WHITEPAPER

MAPPING BEYONDTRUST CAPABILITIES TO MITRE ATT&CK™ NAVIGATOR

BeyondTrust

CONTENTS

MITRE ATT&CK™ 1
Defining the Tactics 2
How BeyondTrust Helps to Mitigate Risks Identified in MITRE ATT&CK Framework ... 4
TA0001 – Initial Access 5
TA0002 – Execution 5
TA0003 – Persistence 7
TA0004 – Privileged Escalation 9
TA0005 – Defense Evasion 11
TA0006 – Credential Access 13
TA0007 – Discovery 15
TA0008 – Lateral Movement 16
TA0009 – Collection 17
TA0010 – Exfiltration 18
TA0011 – Command And Control 19
TA0040 – Impact 20
The Beyondtrust Privileged Access Management Platform 21

MITRE ATT&CK™

With the volume of cyberattacks growing every day, organizations are increasingly relying on third-parties to help discover, prioritize, categorize, and provide guidance to remediate threats. Once such third party is MITRE and their ATT&CK™ knowledge base. MITRE started ATT&CK in 2013 to document common tactics, techniques, and procedures (TTPs) that advanced persistent threats use against Windows enterprise networks.

According to the MITRE website:

- MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

- Open and available to any person or organization for use at no charge, the goal of MITRE ATT&CK is to bring communities together to develop more effective cybersecurity.

BeyondTrust has mapped its PAM solutions for privileged password management, endpoint privilege management, and secure remote access into the ATT&CK framework by tactic and technique. With this mapping, organizations can better optimize the return on their security investments.

Defining the Tactics

The MITRE ATT&CK framework includes the following tactics - all definitions can be found on the MITRE website.

- **Initial Access (TA0001)** Represents the vectors adversaries use to gain an initial foothold within a network.

- **Execution (TA0002)** Represents techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with initial access as the means of executing code once access is obtained, and lateral movement to expand access to remote systems on a network.

- **Persistence (TA0003)** Any access, action, or configuration change to a system that gives an adversary a persistent presence on that system. Adversaries will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or alternate backdoor for them to regain access.

- **Privilege Escalation (TA0004)** The result of actions that allows an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. Adversaries can enter a system with unprivileged access and must take advantage of a system weakness to obtain local administrator or SYSTEM/root level privileges. A user account with administrator-like access can also be used. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.

- **Defense Evasion (TA0005)** Consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as or variations of techniques in other categories that have the added benefit of subverting a particular defense or mitigation. Defense evasion may be considered a set of attributes the adversary applies to all other phases of the operation.

- **Credential Access (TA0006)** Represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or

domain users with administrator access) to use within the network. This allows the adversary to assume the identity of the account, with all of that account's permissions on the system and network and makes it harder for defenders to detect the adversary. With sufficient access within a network, an adversary can create accounts for later use within the environment.

- **Discovery (TA0007)** Consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.

- **Lateral Movement (TA0008)** Consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool.

- **Collection (TA0009)** Consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.

- **Exfiltration (TA0010)** Refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.

- **Command and Control (TA0011)** Represents how adversaries communicate with systems under their control within a target network. There are many ways an adversary can establish command and control with various levels of covertness, depending on system configuration and network topology. Due to the wide degree of variation available to the adversary at the network level, only the most common factors were used to describe the differences in command and control. There are still a great many specific techniques within the documented methods, largely due to how easy it is to define new protocols and use existing, legitimate protocols and network services for communication.

- **Impact (TA0040)** The adversary is trying to manipulate, interrupt, or destroy your systems and data. Impact consists of techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes. Techniques used for impact can include destroying or tampering with data. In some cases, business processes can look fine, but may have been altered to benefit the adversaries' goals. These techniques might be used by adversaries to follow through on their end goal or to provide cover for a confidentiality breach.

How BeyondTrust Helps to Mitigate Risks Identified in MITRE ATT&CK Framework

The following tables map BeyondTrust capabilities to the techniques identified within the tactics categorized in MITRE ATT&CK. The BeyondTrust capability mapping is represented by three columns:

- **Detect –** The ability to identify or discover all or part of the Techniques related to an Enterprise Tactic
- **Prevent –** The ability to stop or mitigate all or part of the Techniques related to an Enterprise Tactic
- **Respond –** The ability to generate notifications or alerts in the form of email, SIEM Event, SNMP Trap, or Scheduled Report

TA0001 – Initial Access

Technique ID	TA0001 – Initial Access	BeyondTrust Capability		
		Detect	Prevent	Respond
T1189	Drive-by Compromise	Y	Y	Y
T1190	Exploit Public-Facing Application	Y	Y	Y
T1133	External Remote Services	Y	Y	Y
T1200	Hardware Additions	Y	Y	Y
T1091	Replication Through Removable Media	Y	Y	Y
T1193	Spearphishing Attachment	Y	Y	Y
T1192	Spearphishing Link	Y	Y	Y
T1194	Spearphishing via Service	Y	Y	Y
T1195	Supply Chain Compromise	n/a		
T1199	Trusted Relationship	Y	Y	Y
T1078	Valid Accounts	Y	Y	Y

