International Journal of Core Engineering & Management
Volume-6, Issue-3, June-2019, ISSN No: 2348-9510

CONTROL MINDER OVER DIFFERENT VERSIONS, DIFFERENCES, ENHANCEMENTS, DETAILING THE ARCHITECTURE

Seema Kalwani,
seemakalwani@gmail.com,
Independent contributor,
IL, USA

Abstract

The article is on Control Minder, scanning through different versions, features, components, architecture and integrations. Looking at different attacks in the security world and the features provided by the tool that come to aid for protection from those attacks.

Keywords: Control Minder, Privileged access management, Password vault, Enterprise Log Manager, User activity Report Manager

I. INTRODUCTION

This article will explore different security attacks and the features control minder has to prevent across those attacks. It will cover the architecture, components of version 12.8 and describe the differences in version 14.0. The benefits derived in viewing audit when in integration with Enterprise Log Manager (ELM) will be briefly touched.

II. ARCHITECTURE AND KEY COMPONENTS (12.8)

A. Components

CA Control Minder is a comprehensive solution that addresses multiple aspects of managing identity. One of the keys to successfully implementing CA Control Minder is to understand its architecture and need for various components. CA Control Minder has 4 key components:

1. Enterprise management server
2. Endpoints
3. Report Portal
4. Central database.

B. Integrations

integrations allowed:

1. User activity Reporting
2. Active Directory

International Journal of Core Engineering & Management
Volume-6, Issue-3, June-2019, ISSN No: 2348-9510

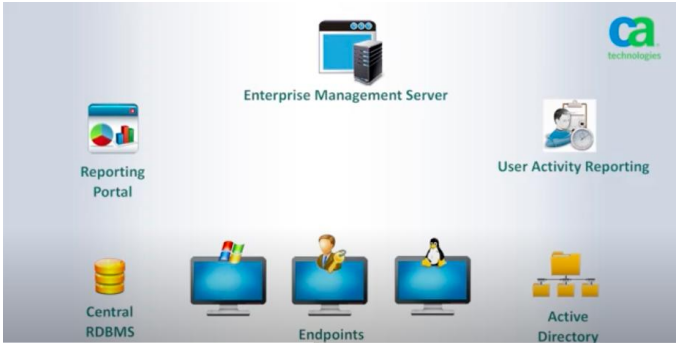

Fig. 1. Used from Steve McCullar, YouTube channel presentation

C. Enterprise Management Server (ENTM)

Enterprise Management Server (ENTM) is the core component of CA Control Minder. Its functionality is

1. Deploy policies to endpoints
2. Manage Privileged accounts
3. Control Unix Host authentication.

ENTM performs all these functions using 3 components – Web based applications, Endpoint management, Password manager.

1. Web based applications – Enables to manage all CA control Minder policies across the enterprise
2. Endpoint management enabled to administer and configure individual CA Control Minder endpoints.
3. Password manager enables to locally store CA Control Minder user passwords when not linking to the Active Directory.

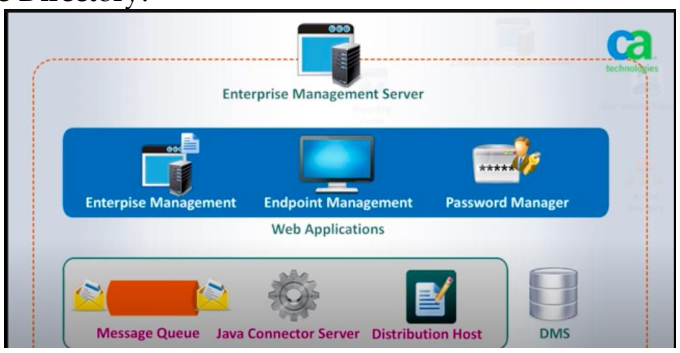

Fig. 2. CA Privileged Identity Manager (formerly CA Control Minder) 12.8 Identify Architectural Layer Features. Used from Steve McCullar, YouTube channel presentation

D. Deployment Map Server (DMS)

This component is the clearing house for all policy activity. It houses policies, rule sets and deployment orders that are distributed to manage endpoints.

E. Distribution Server (DS)

DS acts as primary communication hub between management components and secured endpoints.

The distribution server is a key component of the ENTM. It consists of 3 components

1. Message queue (MQ) Message queue's function is to collect and forward message letter for policy status, report and auditing.
2. Java connector server (JCS) JCS communicates with Java supported devices for SAM (Shared Account Management) actions such as password reset and account exploration.
3. Distribution Host (DH). DH is responsible for distribution of policies to endpoints and receiving their status updates. It is recommended to use multiple relatively light weight distribution servers across the enterprise. This will maximize availability and performance while minimizing chatter over wide area lengths

F. Central Database

Central database stores SAM endpoints and accounts, endpoint reporting data, session data for the wen UI and potentially user data

G. Report portal

CA business intelligence is a robust reporting engine that enables to generate reports based on various factors such as Policy actions, endpoint status, user information, security entitlements, privileged accounts and authentication.

