CYBERARK® SOLUTIONS AND THE MITRE ATT&CK FRAMEWORK

OVERVIEW

MITRE ATT&CK® is a popular, open framework for implementing cybersecurity detection and response programs. Available free of charge, ATT&CK includes a vast knowledge base of adversarial tactics, techniques and procedures (TTPs) based on real-world observations. Businesses around the world use ATT&CK to improve threat detection and mitigation, strengthen security and reduce exposure.

By mimicking the behavior of real-world attackers, the ATT&CK framework helps IT, information security and compliance organizations effectively assess risks, identify security gaps and eliminate vulnerabilities. The framework provides a common taxonomy that lets security professionals (SOC staff, red and blue teams, pen testers, security vendors, threat intelligence providers, etc.) easily exchange information and collaborate using the same language.

As a means to mitigate risk from major breaches and advanced attacks, organizations can leverage the framework and perform adversary emulations using known techniques, tools and behaviors that are specific to hacking groups or nation states. ATT&CK also includes a Groups database that tracks the activities of dozens of threat actors and cybercriminal syndicates across the globe.

This eBook provides a brief introduction to ATT&CK and explains how CyberArk solutions can be an instrumental part of an ATT&CK cybersecurity program.

You will learn:

- Basic ATT&CK concepts and principles
- How organizations can leverage ATT&CK
- Key ATT&CK tactics for enterprise environments
- How CyberArk solutions align to the ATT&CK framework

A BRIEF INTRODUCTION TO MITRE ATT&CK

The MITRE Corporation is a not-for-profit organization that operates the U.S. National Cybersecurity Federally Funded Research and Development Center (FFRDC) and functions as the editor and primary numbering authority for the nation's Common Vulnerabilities and Exposures (CVE) list. In 2013 MITRE researchers began investigating and documenting the various methods bad actors use to compromise information systems and wage attacks.

Since then, MITRE has identified hundreds of different techniques adversaries use to carry out various exploits. ATT&CK organizes these techniques into a collection of tactics to help security professionals efficiently detect, track and mitigate threats. The tactics describe what the adversary is trying to accomplish (e.g. gain illicit credential access) and the techniques describe the actions the adversary takes to achieve their goals (e.g. brute force methods).

MITRE publishes an evolving series of ATT&CK matrices describing common cybersecurity tactics, techniques, procedures and mitigations for various operating environments including:

- ATT&CK for Enterprise Matrix for Windows, macOS, Linux, cloud, and network systems
- ATT&CK for Mobile Matrix for Apple iOS and Android devices
- ATT&CK for Industrial Control Systems Matrix for Supervisory Control and Data Acquisition (SCADA) systems and other industrial control systems

To learn more about ATT&CK visit the ATT&CK Getting Started webpage.

COMMON ATT&CK USE CASES

- Detections and Analytics
- Threat Intelligence
- Adversary Emulation and Red Teaming
- Assessment and Engineering

MITRE ATT&CK FOR ENTERPRISE – THINKING LIKE AN ATTACKER

ATT&CK breaks down and classifies various actions adversaries take to gain illicit access to systems, steal data and inflict damage. Unlike other security frameworks that focus on the tools and malware used by bad actors, ATT&CK focuses on how adversaries interact with systems during an attack.

ATT&CK for Enterprise details the tactics and techniques adversaries typically use to infiltrate an enterprise network, compromise systems, escalate privileges and move laterally without detection. By thinking like an attacker, ATT&CK can help you improve your company's security posture, contain threats and mitigate risk. Over the years MITRE has expanded the scope of ATT&CK for Enterprise to include IaaS, PaaS and SaaS environments, in addition to traditional on-premises IT implementations.

