How BeyondTrust EPM (PMfM) Changes macOS Behavior

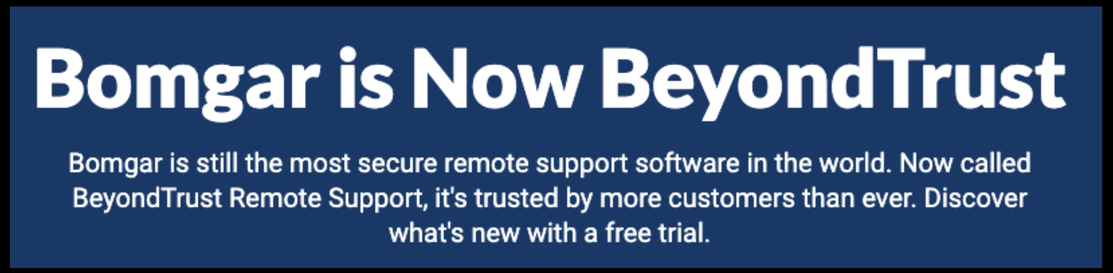
James Reynolds

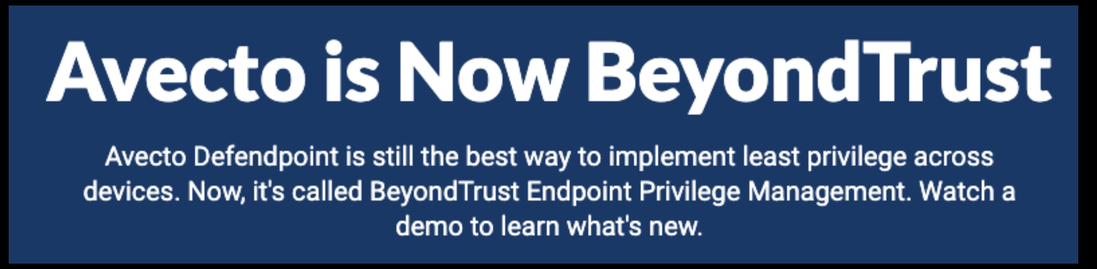
About James Reynolds

- U of U BMus 1999
- 25 years system administration at CFA, Marriott Library, Biology (SBS)
- Security is my “hobby” because I've learned a things for my own reassurance
  - Read a lot of Bruce Schneier and attended a lot of SaintCONs
- I’ve been logging in as a non-admin for probably 15 years
  - I have a good understanding of most macOS auth* mechanisms
  - Read a lot of docs and attended a lot of WWDCs

Lots of Names

- PMfM - Privilege Management for Mac, the preferred name
- EPM-M - Endpoint Privilege Management-Mac
- PMM - Privilege Management Mac
- The reason: (https://www.beyondtrust.com/brand/avecto)





About This Presentation

- This is not about how to use PMfM
  - This is about how PMfM changes the default macOS behavior
  - I am not a PMfM expert!!!
- Why am I doing this presentation?
  - I know macOS security too well and freaked out at what happened
  - I’m too untrusting and I dislike my user experience changing
- I tried to target it for macOS newbies (and related it to Linux where I could)

Agenda

- Should We Be Doing This?
- macOS Security Basics
- The Default Behavior
- Userland macOS Security Components
- PMfM Changes

Should We Be Doing This?

- macOS comes with built-in security system
  - Modularity allows extending and swapping of elements
    - Can add biometrics, MFA, or 3rd party authenticator
    - 3rd party authorization mechanisms
    - It is possible to gut the entire macOS security setup and replace it

Why Change Things?

- Historically, “Security” meant not trusting the OS vendor
- Centralization
  - Improving the worst security by decreasing the best security
- Auditing and compliance
- Principle of least privilege
  - Give users only those privileges which are required to perform their duties

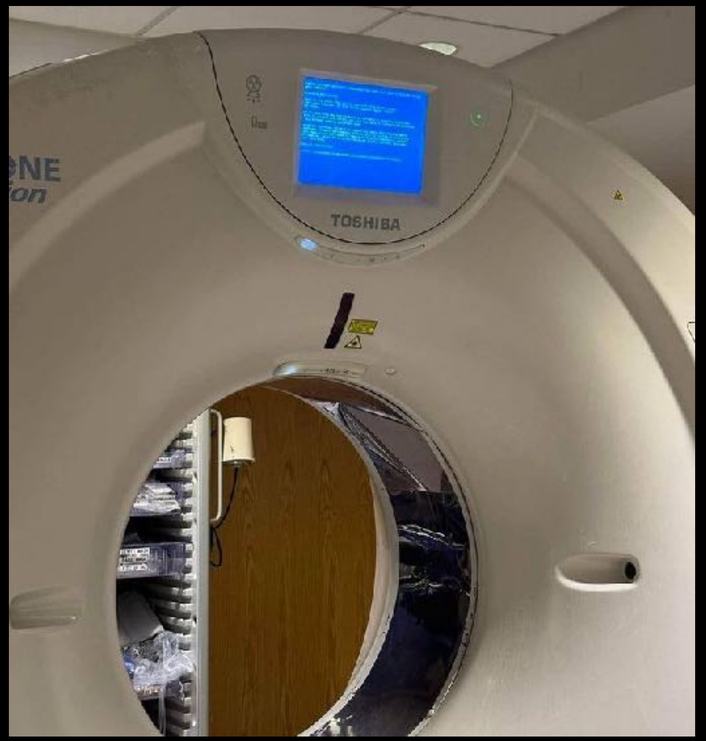
What Could Possibly Go Wrong?

