

For Immediate Release

CyberArk Earns U.S. Department of Defense UC APL Certification

*CyberArk is the First Comprehensive Privileged Account Security Solution Provider on the List of Cyber Security Products Approved for Use within Federal Agency Infrastructures*

**Newton, Mass. – March 29, 2016 –** [CyberArk](http://www.cyberark.com/) (NASDAQ: [CYBR](http://investors.cyberark.com/phoenix.zhtml?c=253582&p=irol-irhome)), the company that protects organizations from [cyber attacks](http://www.cyberark.com/solutions/) that have made their way inside the network perimeter, today announced the CyberArk Privileged Account Security Solution has been added to the U.S. Department of Defense (DoD) Unified Capabilities Approved Products List (UC APL). CyberArk has the only comprehensive [privileged account security](http://www.cyberark.com/products/privileged-account-security-solution/) solution on the list.

The [UC APL](http://www.cyberark.com/wp-content/uploads/2016/03/1509301-Cyber-Ark-Software-Inc.-PAS-Solution-Rel.-9.1-UCAPL-Approval-Memo-1.pdf) is administered by the Defense Information Systems Agency (DISA) and includes only those products approved for use with DoD agencies’ technology infrastructure. This designation identifies products that have undergone a rigorous testing process conducted by the DoD that assures acceptable levels of information assurance and interoperability capabilities.

The [CyberArk Privileged Account Security Solution](http://www.cyberark.com/products/privileged-account-security-solution/) helps identify, lock down and secure existing privileged credentials across networks, and utilizes continuous monitoring of privileged credentials to help detect anomalous behavior and stop an attack early in the cycle to reduce damage. CyberArk was previously granted [Common Criteria](http://www.cyberark.com/solutions/federal-government-solutions/) Evaluation Assurance Level EAL 2+ for the CyberArk Privileged Account Security Solution.

As evidenced by the U.S. Office of Personnel Management (OPM) breach, cyber attackers continue to evolve tactics to target, steal and exploit privileged accounts – the keys to successfully gaining access to an organization’s most sensitive and valuable data. The UC APL milestone is important for CyberArk as new federal mandates and directives emerge to strengthen cyber security controls.

For example, while multi-factor authentication methods like the Common Access Card (CAC) are mandated for validating user identities, there are limitations in securing accounts that do not support CAC authentication natively. CyberArk helps organizations meet these mandates by enabling CAC card authentication to all systems and applications managed by a privileged account security solution – even applications that cannot directly support public key infrastructure (PKI) or two-factor authentication.

“Being added to the UC APL is a significant accomplishment that accelerates CyberArk’s ability to deliver innovative cyber security solutions to the federal sector. CyberArk is on an exclusive list of DoD-approved solutions that reinforces CyberArk as a trusted solutions provider for their most critical cyber security initiatives,” said Kevin Corbett, director of U.S. Federal Business at CyberArk. “This achievement will assist DoD security decision making by demonstrating the ability to help close security gaps associated with enforcing multi-factor authentication across all system types.”

[Corsec Security](https://corsec.com/certifications/uc-apl/), a global leader in product hardening through security certifications and validations, was CyberArk’s strategic advisor in the UC APL processes. “By completing STIG and JITC testing, CyberArk surpassed all information assurance and interoperability requirements set forth by the U.S. DoD. Following its Common Criteria certification, the UC APL listing is further evidence of CyberArk’s commitment to product security,” said Darcy Dinga, executive vice president, Corsec.

Further reinforcing the benefits of CyberArk’s innovative cyber security solutions for the federal sector, in addition to achieving Common Criteria certification, the company was recently named a winner in the [2015 GSN Homeland Security Awards](http://www.cyberark.com/press/cyberark-wins-2015-government-security-news-homeland-security-awards/) in two categories: Best Privileged Access Management Solution and Best Continuous Monitoring and Mitigation System.

**About CyberArk**

[CyberArk](http://www.cyberark.com) is the only security company focused on eliminating the most advanced [cyber threats](http://www.cyberark.com/products/); those that use insider privileges to attack the heart of the enterprise. Dedicated to stopping attacks before they stop business, CyberArk proactively secures against cyber threats before attacks can escalate and do irreparable damage. The company is trusted by the world’s leading companies – including more than 40 percent of the Fortune 100 and 17 of the world’s top 20 banks. CyberArk’s dedicated team based in Washington, D.C. works closely with many U.S. federal agencies to help protect their highest value information assets, infrastructure and applications. CyberArk’s U.S. headquarters are located in Newton, Mass. To learn more about CyberArk, visit [www.cyberark.com](http://www.cyberark.com/), read the company blog, <http://www.cyberark.com/blog/>, follow on Twitter [@CyberArk](https://twitter.com/cyberark) or Facebook at <https://www.facebook.com/CyberArk>.

**Forward-Looking Statements**

This release may contain forward-looking statements, which express the current beliefs and expectations of CyberArk’s (the “Company”) management. In some cases, forward-looking statements may be identified by terminology such as “believe,” “may,” “estimate,” “continue,” “anticipate,” “intend,” “should,” “plan,” “expect,” “predict,” “potential” or the negative of these terms or other similar expressions. Such statements involve a number of known and unknown risks and uncertainties that could cause the Company’s future results, performance or achievements to differ significantly from the results, performance or achievements expressed or implied by such forward-looking statements. Important factors that could cause or contribute to such differences include risks relating to: changes in the rapidly evolving cyber threat landscape; failure to effectively manage growth; near-term declines in the Company’s operating and net profit margins and its revenue growth rate; real or perceived shortcomings, defects or vulnerabilities in the Company’s solutions or internal network system, or the failure of the Company’s customers or channel partners to correctly implement the Company’s solutions; fluctuations in quarterly results of operations; the inability to acquire new customers or sell additional products and services to existing customers; competition from IT security vendors; the Company’s ability to successfully integrate recent and or future acquisitions; and other factors discussed under the heading “Risk Factors” in the Company’s most recent annual report on Form 20-F filed with the Securities and Exchange Commission. Forward-looking statements in this release are made pursuant to the safe harbor provisions contained in the Private Securities Litigation Reform Act of 1995. These forward-looking statements are made only as of the date hereof, and the Company undertakes no obligation to update or revise the forward-looking statements, whether as a result of new information, future events or otherwise.

# # #

*Copyright © 2016 CyberArk Software. All Rights Reserved. All other brand names, product names, or trademarks belong to their respective holders.*

**Media Relations Contacts:**

Brian Merrill, fama PR Liz Campbell, CyberArk

Phone: +1-617-986-5005 Phone: +1-617-558-2191

Email: [cyberark@famapr.com](mailto:cyberark@famapr.com) Email: [press@cyberark.com](mailto:press@cyberark.com)

**Investor Relations Contact:**

Erica Smith, CyberArk

Phone: +1 617-630-6426

Email: [ir@cyberark.com](mailto:staci.mortenson@icrinc.com)