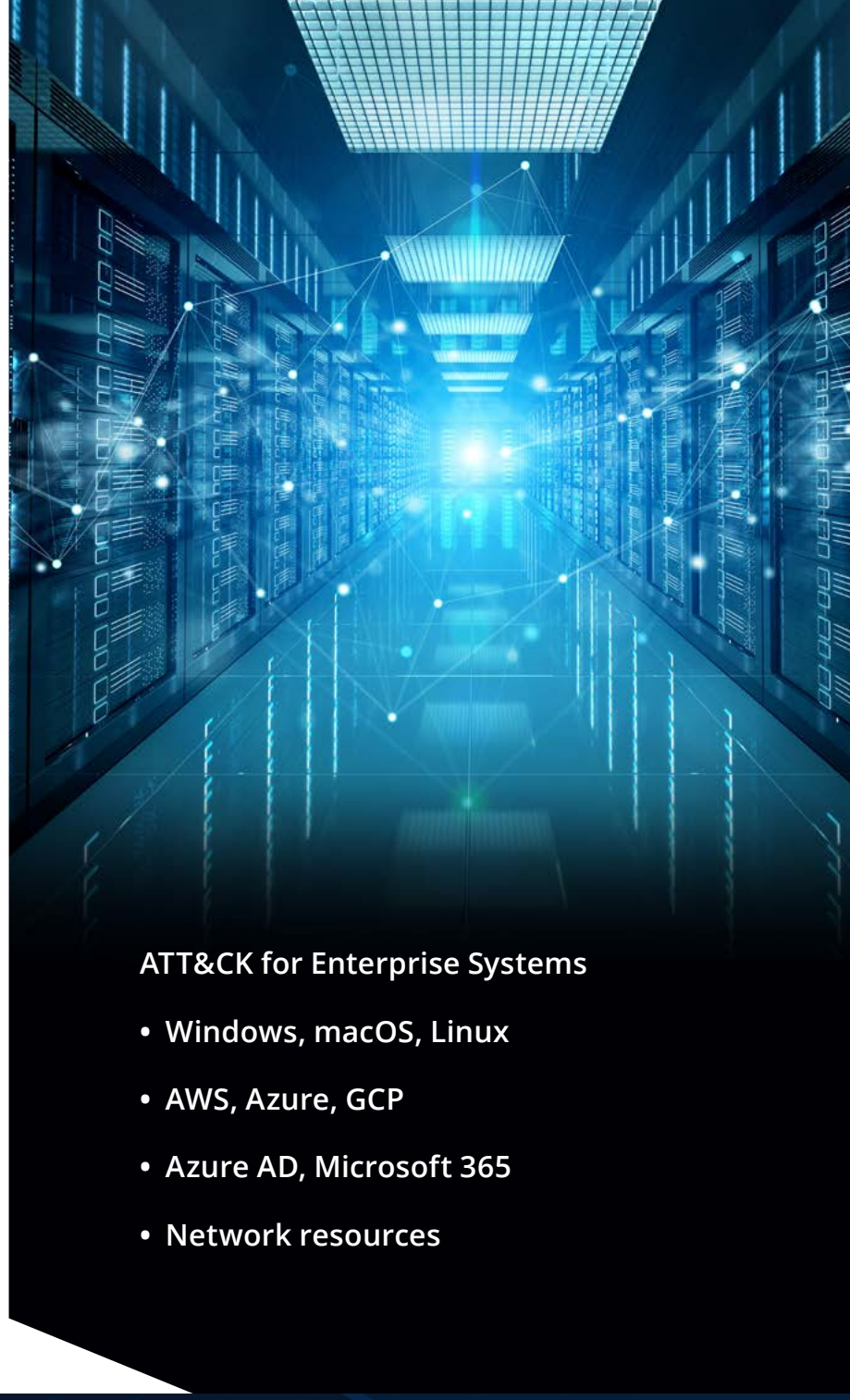
The latest ATT&CK for Enterprise Matrix, v8, introduces support for network infrastructure devices and details a range of pre-attack and co-attack adversarial tactics and techniques. More specifically, it includes two pre-attack tactics (collections of actions performed prior to an attack) and 14 attack tactics (collections of actions performed during an attack). ATT&CK for Enterprise tactics apply to various enterprise operating systems (Windows, macOS, Linux), cloud platforms (AWS, Microsoft Azure, Google Cloud Platform), SaaS solutions (Azure AD, Microsoft 365) and network resources.

