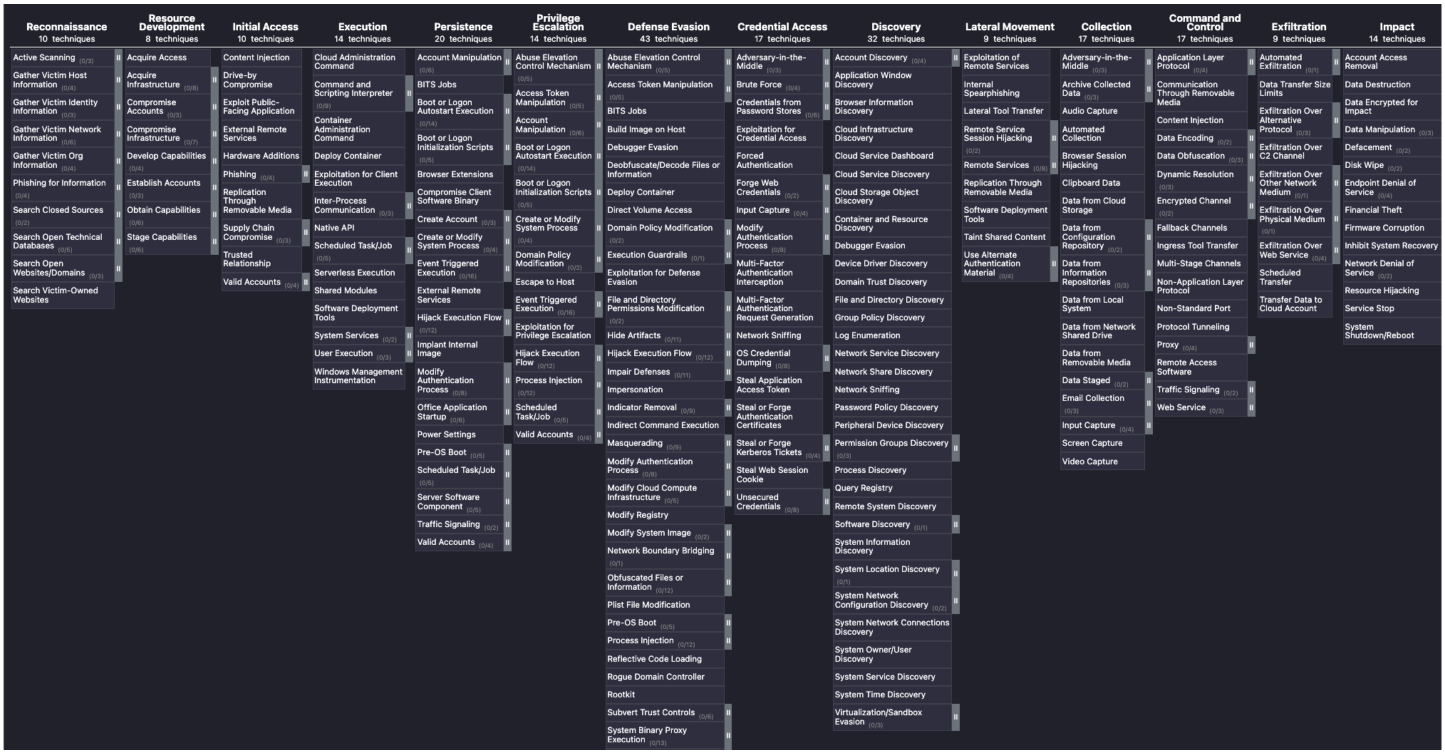
Mastering MITRE ATT&CK for Enterprise with a Zero Trust Model

How Zero Trust Access and Protection Stops Threats

In an era of escalating cyberattacks using a growing set of tactics, techniques, and procedures, enterprises are striving to identify and plug holes in their own security.

Understanding the MITRE ATT&CK Enterprise Matrix

The MITRE ATT&CK Matrix for Enterprise is a globally-recognized knowledge base used for understanding cyberattacker behavior. It catalogs real world cyberattacker tactics, techniques, and procedures—providing a structured approach to identifying security gaps and recommending detection and mitigation strategies. However, the complexity and sophistication of these attack tactics means that preventing them requires advanced security solutions.



Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 43 techniques	Credential Access 17 techniques	Discovery 32 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 17 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Create Account (0/3)	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Escape to Host	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (0/4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Implant Internal Image	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (0/3)	Modify Authentication Process (0/8)	Scheduled Task/Job (0/5)	Hide Artifacts (0/11)	Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (0/6)	Valid Accounts (0/4)	Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (0/3)	Proxy (0/4)		System Shutdown/Reboot
				Power Settings		Impair Defenses (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery		Input Capture (0/4)	Remote Access Software		
				Pre-OS Boot (0/5)		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling (0/2)		
				Scheduled Task/Job (0/5)		Indicator Removal (0/9)	Unsecured Credentials (0/8)	Network Sniffing		Video Capture	Web Service (0/3)		
				Server Software Component (0/5)		Indirect Command Execution		Password Policy Discovery					
				Traffic Signaling (0/2)		Masquerading (0/9)		Peripheral Device Discovery					
				Valid Accounts (0/4)		Modify Authentication Process (0/8)		Permission Groups Discovery (0/3)					
						Modify Cloud Compute Infrastructure (0/5)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (0/2)		Remote System Discovery					
						Network Boundary Bridging (0/1)		Software Discovery (0/1)					
						Obfuscated Files or Information (0/12)		System Information Discovery					
						Plist File Modification		System Location Discovery (0/1)					
						Pre-OS Boot (0/5)		System Network Configuration Discovery (0/2)					
						Process Injection (0/12)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls (0/6)		Virtualization/Sandbox Evasion (0/3)					
						System Binary Proxy Execution (0/13)							

MITRE ATT&CK Framework for Enterprise

The MITRE ATT&CK Matrix for Enterprise is divided into fourteen tactic categories, each with 8-43 techniques listed underneath. Many of the techniques throughout the framework rely on the attacker having gained access to legitimate credentials in the target environment.