- Crowdstrike’s crash is “the largest IT failure in history”


North Checkpoint
Main Checkpoint
1


Jetstar
Jetstar
Jetstar


DELTA
INFORMATION
TECHNOLOGY


TOSHIBA


:(
Your PC ran into a problem and needs to restart.
Just collecting some error info, and then we'll restart
you.
20% complete


Card Only
Card Only
Card Only
Card Only
Card Only
Card Only


Driver Frame
to select


A problem has been detected and Windows has been shut do
to your computer.
The problem seems to be caused by the following file:
Technical information:
Beginning dump of physical memory
ZENITH

What Could Possibly Go Wrong?

- The dust hasn't settled yet
  - Did Microsoft and Crowdstrike both push updates at the same time?
- Estimated cost up to $10B
- 2023 ransomware payments estimated at $1.1B
- Apr 2023 - Apr 2024 Crowdstrike revenue was $3.3B
- Minimal consequences will mean that companies will be careless

“Redundancies are unprofitable. Being slow and careful is unprofitable. Being less embedded in and less essential and having less access to the customers’ networks and machines is unprofitable—at least in the short term, by which these companies are measured. This is true for companies like CrowdStrike. It’s also true for CrowdStrike’s customers, who also didn’t have resilience, redundancy, or backup systems in place for failures such as this because they are also an expense that affects short-term profitability... We have to deliberately break things and keep breaking them. This repeated process of breaking and fixing will make these systems reliable. And then a willingness to embrace inefficiencies will make these systems resilient. But the economic incentives point companies in the other direction, to build their systems as brittle as they can possibly get away with.”

Bruce Schneier
https://www.schneier.com/blog/archives/2024/07/the-crowdstrike-outage-and-market-driven-brittleness.html

Who Do You Trust More?

- Microsoft blames EU as the reason it can’t secure Windows like Apple secures macOS [1]
- This isn't funny because Apple’s ability to lockdown ***the hardware*** actually puts Macs at a greater risk of turning into worse bricks [2]
- Do you trust the OS vendor, the ***hardware*** vendor, or the security tool vendor more?
- Modify this critical behavior with extreme caution!
- Blanket unquestioning trust is a BAD IDEA

1. https://www.msn.com/en-us/money/news/microsoft-blames-european-commission-agreement-as-reason-it-cant-secure-windows-like-apple-secures-macos-after-crowdstrike-outage/ar-BB1qp2TT
2. https://arstechnica.com/gadgets/2021/11/why-macos-updates-might-brick-your-mac-and-what-you-can-do-about-it/, https://tidbits.com/2016/02/29/el-capitan-system-integrity-protection-update-breaks-ethernet/, https://eclecticlight.co/2024/07/22/could-our-macs-be-crowdstruck/

PMfM Is Not “Fire and Forget”

- Threats and Vulns are always being discovered
- Every update and config change creates risk
- Each customer's setup is unique...
- Do you trust yourself to race a Ferrari?

- “With great power comes great responsibility”– Uncle Ben
- There are no solutions, only trade-offs
  - You get the principle of least privilege, but you're responsible

Into the Weeds We Go!

macOS Security Basics

- PMfM is pointless if you don't do the *other things*
- A lot of this came from Apple securing the iPhone from the nation states
- Securing macOS begins before the computer is booted the 1st time
- I'm just going to run through this, please see other sources for details

https://support.apple.com/guide/security
https://support.apple.com/guide/deployment

Supervision

- Enroll the computer in an MDM
- Locks the device to an organization and prevents MDM unenrollment
- Turn on with Apple School Manager
- How to tell if it's on for a device?
  - System Settings->Privacy & Security->Profiles
  - “This Mac is supervised and managed” (and “MDM Profile” can't be removed)

https://support.apple.com/guide/deployment/about-device-supervision-dep1d89f0bff/web

Jamf PreStage Enrollment

- PreStage Enrollment requires Automated Device Enrollment
  https://learn.jamf.com/en-US/bundle/jamf-pro-documentation-10.40.0/page/Computer_PreStage_Enrollments.html
  - Set Recovery Lock Password
  - Enable/disable Activation Lock
    https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web
- Recovery Lock *can* be set after Enrollment
  https://gingerscripting.com/setting-an-apple-silicon-recovery-lock-password-through-the-jamf-api/

Recovery Lock Password

Boot Protection

- recoveryOS can
  - Change Security setting (Full, Reduced, Permissive)
  - Erase the hard drive
  - Run terminal commands (disable SIPS)
  - Use Safari unfiltered

  https://support.apple.com/guide/deployment/startup-security-dep5810e849c/web
- DFU Mode & Apple Configurator can still erase a Mac

Activation Lock

Theft Protection

- You don't want users locking your devices
- https://support.apple.com/guide/deployment/activation-lock-depf4ab94ef1/web

The First User Account

- Is added to the admin group
- Has a SecureToken
  - Used to unencrypt FileVault (FDE or Full Disk Encryption)
  - Used to give other users Secure Tokens
  - This is a setting is saved in a user’s Directory Service record
- Is a “volume owner” (I don’t know where this setting is saved)
- “Bootstrap token” allows an MDM to create SecureTokens and set volume owners

