enable Social engineering attack
 Enable Virtual Analyzer



Set level = 2

- Enable the all Standard IP Reputation Setting Known Spam Source (RBL)
- Dynamically Assigned IP (DUL) Emerging Threat List (ETL)

Enable SPF checking

Enable **DKIM SIGNATURE** checking

DOMAIN-BASED AUTHENTICATION

- OTHER POLICY SETTINGS
 - Security level = N

• Enable Recipient filter

Virus Policy

Enable DMARC checking



OUTBOUND MAIL PROTECTION

Enable Malware or malicious code

- Enable Transport Layer Security (TLS) for trusted domains

Enable Transport Layer Security (TLS) for trusted domains

 Add SPF record TXT: v=spf1 include:spf.hes.trendmicro.com

Enable **DKIM Signing**

Security level = Mandatory



TWO FACTOR AUTHENTICATION

- Enable 2FA Authentication DUO Security
- Google Authenticator