H. Endpoints

CA Control Minder protects access to host resources like file systems, registry keys, process and applications, network resources, authentication services and shared account passwords. These resources are protected by the policy for 2 types of endpoints

1. Windows
2. Unix

I. Active Directory

CA Control Minder connects to the active directory and uses the groups and users that are defined in the active directory. Enables user of a single data store for all the users.

J. CA User Activity reporting (Later called ELM – Enterprise Log Manager)

UARM collects events from the audit queue, from the distribution server and sends the audit events to the UARM server for processing, storage analysis and reporting. To report on auditing data CA UARM needs to be integrated with CA Control Minder

III. COMPREHENSIVE SOLUTION

This section covers the attacks prevalent in the enterprise space and describes the core of CA Control Minder – Fine grained access control functionality that addresses the attacks. Below diagram shows the features of CA Control Minder.

International Journal of Core Engineering & Management
Volume-6, Issue-3, June-2019, ISSN No: 2348-9510

Fig. 3. Different functionalities of CA Control Minder

A. Unique host based fine grained controls

Unique host based fine grained controls provides effective defense against cyber-attacks.

1. 1.Protection from externally and internally focused threats
2. Complements a defense-in-depth strategy
3. 3.Pro-active and comprehensive

B. Prevalent Attacks

A new breed of cyber threats has been attacking enterprises. These attacks are referred to as Advanced Persistent Threat (APT). Most often the attacker is motivated by financial gain or by gaining access to intellectual property or by political motives among other goals. Unlike malware that has no specific target APT have targeted specific enterprises because of who they are and what they have.

An advanced persistent threat (APT) is a covert cyber-attack on a computer network where the attacker gains and maintains unauthorized access to the targeted network and remains undetected for a significant period.

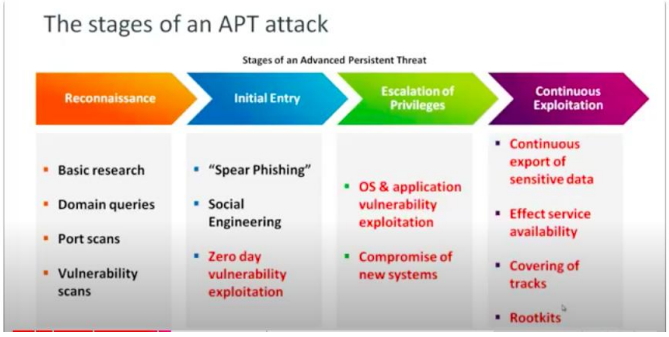

Fig. 4. APT attack layering

- Reconnaissance – Consists of sizing up the victim
- Initial Entry - the attackers perform an initial penetration to the enterprise by tricking in the insider through fishing or other social engineering. The attacker may also exploit a zero-day vulnerability which is unpatched and probably undocumented that requires specialized expertise to exploit. Because the vulnerabilities might be unknown it might be difficult for the victim to defend themselves.

International Journal of Core Engineering & Management
Volume-6, Issue-3, June-2019, ISSN No: 2348-9510

- Escalate privileges - Having gained the initial entry in the system the attacker will ultimately escalate privileges on the targeted server and use those escalated privileges to compromise new systems.
- Continuous exploitation - Escalated privileges can be used to open back door for themselves and move on to a more continuous exploitation of the victims environment.
- Challenge – Victim's challenge is to detect and prevent the attacker from succeeding.

C. Capabilities of CA Control Minder

CA Control Minder is a mature host-based software solution that can help the servers from being compromised and from server resources from being accessed if the event breach does occur.

Fig. 5 Capabilities of CA Control Minder

- Trusted program execution – CA Control Minder monitors critical programs to determine whether the program has been tampered with by checking the integrity of the program by checking a variety of measure. If CA Control Minder determines that the program has been tampered with it will not only generate alerts but optionally block the execution of the suspect program until the investigation has been made. In this way the use of trusted computing base is ensured and is protected by the potential damage that could occur by executing a program that might contain malware.
- File and directory controls – CA Control Minder implements granular fine grained access control for files and directories. Even the Unix/Linus root user and the windows administrator accounts are subject to the controls. Even if the attacker is running with super user privileges, they will not be able to access protected resources in the file system. This is useful for protecting data at rest and also to ensure the integrity of the systems and their configurations. This feature could also protect the accounts being compromised in the first place.
- Windows registry protection - CA Control Minder protects the registry keys and values being accessed by unauthorized users. This is an important feature for defending the windows servers from being compromised by malware. Generally, any type of software that gets deployed on windows must update the registry and that include malware. By protecting the registry, the windows servers are defended from being infected by malicious software. Windows Services and Unix Process Protection
- Lock down of ports and services - CA Control Minder protects UNIX/Linux processes and windows services from being terminated by unauthorized users. Like the other features this protection is applicable even if user is running s UNIX/Linux root or windows administrator. This capability can help ensure the availability of systems and applications. CA Control