Volume Owner

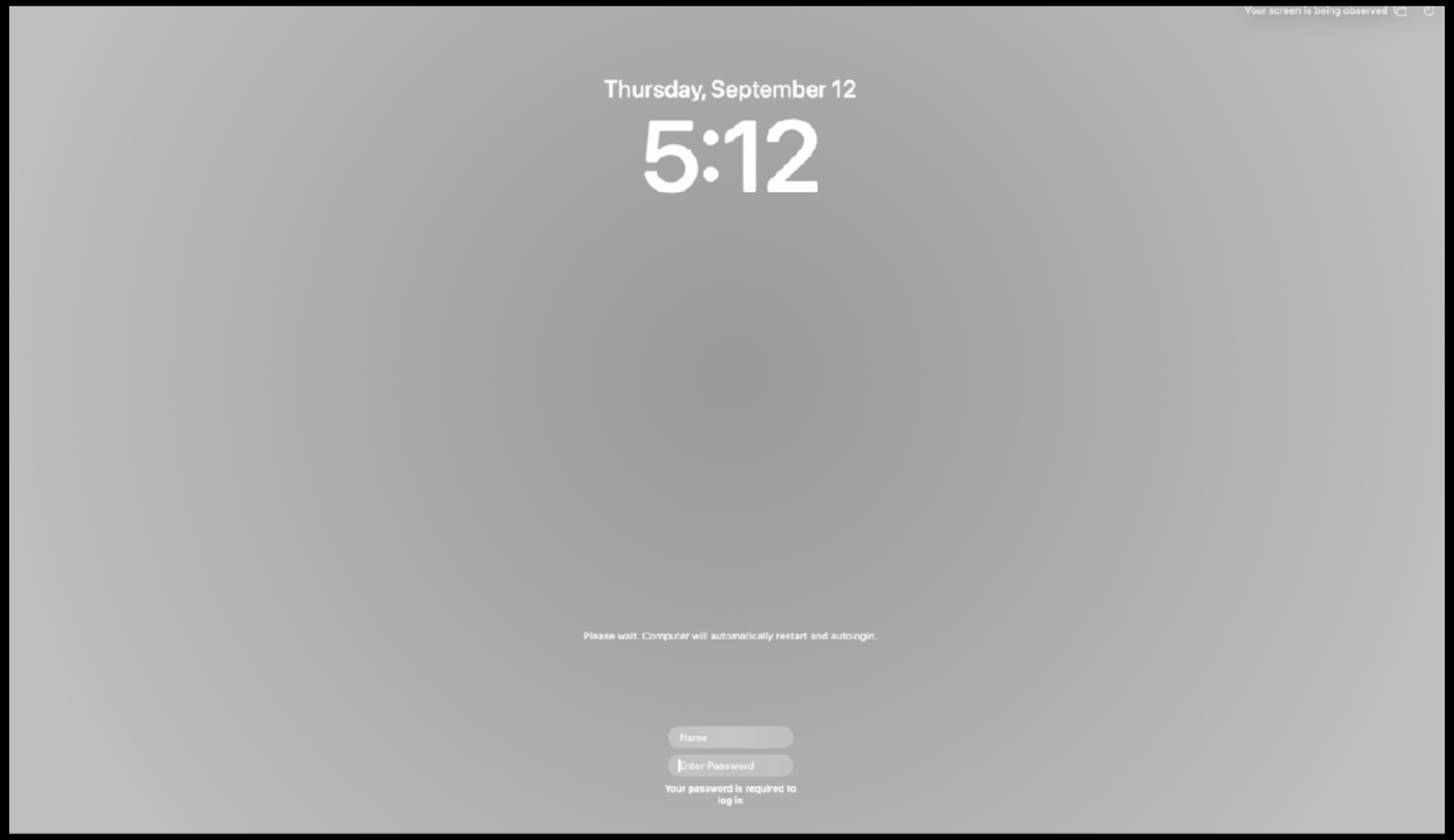
- Volume Owner + Standard user
  - Can update OS
- Volume Owner + Admin user
  - Can change which version of macOS can boot
  - Enable third-party kernel extensions (kexts are deprecated)
  - Can “Erase All Contents and Settings”

https://support.apple.com/guide/deployment/use-secure-and-bootstrap-tokens-dep24dbdcf9e/web

Encrypt the Boot Disk

- Using MDM to encrypt stores the keys in the MDM

The Default Behavior



The Default Behavior

- The different ways to use the default behavior
  - admin (the 1st user)
  - standard with the admin password (“power user”)
  - standard
  - guest

Standard vs Admin User

- /Applications read only
- Can't change most configs unless user has an admin password
  - There are no silent denies, a password prompt is always displayed
- no sudo access, however:
  - `su admin` + `sudo`
  - modify group memberships, or /etc/sudoers

The Standard User + Admin Password

- This is what everyone (including you) should be using but few are
  - ARD requires logging in as admin to set a config
  - A very few apps require the user to login as admin
  - I've been using standard with the admin password for over 15 years

Userland macOS Security Components

- Configuration Profiles
- Directory Service
- Filesystem permissions
- sudo
- Authorization Framework

Configuration Profiles

- This topic is covered in depth elsewhere and not relevant to PMfM
- This is Apple's endorsed way to manage computers using MDM
- I include it here because profiles can enable and disable many OS features including system preferences and it can block applications from running
  - It does not have ways to allow elevating permissions though
  - It should be noted that there are 3rd party apps that do elevation, like https://github.com/robjschroeder/Elevate and https://github.com/SAP/macOS-enterprise-privileges

Directory Services

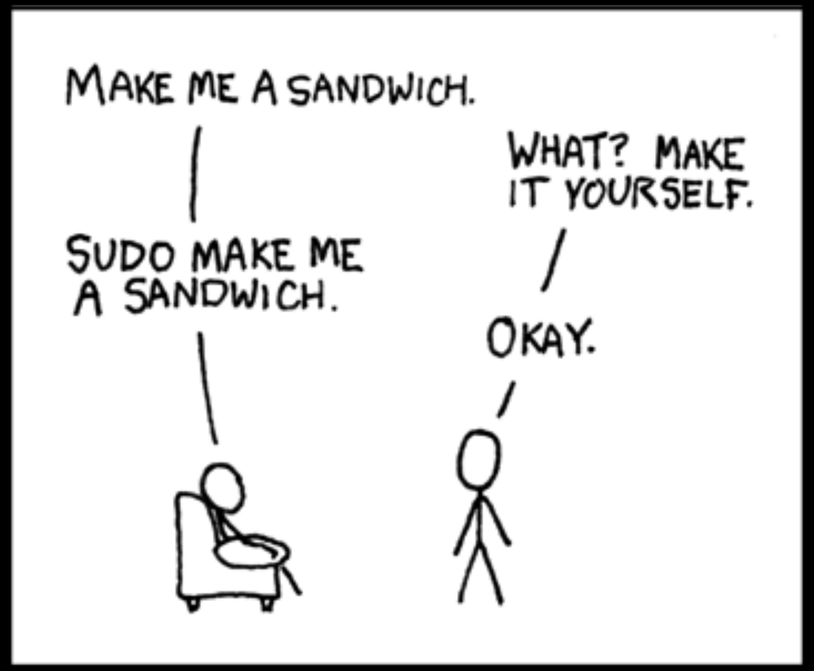
- This topic is covered in depth elsewhere and not relevant to PMfM
- Users, groups, computers, etc.
- Default: /var/db/dslocal
- LDAP, Active Directory (System Settings -> Users and Groups -> Network account server)