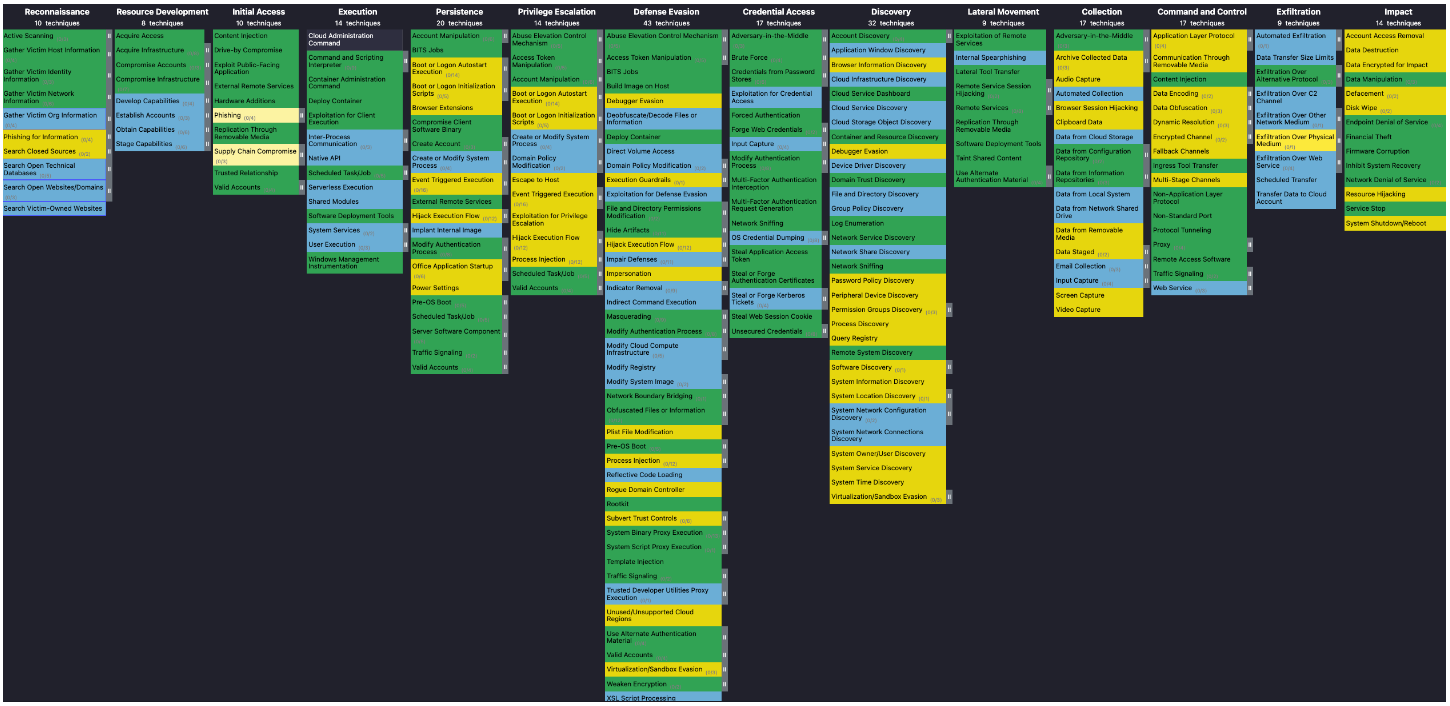
The Rise of Zero Trust

Real world circumstances like the rise of remote work, cloud, and bring-your-own-device policies, have driven a huge transformation in the types of interactions and access patterns occurring on critical enterprise systems. Data and applications that would formerly have only been accessible at the physical location of an enterprise's headquarters have been made available via the cloud and remote access software, accelerating business but also ballooning risk. Zero Trust Architectures for enabling this access while maintaining strict control over who can access what and when have become vitally important to the survival of the enterprise.

> ***"Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources…Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Authentication and authorization (both subject and device) are discrete functions performed before a session to an enterprise resource is established."***
>
> **- NIST 800-207 ZERO TRUST ARCHITECTURE**

Xage's Zero Trust Approach to Blocking Threats

Xage provides secure access and asset protection solutions with zero trust built in from the ground up. Xage provides mitigations for many of the techniques across the MITRE ATT&CK Matrix for Enterprise, in every tactic category. The following is a subset of Xage capabilities, with examples of how Xage protects against key high risk tactics, techniques, and procedures, including MITRE T-codes for each tactic and technique being discussed.



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/6)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (0/9)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/6)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts (0/5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/4)	Establish Accounts (0/3)	Phishing (0/4)	Inter-Process Communication (0/3)	Compromise Client Software Binary	Create or Modify System Process (0/4)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Create Account (0/3)	Domain Policy Modification (0/2)	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Web Service (0/4)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create or Modify System Process (0/4)	Escape to Host	Direct Volume Access	Modify Authentication Process (0/8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (0/3)		Trusted Relationship	Serverless Execution	Event Triggered Execution (0/16)	Event Triggered Execution (0/16)	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Ingress Tool Transfer	Transfer Data to Cloud Account	Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (0/4)	Shared Modules	External Remote Services	Exploitation for Privilege Escalation	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Multi-Stage Channels		Inhibit System Recovery
			Software Deployment Tools	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Implant Internal Image	Process Injection (0/12)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	File and Directory Discovery		Data from Removable Media	Non-Standard Port		Resource Hijacking
			User Execution (0/3)	Modify Authentication Process (0/8)	Scheduled Task/Job (0/5)	Hide Artifacts (0/11)	Steal Application Access Token	Group Policy Discovery		Data Staged (0/2)	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Office Application Startup (0/6)	Valid Accounts (0/4)	Hijack Execution Flow (0/12)	Steal or Forge Authentication Certificates	Log Enumeration		Email Collection (0/3)	Proxy (0/4)		System Shutdown/Reboot
				Power Settings		Impair Defenses (0/11)	Steal or Forge Kerberos Tickets (0/4)	Network Service Discovery		Input Capture (0/4)	Remote Access Software		
				Pre-OS Boot (0/5)		Impersonation	Steal Web Session Cookie	Network Share Discovery		Screen Capture	Traffic Signaling (0/2)		
				Scheduled Task/Job (0/5)		Indicator Removal (0/9)	Unsecured Credentials (0/8)	Network Sniffing		Video Capture	Web Service (0/3)		
				Server Software Component (0/5)		Indirect Command Execution		Password Policy Discovery					
				Traffic Signaling (0/2)		Masquerading (0/9)		Peripheral Device Discovery					
				Valid Accounts (0/4)		Modify Authentication Process (0/8)		Permission Groups Discovery (0/3)					
						Modify Cloud Compute Infrastructure (0/5)		Process Discovery					
						Modify Registry		Query Registry					
						Modify System Image (0/2)		Remote System Discovery					
						Network Boundary Bridging (0/1)		Software Discovery (0/1)					
						Obfuscated Files or Information (0/12)		System Information Discovery					
						Plist File Modification		System Location Discovery (0/1)					
						Pre-OS Boot (0/5)		System Network Configuration Discovery (0/2)					
						Process Injection (0/12)		System Network Connections Discovery					
						Reflective Code Loading		System Owner/User Discovery					
						Rogue Domain Controller		System Service Discovery					
						Rootkit		System Time Discovery					
						Subvert Trust Controls (0/6)		Virtualization/Sandbox Evasion (0/3)					
						System Binary Proxy Execution (0/13)							
						System Script Proxy Execution (0/1)							
						Template Injection							
						Traffic Signaling (0/2)							
						Trusted Developer Utilities Proxy Execution (0/1)							
						Unused/Unsupported Cloud Regions							
						Use Alternate Authentication Material (0/4)							
						Valid Accounts (0/4)							
						Virtualization/Sandbox Evasion (0/3)							
						Weaken Encryption (0/2)							
						XSL Script Processing							