International Journal of Core Engineering & Management
Volume-6, Issue-3, June-2019, ISSN No: 2348-9510

Minder can protect the use of incoming and outgoing TCP/IP ports. This feature enable the use of ports and services from specific sources. There by blocking communication from potentially malicious sources. Also helps to protect the potential exfiltration of sensitive data to untrusted systems

- Substitute User Controls User Accountability - CA Control Minder protects against unauthorized use of privileged identities. In case of UNIX/Linux systems it prevents unauthorized users from switching to privileged accounts such as root or oracle even if the password is known. For UNIX/Linux and Windows systems it can require that if the user is logging in with a privileged identity that user is using only prescribed login application for that identity and only from trusted sources such as specific domains or IP addresses. This can ensure that those identities are being used only in an authorized way by authorized users.
- Application Jailing - Powerful capabilities of application jailing can protect the enterprise from being compromised by attackers who are exploiting zero-day vulnerability. If the attacker is trying to exploit a vulnerability in an application or process that is running on the servers that exploit will be blocked. This feature effectively provides a unique virtual patching capability to even prevent vulnerable applications from being exploited to perform unauthorized actions

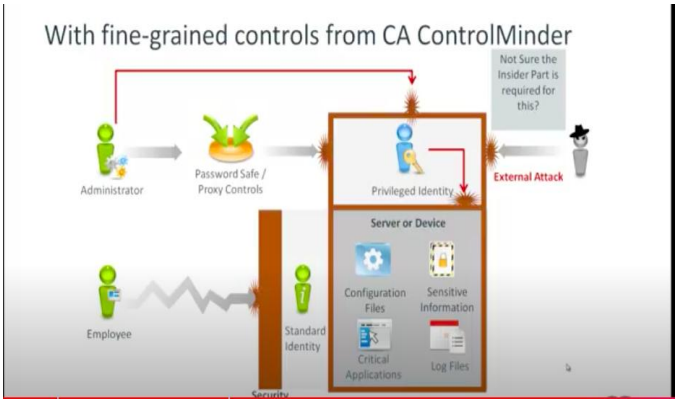

Fig. 6 Protection via fine grained controls

Host based fine grained controls provide a powerful defense from defending the servers from malicious attacker. Whatever the source weather insiders or outsiders CA Control Minder is a modular and comprehensive solution for privileged identity management

IV. ENHANCEMENTS FROM 12.8 TO 14.0

CA Control Minder uses few technologies as the base to provide its functionalities. Version 14.0 is an enhancement to include newer technologies and improve upon some functionality as well. Below is the list of updates:

A. Technology Stack upgrade

The technology stack upgrade was made to include below versions

- JDK 1.8
- RHEL 7.2
- Apache Tomcat 7.0.72
- Active MQ Message Server.

B. New Reporting Engine

CA User activity reporting engine enabled enterprises to collect, normalize, aggregate and report the user activity via a newer mechanism of engine. The new engine facilitates search functionality enables a user to view refined set of results in a dashboard /report based on the search input keyword.

C. Tibco-Apache ActiveMQ Bridge

With the Tibco-to-ActiveMQ bridge, all the legacy endpoints with Tibco as the Message Queue are supported in Privileged Identity Manager release 14.

D. Reduced Password Brute force attack

After a defined number of failed logins this feature automatically disables the user, preventing the password brute force attack from happening.

E. Proxy database login

Initiates and records proxy session to Microsoft SQL Server and Oracle server database which was unavailable in the previous version.

F. Group Checkout

Increases operational efficiency by allowing multiple checkouts of privileged accounts at once

G. Advanced Proxy Login

Allows a user to login to a member server by using an active directory domain account.

H. Grayscale proxy recording

Consumes less disk space as it reduces the size of the proxy session recordings.

V. CONCLUSION

Control Minder is a traditional password management tool with Unix and Windows based security features at the endpoint level. Most effective for small or medium based enterprise to protect the resources and deployment of enterprise level policies with ease.

REFERENCES

1. Broadcom, Privileged Access management, https://community.broadcom.com/communities/communityhome/digestviewer/viewthread?GroupId=1501&MID=781997&CommunityKey=3e91a086-c7b2-4bd0-9f8d-3493ed834111#bmf629e930-67dc-42e6-a14b-564fa7394d14, Published Nov 21 2017
2. Advanced Technology Partners, Privileged Access management, https://www.advancedtech.cz/en/controlminder-en.php, (accessed Jan 2018)
3. Steve McCullar, CA Control Minder, https://www.youtube.com/playlist?list=PLynEdQRJawmyDiqQquADdbBG5RupTy04x, published 2014
4. Nagios support forum, CA Control Minder,

https://support.nagios.com/forum/viewtopic.php?t=43786, published May 9 2017
5. CA Technologies, Product sheet, https://d3alc7xa4w7z55.cloudfront.net/static/upload/201/0019/2012_casecjournal_solutionbrief_caaccesscontrol.pdf, (accessed Jan 2018)