Filesystem Permissions

- 3 main areas
  - System: SSV (Signed System Volume) + SIP (System Integrity Protection) + Cryptex (CRYPTographically-sealed EXTension)
    https://support.apple.com/guide/security/signed-system-volume-security-secd698747c9/web
    https://eclecticlight.co/2023/04/05/how-cryptexes-are-changing-macos-ventura/
  - User: POSIX (0755) + NFSv4 ACLs (`ls -le ~`)
  - Apps: TCC + MAS sandboxes
    https://eclecticlight.co/2023/02/11/permissions-sip-and-tcc-whos-controlling-access/
- SIPs is a MAC (mandatory access control) like Selinux
- SIPs: “Operation not permitted” vs POSIX/ACLs: “Permission denied”

SUDO

- This topic is relevant to PMfM
- I'm not going to cover it except for this:



https://xkcd.com/149/

macOS Authorization Database

- AuthDB is the macOS GUI authorization system (it doesn't do authentication)
  - Finder, System Settings, Application elevation requests
  - https://developer.apple.com/documentation/security/authorization_services
- AuthDB is like sudo for the GUI
- It's a whole framework
- The settings are stored in a sqlite db located at /var/db/auth.db
- PMfM modifies the database quite a bit (I'll get to that later)

/System/Library/Security/authorization.plist

Default Rights

- "" (default, catch all), rule: default
- "com.apple.", rule: default
- "com.apple.DiskManagement.", is-root, is-admin, on-console, default
- "com.apple.DiskManagement.internal.", is-root, is-admin, default
- "com.apple.DiskManagement.reserveKEK" (Key Encryption Key), root/admin
- "com.apple.KerberosAgent", mechanisms: KerberosAgent:kerberos-dialog...

/System/Library/Security/authorization.plist

Default Rules

- Classes
  - allow
    - Just do it
  - rule
    - Combination of rules
  - user
  - evaluate-mechanisms

/System/Library/Security/authorization.plist

Default User Rules

- Checks if user is in a group
  - _appstore, _developer, _lpadmin*, _lpoperator, _mbsetupuser-nonshared, _webdeveloper, admin, appserveradm, appserverusr, staff
  - Key: admins only, admins and non-admins, *I add non-admins to _lpadmin
- Options
  - allow-root, authenticate-user, entitled, entitled-group, extract-password (FDE, Continuity), password-only, require-apple-signed, session-owner, shared, timeout, vpn-entitled-group

/System/Library/Security/authorization.plist

Default Evaluate-mechanism Rules

- /Library/Security/SecurityAgentPlugins
  - https://developer.apple.com/documentation/security/authorization_plug-ins/extending_authorization_services_with_plug-ins
- /System/Library/CoreServices/SecurityAgentPlugins
  - CryptoTokenKit, DiskUnlock, FamilyControls, HomeDirMechanism, KerberosAgent, LocalAuthentication, loginKC, loginwindow, MCXMechanism, PKINITMechanism, PSSOAuthPlugin, RestartAuthorization

PMfM Changes

macOS vs PMfM

- macOS model
  - admin, standard, guest users
- PMfM model
  - Everyone is a macOS standard user
  - Give those users “Workstyles:” High, medium, and low flexibility
  - High = admin, medium = power user, low = standard
  - And you get to fine tune it to meet your specific needs

How To Learn the PMfM Model?

- Create 3 accounts on a test computer
  - “high”
  - “med”
  - “low”
- Create filters for each workstyle that match those names
- Login and test it all out
- (This might be the most valuable slide of this presentation...)

PMfM Privilege Elevation (“Messages”)

- PMfM has it's own authentication dialogs
  - PMfM can silently deny (kills the process)
  - PMfM can allow but require the user to enter an explanation
  - PMfM can require a one time code
  - And more...

PMfM Changes

- System Extension uses the EndpointSecurity framework
  - Listens for and approves execution events
- Finder Extension
  - Implements install and uninstall actions for downloaded apps
- /etc/sudo.conf added (https://linux.die.net/man/8/sudo_plugin)

```
Plugin avecto_policy /usr/local/libexec/Avecto/Defendpoint/1.0/sudo/sudoers.so
```

- AuthorizationDB changes and Authorization Plugin

Authorization Database Changes

- ~90 out of ~140 rules are changed (or something like that, too many rules)
- “If you don't set something in PMfM then it goes back to the defaults”
- Except fine grained default authdb rules have been ***replaced*** w/ PMfM
- These authdb changes are global and so they apply for admin users as well
  - Meaning installing PMfM changes the default setup, even w/o a profile

Items w/ session-owner replaced

- com.apple.configurationprofiles.userenrollment.install
- com.apple.icloud.passwordreset
- com.apple.Safari....
- system.identity.write.self
- system.platformsso.auth

PMfM's Changes

- How to view the changes
  - `sqlite3 /private/var/db/auth.db .dump`
  - `/usr/bin/security authorizationdb read *name*`
- `sudo /usr/local/bin/pmfm authorization enable` or `disable` to toggle
  - ~90 out of ~140 rules are changed to be either
    - com.avecto.defendpointd.standard
    - dppolicyplugin:magicmechanism.