ATT&CK FOR ENTERPRISE TACTICS

PRE-ATTACK → **ATTACK**

Reconnaissance	Inital Access	Defense Evasion	Collection
Resource Development	Execution	Credential Access	Command & CControl
	Persistence	Discovery	Exfiltration
	Privilege Escalation	Lateral Movement	Impact

Use ATT&CK Navigator to easily explore ATT&CK matrices and examine individual tactics, techniques and sub-techniques.

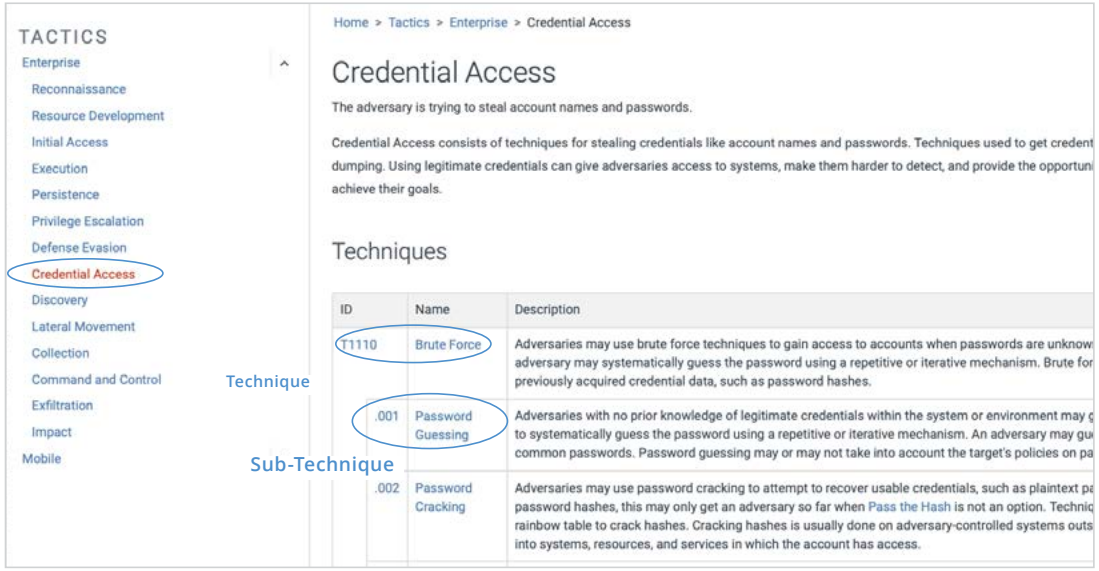


ATT&CK for Enterprise Systems

- Windows, macOS, Linux
- AWS, Azure, GCP
- Azure AD, Microsoft 365
- Network resources

TACTICS, TECHNIQUES AND SUB-TECHNIQUES

ATT&CK for Enterprise Matrix v8 includes 14 distinct tactics comprised of 177 techniques and 348 sub-techniques. Tactics can be defined as what the attacker is trying to achieve; whereby techniques and sub-techniques can be defined as how they are achieved. For example, the Credential Access tactic contains 14 techniques and 35 sub-techniques. Brute Force methods is one example of a Credential Access technique. Password Guessing and Password Cracking are examples of Brute Force sub-techniques.



Source: MITRE ATT&CK

With over 500 techniques and sub-techniques, it can be a challenge scoping out how to address these different areas, and where to begin. Establishing a cybersecurity program that aligns with the MITRE framework requires organizations to investigate areas across the attack chain that present the highest levels of risk and prioritize them accordingly. Implementing security controls that counter the techniques and sub-techniques also require prioritization; so it's not just the controls that are to be applied, it's to which systems they need to be applied to. Partnering with the right technology vendor and having the right plan in place will produce more positive outcomes in detecting and preventing these known techniques and sub-techniques.