TA0002 – Execution

Technique ID	TA0002 – Execution	BeyondTrust Capability		
		Detect	Prevent	Respond
T1155	AppleScript	Y	Y	Y
T1191	CMSTP	Y	Y	Y
T1059	Command-Line Interface	Y	Y	Y
T1223	Compiled HTML File	Y	Y	Y
T1175	Component Object Model and Distributed COM	Y	Y	Y
T1196	Control Panel Items	Y	Y	Y
T1173	Dynamic Data Exchange	Y	Y	Y
T1106	Execution through API	Y	Y	Y

Technique ID	TA0002 – Execution	BeyondTrust Capability		
		Detect	Prevent	Respond
T1129	Execution through Module Load	Y	Y	Y
T1203	Exploitation for Client Execution	Y	Y	Y
T1061	Graphical User Interface	Y	Y	Y
T1118	InstallUtil	Y	Y	Y
T1152	Launchctl	Y	Y	Y
T1168	Local Job Scheduling	Y	Y	Y
T1177	LSASS Driver	Y	Y	Y
T1170	Mshta	Y	Y	Y
T1086	PowerShell	Y	Y	Y
T1121	Regsvcs/Regasm	Y	Y	Y
T1117	Regsvr32	Y	Y	Y
T1085	Rundll32	Y	Y	Y
T1053	Scheduled Task	Y	Y	Y
T1064	Scripting	Y	Y	Y
T1035	Service Execution	Y	Y	Y
T1218	Signed Binary Proxy Execution	Y	Y	Y
T1216	Signed Script Proxy Execution	Y	Y	Y
T1153	Source	Y	Y	Y
T1151	Space after Filename	Y	Y	Y
T1072	Third-party Software	Y	Y	Y
T1154	Trap	Y	Y	Y
T1127	Trusted Developer Utilities	Y	Y	Y
T1204	User Execution	Y	Y	Y
T1047	Windows Management Instrumentation	Y	Y	Y
T1028	Windows Remote Management	Y	Y	Y
T1220	XSL Script Processing	Y	Y	Y

TA0003 – Persistence

Technique ID	TA0003 – Persistence	BeyondTrust Capability		
		Detect	Prevent	Respond
T1156	.bash_profile and .bashrc	Y	Y	Y
T1015	Accessibility Features	Y	Y	Y
T1098	Account Manipulation	Y	Y	Y
T1182	AppCert DLLs	Y	Y	Y
T1103	AppInit DLLs	Y	Y	Y
T1138	Application Shimming	Y	Y	Y
T1131	Authentication Package	Y	Y	Y
T1197	BITS Jobs	Y	Y	Y
T1067	Bootkit	Y	Y	Y
T1176	Browser Extensions	Y	Y	Y
T1042	Change Default File Association	Y	Y	Y
T1109	Component Firmware	n/a		
T1122	Component Object Model Hijacking	Y	Y	Y
T1136	Create Account	Y	Y	Y
T1038	DLL Search Order Hijacking	Y	Y	Y
T1157	Dylib Hijacking	Y	Y	Y
T1519	Emond	Y	Y	Y
T1133	External Remote Services	N	Y	N
T1044	File System Permissions Weakness	Y	Y	Y
T1158	Hidden Files and Directories	Y	Y	Y
T1179	Hooking	Y	Y	Y
T1062	Hypervisor	n/a		
T1183	Image File Execution Options Injection	n/a		
T1525	Implant Container Image	Y	Y	Y
T1215	Kernel Modules and Extensions	Y	Y	Y

Technique ID	TA0003 – Persistence	BeyondTrust Capability		
		Detect	Prevent	Respond
T1159	Launch Agent	N	Y	N
T1160	Launch Daemon	N	Y	N
T1152	Launchctl	Y	Y	Y
T1161	LC_LOAD_DYLIB Addition	n/a	n/a	n/a
T1168	Local Job Scheduling	Y	Y	Y
T1162	Login Item	Y	Y	Y
T1037	Logon Scripts	Y	Y	Y
T1177	LSASS Driver	Y	Y	Y
T1031	Modify Existing Service	Y	Y	Y
T1128	Netsh Helper DLL	Y	Y	Y
T1050	New Service	Y	Y	Y
T1137	Office Application Startup	Y	Y	Y
T1034	Path Interception	Y	Y	Y
T1150	Plist Modification	Y	Y	Y
T1205	Port Knocking	n/a		
T1013	Port Monitors	n/a		
T1504	PowerShell Profile	Y	Y	Y
T1163	Rc.common	Y	Y	Y
T1164	Re-opened Applications	n/a	n/a	n/a
T1108	Redundant Access	n/a		
T1060	Registry Run Keys / Startup Folder	Y	Y	Y
T1053	Scheduled Task	Y	Y	Y
T1180	Screensaver	Y	Y	Y
T1101	Security Support Provider	Y	Y	Y
T1505	Server Software Component	Y	Y	Y
T1058	Service Registry Permissions Weakness	Y	Y	Y
T1166	Setuid and Setgid	Y	Y	Y