Login is not modified by PMfM

Login is managed by the `system.login.console` rule

```
builtin:prelogin
builtin:policy-banner
loginwindow:login
builtin:login-begin
builtin:reset-password,privileged
loginwindow:FDESupport,privileged
builtin:forward-login,privileged
builtin:auto-login,privileged
builtin:authenticate,privileged
PKINITMechanism:auth,privileged
builtin:login-success
loginwindow:success
HomeDirMechanism:login,privileged
HomeDirMechanism:status
MCXMechanism:login
CryptoTokenKit:login
PSSOAuthPlugin:login-auth
loginwindow:done
```

Some of the Changed Rights and Rules

- com.apple.
- com.apple.app-sandbox.
- com.apple.applepay.reset
- com.apple.appserver.privilege.
- com.apple.configurationprofiles.
- com.apple.container-repair
- com.apple.DiskManagement.internal.
- com.apple.library-repair
- com.apple.pf.rule
- com.apple.security.sudo
- com.apple.SoftwareUpdate.
- com.apple.system-extensions.admin
- com.apple.system-migration.
- com.apple.tcc.util.admin
- com.apple.trust-settings.admin
- com.apple.uninstalld.uninstall
- config.
- sys.openfile.
- system.csfde.requestpassword.weak
- system.global-login-items.
- system.install.
- system.keychain.modify
- system.login.tty
- system.preferences
- system.print.
- system.privilege.admin
- system.services.network extension.
- system.sharepoints.
- system.volume.

`security authorizationdb read system.preferences.accounts`

Before

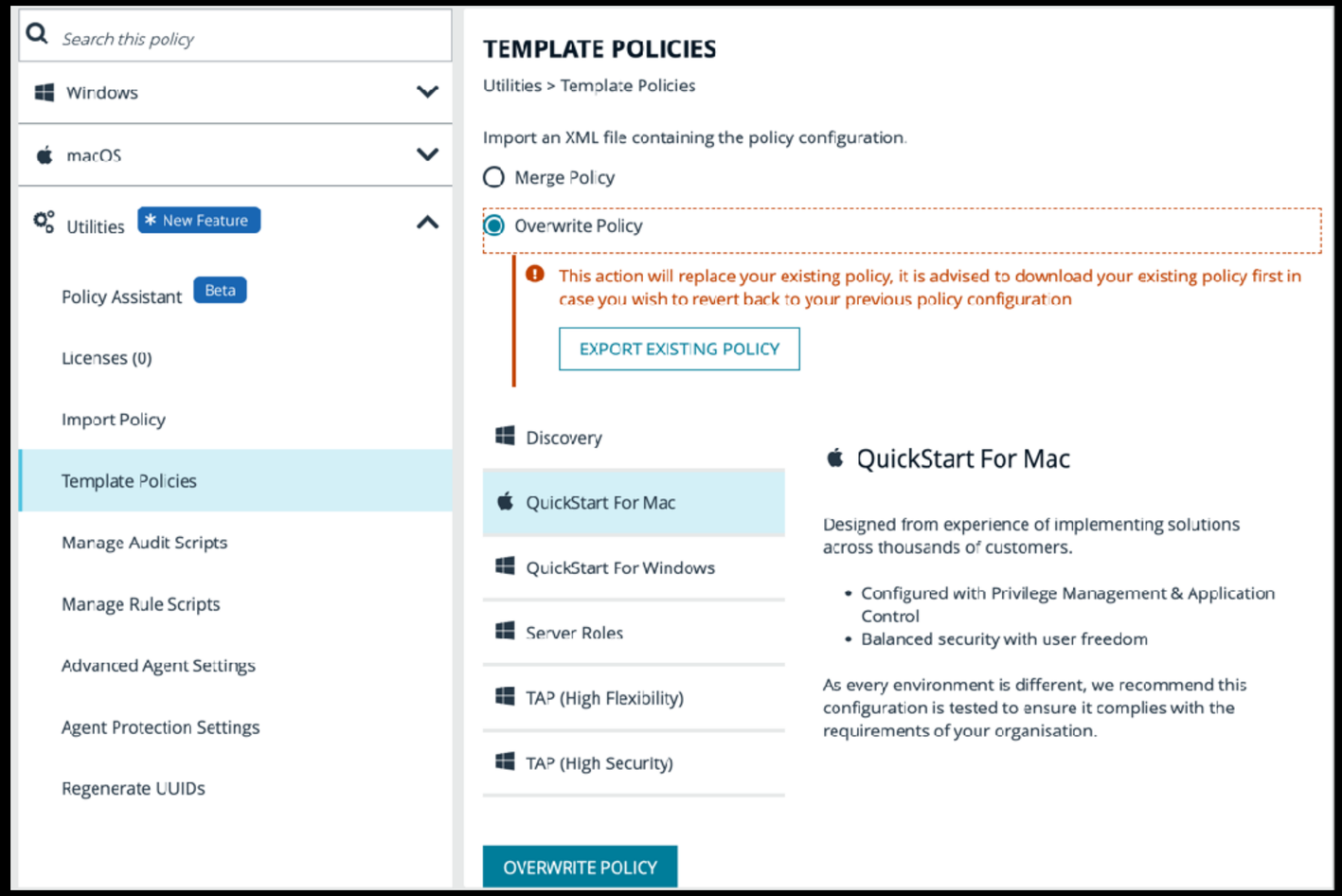
```
<key>allow-root</key>
<true/>
<key>authenticate-user</key>
<true/>
<key>class</key>
<string>user</string>
<key>group</key>
<string>admin</string>
<key>session-owner</key>
<false/>
<key>shared</key>
<false/>
<key>timeout</key>
<integer>2147483647</integer>
<key>tries</key>
<integer>10000</integer>
```

