

CIGENT D3E AND CYBERARK ENDPOINT PRIVILEGE MANAGER

PROTECT SENSITIVE FILES IN AN ELEVATED THREAT ENVIRONMENT

HIGHLIGHTS

When your traditional defense lines fail to cope with today's attack surface, CyberArk & Cigent integration is here for the rescue.

With the proactive approach by CyberArk Endpoint privilege manager, detected threats are marked and then diverted to Cigent's Dynamic Data Defense Engine for Windows 10 (D3E) that proactively locks access to sensitive files disk partitions on the endpoints.

Cigent's Dynamic Data Defense Engine for Windows 10 (D3E) ingests threats detected by CyberArk Endpoint Privilege Manager and proactively locks access to sensitive files and disk partitions on the Windows endpoint with a step up authentication until the threat is cleared.

THE CHALLENGE

There is a gaping hole in endpoint data protection. When an endpoint is under duress by malware, ransomware, stolen credentials, or lost / stolen devices, it's nearly impossible protect sensitive personal and corporate files in the event the system is compromised. Full disk encryption protects data at rest but is not effective when the user is logged in.

Cigent and CyberArk recently established a technology partnership to reduce the risk of financial and reputational loss due to advanced cyber threats by helping organizations secure their sensitive files during a suspected cyber attack.

THE SOLUTION

CyberArk Endpoint Privilege Manager helps remove the barriers to enforcing least privilege and allows organizations to block and contain attacks at the endpoint, reducing the risk of information being stolen or encrypted and held for ransom.

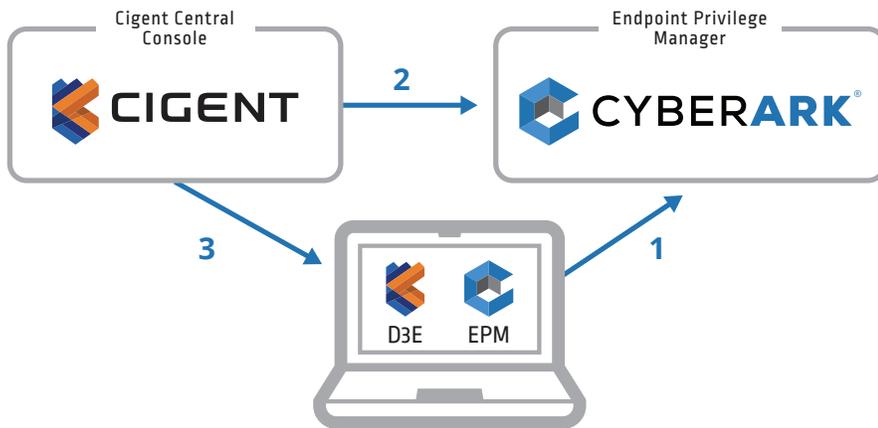
Cigent D3E brings cyber security best practices to the data layer of Windows 10 devices with threat aware 2 factor authentication, deception, artificial intelligence, and integration with leading enterprise security solutions. D3E is designed to prevent the loss of critical data in the event of a suspected cyber attack or breach.

- Protects any files based on file type / folder designation
- Provides multiple options for seamless step up authentication
- Extends multi-factor authentication to encrypted disk partitions
- Supports dynamic file / partition locking based on threat level
- Manage file protections and group file locking by global policy



HOW THE JOINT SOLUTION WORKS

1. The EPM agent detects a threat and creates an alert in the Endpoint Privilege Manager console.
2. The Cigent Console polls Endpoint Manager for threats to managed devices.
3. The Cigent Console engages ActiveLock on the Cigent D3E endpoint to protect files and disk partitions with a step up authentication until the threat is resolved or investigated.



CYBERARK PRODUCTS

- Endpoint Privilege Manager
- Endpoint Manager

PARTNER PRODUCTS

- D3E for Windows 10
- D3E Management Console

VALUE

The integration with CyberArk EPM provides:

- Improved protection of sensitive files on the endpoint
- Automated and rapid response to threats
- Increased protection from ransomware and insider threats

About CyberArk

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk delivers the industry's most complete solution to reduce risk created by privileged credentials and secrets. The company is trusted by the world's leading organizations, including more than 50 percent of the Fortune 500. To learn more, visit www.cyberark.com.

About Cigent

Cigent Technology, Inc. provides network and endpoint security solutions that protect your data from the inside out. Our software and nextgen firmware based endpoint detection and response solutions thwart advanced cyber attacks, preventing exfiltration of critical data, even in the event of a breach. www.cigent.com.

©CyberArk Software Ltd. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners. U.S., 10.20. Doc. 145510

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.