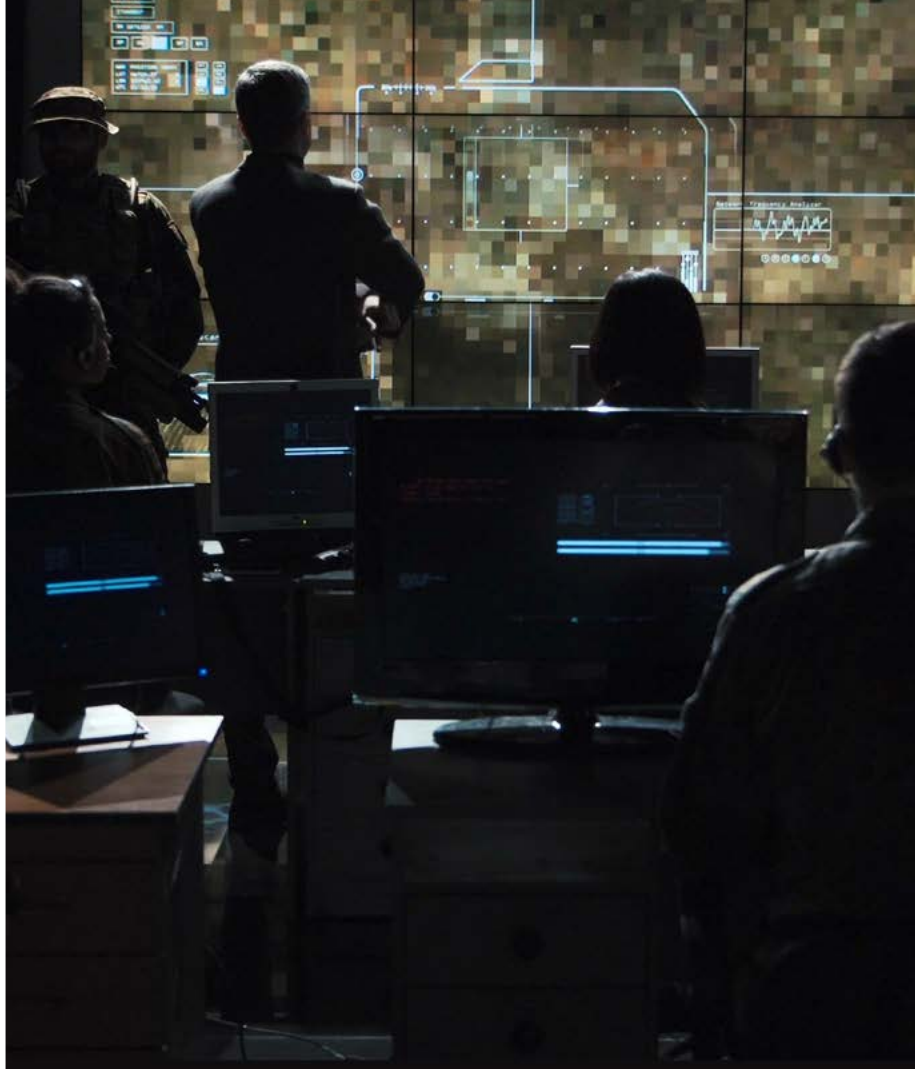
ATT&CK for Enterprise v8 describes 14 different tactics comprising 177 techniques and 348 sub-techniques.

BREAKING DOWN ADVERSERIAL BEHAVIOR DURING AN ATTACK

The 14 Enterprise attack tactics cover the various techniques adversaries typically use to infiltrate a network, compromise hosts, escalate privileges and move laterally undetected to steal data and inflict damage. Organizations can use these tactics and techniques to analyze security coverage, identify gaps in existing controls and defenses, hunt threats or carry out red team/blue team exercises.