After

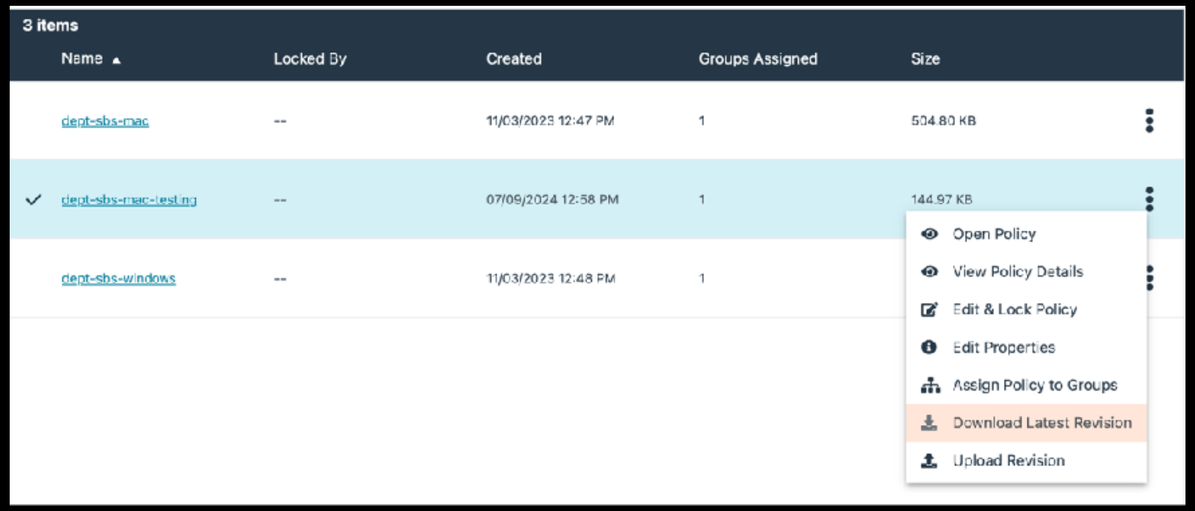
```
<key>class</key>
<string>rule</string>
<key>default-prompt</key>
<dict>
  <key>PMFM</key>
  <string>interactionAllowed</string>
</dict>
<key>k-of-n</key>
<integer>1</integer>
<key>rule</key>
<array>
  <string>is-root</string>
  <string>com.avecto.defendpointd.standard</string>
</array>
```

The Default Template Policy

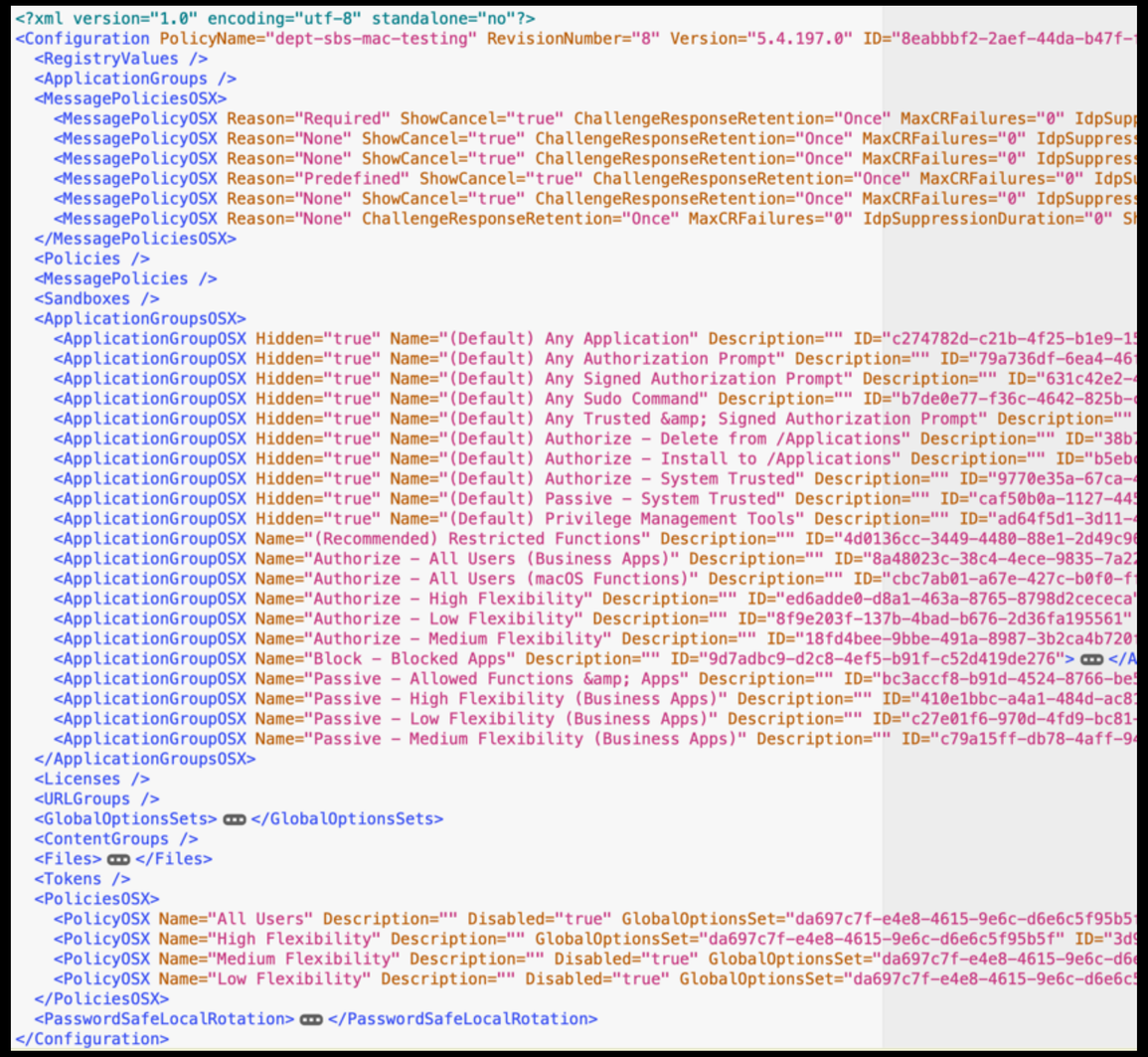
- Created by the company
- The template changes!
- There's no way for you to know which version you have except by checking when you created it (so date your policies)