Xage MITRE ATT&CK Enterprise Coverage

1. Zero Trust Identity and Access Management: Xage enforces strict identity verification for every device and user, ensuring that only authenticated and authorized entities can access system components. This directly prevents techniques like Valid Accounts (T1078) and User Execution (T1204) listed in the MITRE matrix. Since the vast majority of cyberattacks leverage stolen valid accounts acquired either through phishing or purchased on the dark web, preventing the abuse of valid accounts has an enormous positive impact on any organization's overall security posture.

2. Least Privilege Access: By implementing least privilege access controls, Xage ensures that even authenticated users are only given access to resources essential for their tasks. This limits the potential impact of numerous techniques in the tactic categories of Privilege Escalation (TA0004), Lateral Movement (TA0008), and Persistence (TA0003). These tactic categories, and particularly the technique of abusing Valid Accounts (T1078), have been used in some of the biggest cyberattacks of the last several years.

3. Continuous Monitoring and Breach Prevention: Xage's system continuously monitors network access events, identifying and preventing attempted policy violations in real-time. Xage also logs all access events and provides screen recordings of each session for rapid investigation and incident response. This capability is crucial for detecting and mitigating Command and Control (TA0011) tactics and Defense Evasion (TA0005) techniques.

4. Encryption, Data Integrity, and Data Access Control: Within Xage, all communications within the enterprise network are encrypted, and data integrity checks are a standard. All data access and data transfer is controlled based on centrally-managed least privilege policies. This combats Adversary-in-the-Middle (T1557) and Data Destruction (T1485) threats and prevents data from being exfiltrated or shared with the wrong parties either maliciously or by accident.

5. Segmentation and Microsegmentation: Xage creates secure zones within the enterprise network environment, isolating critical components. This segmentation is vital for protecting against a dozen techniques contained in the Target Discovery (TA0007) and Lateral Movement (TA0008) tactic categories and reducing the blast radius of any potential breach. Xage delivers zero trust microsegmentation that can extend all the way to the enterprise edge, and even into operational and Industrial Control Systems. Learn more about Xage's coverage of the MITRE ATT&CK Matrix for ICS here.

Real-World Outcomes in Enterprise Cybersecurity

Many organizations have adopted Xage's Zero Trust Access and Protection solutions and achieved significant enhancements in their security posture. A major energy company eliminated risk against thousands of user accounts that had access to critical assets. The United States Space Force is achieving the goals of the Department of Defense's Zero Trust Roadmap, using Xage.

The Department of Energy's National Renewable Energy Lab tested Xage's ability to block critical, real-world MITRE techniques, using a realistic cyber range emulating actual power utility environments. Xage prevented numerous MITRE techniques pulled straight from recent, attacks against critical energy infrastructure. Read More

MITRE-Enhanced Security with Xage

The MITRE ATT&CK Matrix for Enterprise provides a valuable framework for understanding potential threats in enterprise environments with complexities such as hybrid and multi-cloud deployments, local and remote workers, and a combination of legacy and modern assets. However, the real game-changer is implementing a robust defense mechanism against these threats. Xage's Zero Trust solutions demonstrate a proactive and effective approach to securing enterprise infrastructure, from on-premises to private datacenter to multiple public clouds, while still enabling access and ease-of-use, offering a much-needed shield in an increasingly hostile digital landscape.

Contact us for further information about the MITRE ATT&CK Matrix for Enterprise and how Xage's Zero Trust Access and Protection solutions provide protection across every Tactic category in the framework and robust attack prevention against the most common and devastating techniques.