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

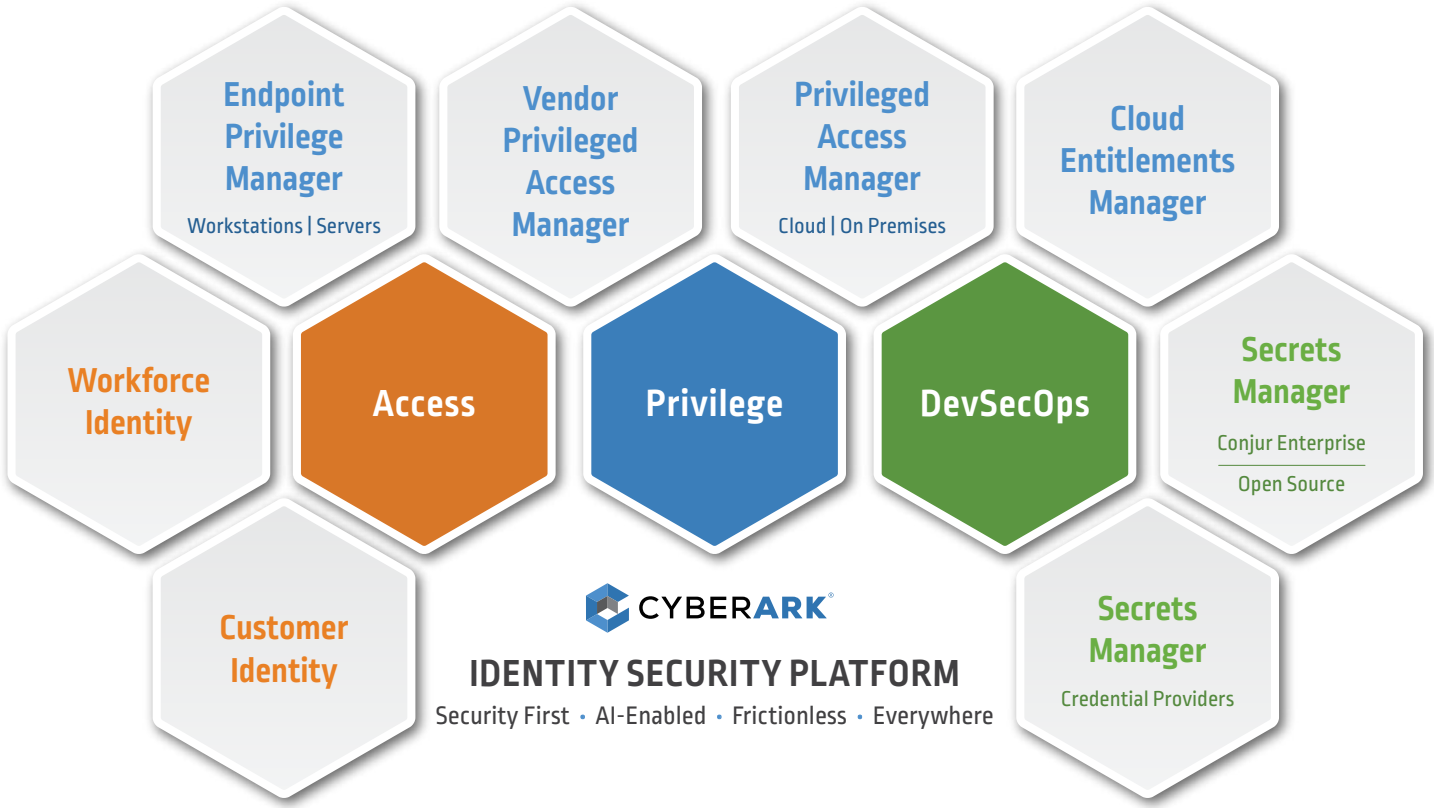
Click on the links in the table to explore the techniques and sub-techniques associated with a particular tactic.



Tactics describe what the adversary is trying to accomplish. Techniques describe the specific actions the adversary takes to achieve their goals.

CYBERARK SOLUTIONS AND THE MITRE ATT&CK FRAMEWORK

CyberArk's wide-ranging Identity Security Platform helps businesses protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. Ideal for security organizations adopting the MITRE ATT&CK framework, the CyberArk portfolio includes an extensive collection of access management, privileged access management and DevSecOps solutions – all of which provide foundational controls to the framework.



More than 6,300 organizations place their trust in CyberArk to provide comprehensive Identity Security solutions

Over 50% of the Fortune 500 use the CyberArk Identity Security Platform

MAPPING CYBERARK SOLUTIONS TO ATT&CK TACTICS AND TECHNIQUES

The CyberArk Identity Security Platform will help detect and mitigate a variety of ATT&CK for Enterprise techniques to defend your business against data breaches and malicious attacks. The solutions help prevent unauthorized access, stop lateral movement, and limit privilege escalation and abuse.

CyberArk Privileged Access Manager

CyberArk Privileged Access Manager Cloud and On Premises solutions efficiently manage privileged account credentials and access rights, proactively monitor and control privileged account activity, intelligently identify suspicious activity, and quickly respond to threats. The solutions help address a variety of Enterprise ATT&CK tactics including Initial Access, Persistence, Privilege Escalation, Credential Access and Lateral Movement.