The Policy Lives In A Single File



- /etc/defendpoint/ic3.xml

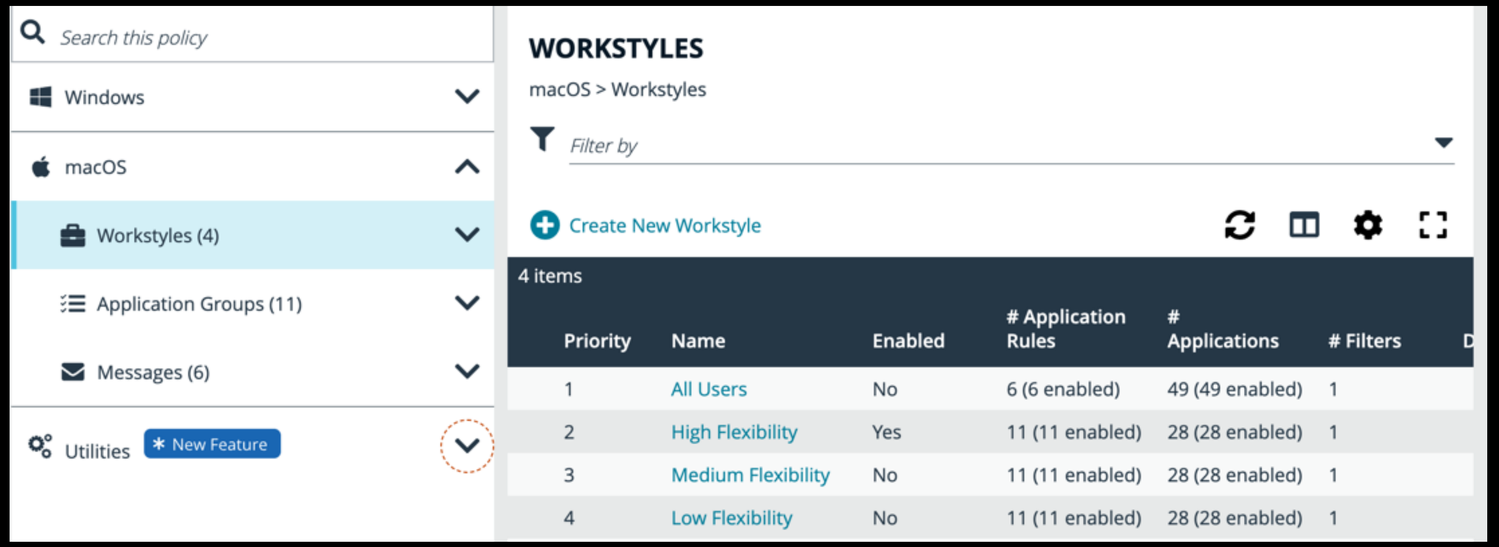


All The Levels

- Computers
  - Computer Groups
    - Policies
      - Workstyles (activated w/ “Filters”)
        - Application Rules = Application Group + Action + Messages
          - Application Groups
            - Application

The Default Template

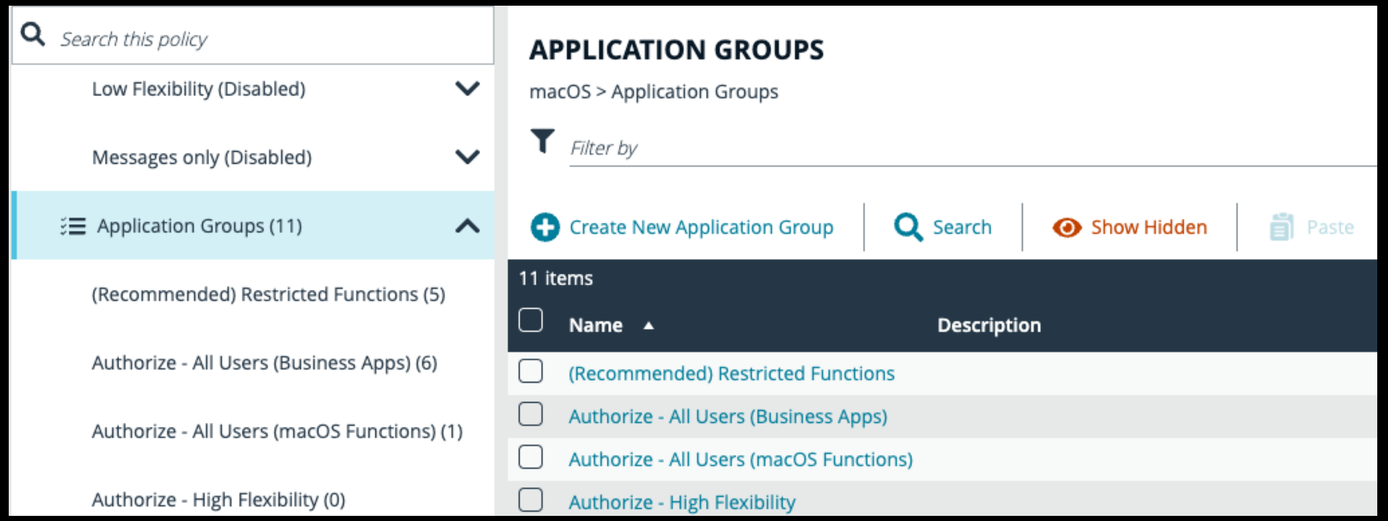
- 4 Workstyles (Really just 3)
- 11 Application Groups
  - 77 Application Rules
- 6 Messages



https://www.beyondtrust.com/docs/privilege-management/mac/admin/policies-and-templates/templates.htm