CyberArk Endpoint Privilege Manager

CyberArk Endpoint Privilege Manager enforce least privilege security and application controls at the endpoint, helping contain attackers at the point of entry, before they can traverse your network and inflict serious damage. The solution supports Windows Server, Windows Desktop and Mac endpoints. Endpoint Privilege Manager helps defend against a number of Enterprise ATT&CK tactics including Initial Access, Execution, Persistence, Privilege Escalation, Credential Access and Lateral Movement.

CyberArk Secrets Manager

CyberArk Secrets Managermanages privileged access credentials and secrets used by commerical off-the-shelf software, internally developed applications and cloud-native apps. The solution strengthens security by removing credentials from applications and scripts, and keeping them out of public code repositories like Github where they are easy targets for adversaries. Secrets Manager helps address a variety of Enterprise ATT&CK tactics including Initial Access, Persistence, Privilege Escalation, Credential Access and Lateral Movement.

CyberArk Workforce Identity

CyberArk Workforce Identity is a SaaS-delivered suite of services designed to simplify identity management in enterprises. Workforce Identity unifies Single Sign-On, Adaptive Multi-Factor Authentication, Identity Lifecycle Management, and AI-powered User Behavior Analytics capabilities in a single platform. Workforce Identity helps address multiple areas across Enterprise ATT&CK tactics, including initial access, privilege escalation, lateral movement, and others.

Most businesses rely on a collection of security applications and services to cover the entire ATT&CK for Enterprise matrix. You can use CyberArk products, in conjunction with CyberArk-certified solutions, as part of a comprehensive ATT&CK cybersecurity program. The CyberArk C³ Alliance partner program and marketplace includes 200+ certified solutions from leading enterprise software, infrastructure, and security providers.

The table below provides a high-level solutions mapping to the MITRE Enterprise matrix. The CyberArk Identity Security Platform addresses many of the key areas categorized in this matrix through a defense-in-depth approach. Note that the darker the colors are in this table, the stronger the CyberArk controls and capabilities address these areas within the matrix. It's important to note that no single vendor can address all 14 tactics across the MITRE framework.

The CyberArk C³ Alliance is committed to integrating best of breed solutions that work together to minimize attack surface vulnerabilities, and maximize the ability to deter and respond to attacks while keeping operations running smoothly and efficiently. This broad ecosystem of technology partners complements CyberArk solutions to cover additional techniques and sub-techniques, providing end-to-end protection in the following categories: Reconnaissance, Resource Development, and Exfiltration, among many others.

CYBERARK®

	Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Access														
Privilege														
DevSecOps														

CONCLUSION

Malicious attackers can penetrate environments and move laterally to steal data or take down critical business systems. The MITRE ATT&CK framework can help reduce security vulnerabilities and mitigate risk by "thinking like an attacker" and defending against common adversarial tactics and techniques.

The CyberArk Identity Security Platform can help mitigate a number of ATT&CK for Enterprise tactics and techniques. CyberArk solutions can help avoid costly data breaches and crippling cyberattacks by detecting and containing bad actors in their tracks, before they can traverse the network and inflict serious damage.

Learn more

To learn more about ATT&CK, download the Getting Started with ATT&CK eBook from MITRE. It provides helpful tips and guidelines for putting ATT&CK into action based on available resources and overall maturity.

As the leader in Identity Security, CyberArk has the knowledge and resources to help secure critical areas across MITRE, and many other frameworks and standards. Start mitigating risk today from major breaches and advanced attacks by visiting www.cyberark.com to learn more about CyberArk solutions and services.

CYBERARK®

Why CyberArk

CyberArk (NASDAQ: **CYBR)** is the global leader in Identity Security. Centered on privileged access management, CyberArk provides the most comprehensive security solutions for any identity – human or machine – across business applications, distributed workforces, hybrid cloud workloads, and throughout DevOps pipelines. The world's leading organizations trust Cyberark to help secure their most critical assets.
To learn more about CyberArk, visit **www.cyberark.com**.