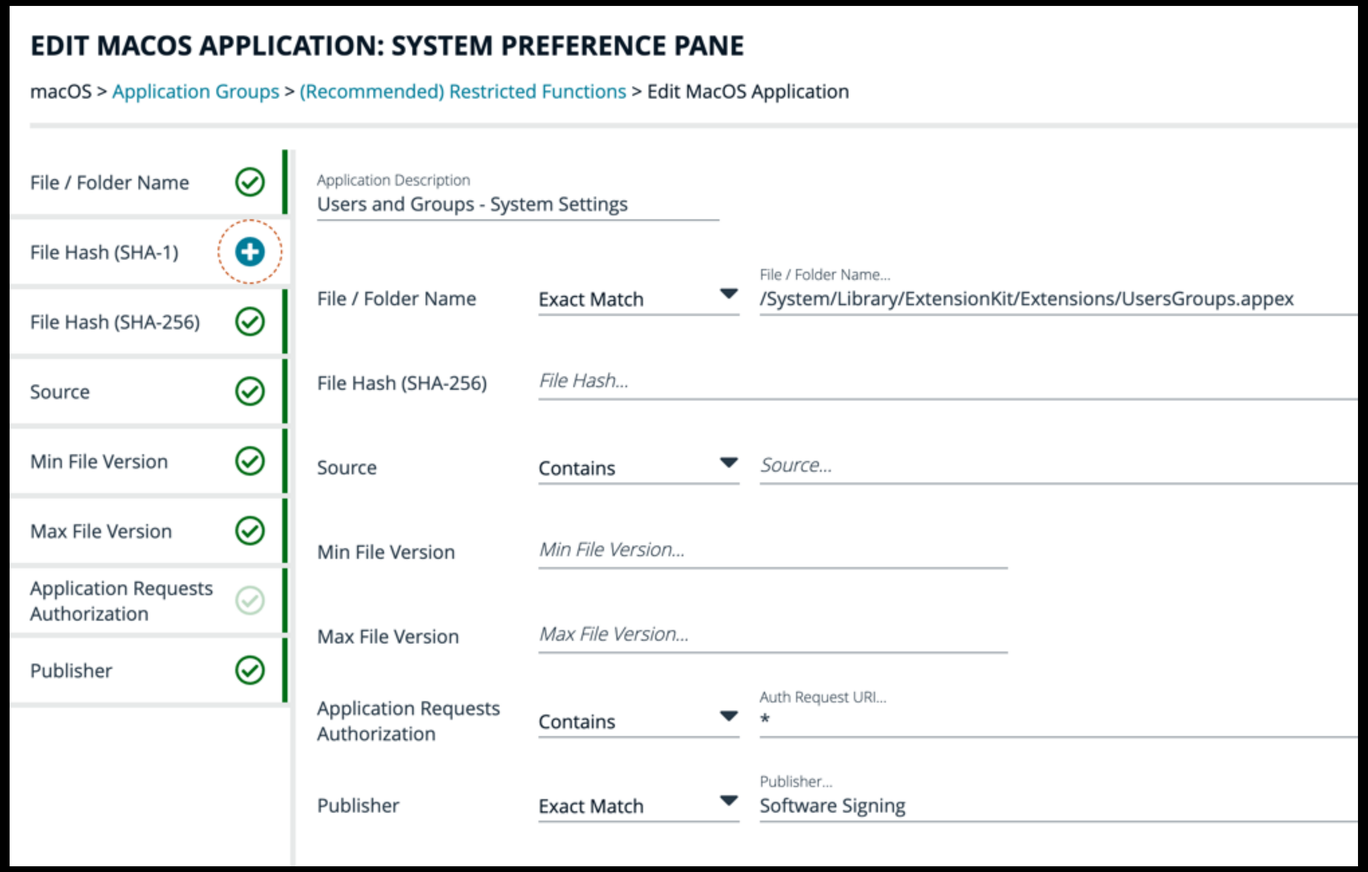
Application Groups

- 44 are hidden, named “(Default)”
- Click “Show Hidden” to view all application groups



Application

- Application can be one of:
  - Binary
  - Bundle
  - Package
  - Script
  - Sudo command
  - System Preference Pane



Application

	Binary	Bundle	Package	Script	Sudo	Pref Pane
File / Folder Name	X	X	X	X	X	X
File Hash (SHA-1)	X	X	X	X	X	X
File Hash (SHA-256)	X	X	X	X	X	X
Source		X				X
URI		X				
Min File Version		X				X
Max File Version		X				X
Application Requests Authorization	X	X	X			X
Command Line Arguments	X			X	X	
Publisher	X	X	X		X	X
Parent Process	X	X		X	X	
Install Action match		X				
Delete Action match		X				

How to Learn 77 Application Rules?

- 20 years ago I learned XSLT and then forgot it. So, I asked AI and...
- xsltproc -o output.csv ApplicationGroupOSX.xsl default-mac-template.xml
- I split the data into 2 focus areas:
  - Application groups and rules
  - Application Rules (Application groups, Message, Action)
  - Demo

Problems I've Encountered

- Printing
- Ejecting USB
- Couldn't get policies to update on clients (so frustrating and time wasted...)
- Couldn't get policies to work (I forgot to add the license to the policy)
- 30-60 second Freezes every 60 minutes (crashes)
- Admin account doesn't work unless you restart

Resources

- Tom Ziegmann 2022 Mac Admins presentation: https://stream.lib.utah.edu/index.php?c=details&id=13526
- Join the #beyondtrust-priv-man Slack https://www.macadmins.org/