Technique ID	TA0003 – Persistence	BeyondTrust Capability		
		Detect	Prevent	Respond
T1023	Shortcut Modification	Y	Y	Y
T1198	SIP and Trust Provider Hijacking	Y	Y	Y
T1165	Startup Items	Y	Y	Y
T1019	System Firmware	n/a		
T1501	Systemd Service	Y	Y	Y
T1209	Time Providers	Y	Y	Y
T1154	Trap	n/a	n/a	n/a
T1078	Valid Accounts	Y	Y	Y
T1100	Web Shell	Y	Y	Y
T1084	Windows Management Instrumentation Event Subscription	Y	Y	Y
T1004	Winlogon Helper DLL	Y	Y	Y

TA0004 – Privileged Escalation

Technique ID	TA004 – Privilege Escalation	BeyondTrust Capability		
		Detect	Prevent	Respond
T1134	Access Token Manipulation	Y	Y	Y
T1015	Accessibility Features	Y	Y	Y
T1182	AppCert DLLs	Y	Y	Y
T1103	AppInit DLLs	Y	Y	Y
T1138	Application Shimming	Y	Y	Y
T1088	Bypass User Account Control	Y	Y	Y
T1038	DLL Search Order Hijacking	Y	Y	Y
T1157	Dylib Hijacking	Y	Y	Y
T1514	Elevated Execution with Prompt	Y	Y	Y
T1519	Emond	Y	Y	Y
T1068	Exploitation for Privilege Escalation	Y	Y	Y
T1181	Extra Window Memory Injection	n/a		

Technique ID	TA004 – Privilege Escalation	BeyondTrust Capability		
		Detect	Prevent	Respond
T1044	File System Permissions Weakness	Y	Y	Y
T1179	Hooking	Y	Y	Y
T1183	Image File Execution Options Injection	Y	Y	Y
T1160	Launch Daemon	Y	Y	Y
T1050	New Service	Y	Y	Y
T1502	Parent PID Spoofing	Y	Y	Y
T1034	Path Interception	Y	Y	Y
T1150	Plist Modification	Y	Y	Y
T1013	Port Monitors	Y	Y	Y
T1504	PowerShell Profile	Y	Y	Y
T1055	Process Injection	Y	Y	Y
T1053	Scheduled Task	Y	Y	Y
T1058	Service Registry Permissions Weakness	Y	Y	Y
T1166	Setuid and Setgid	Y	Y	Y
T1178	SID-History Injection	Y	Y	Y
T1165	Startup Items	Y	Y	Y
T1169	Sudo	Y	Y	Y
T1206	Sudo Caching	Y	Y	Y
T1078	Valid Accounts	Y	Y	Y
T1100	Web Shell	Y	Y	Y

TA0005 – Defense Evasion

Technique ID	TA005 – Defense Evasion	BeyondTrust Capability		
		Detect	Prevent	Respond
T1134	Access Token Manipulation	Y	Y	Y
T1527	Application Access Token	Y	Y	Y
T1009	Binary Padding	Y	Y	Y
T1197	BITS Jobs	N	Y	N
T1088	Bypass User Account Control	Y	Y	Y
T1146	Clear Command History	Y	Y	Y
T1191	CMSTP	Y	Y	Y
T1116	Code Signing	Y	Y	Y
T1500	Compile After Delivery	Y	Y	Y
T1223	Compiled HTML File	Y	Y	Y
T1109	Component Firmware	n/a		
T1122	Component Object Model Hijacking	Y	Y	Y
T1090	Connection Proxy	n/a		
T1196	Control Panel Items	Y	Y	Y
T1207	DCShadow	Y	Y	Y
T1140	Deobfuscate/Decode Files or Information	Y	Y	Y
T1089	Disabling Security Tools	Y	Y	Y
T1038	DLL Search Order Hijacking	Y	Y	Y
T1073	DLL Side-Loading	Y	Y	Y
T1480	Execution Guardrails	n/a		
T1211	Exploitation for Defense Evasion	Y	Y	Y
T1181	Extra Window Memory Injection	n/a		
T1222	File and Directory Permissions Modification	Y	Y	Y
T1107	File Deletion	Y	Y	Y

Technique ID	TA005 – Defense Evasion	BeyondTrust Capability		
		Detect	Prevent	Respond
T1006	File System Logical Offsets	n/a	n/a	n/a
T1144	Gatekeeper Bypass	Y	Y	Y
T1484	Group Policy Modification	Y	Y	Y
T1158	Hidden Files and Directories	Y	Y	Y
T1147	Hidden Users	Y	Y	Y
T1143	Hidden Window	Y	Y	Y
T1148	HISTCONTROL	Y	Y	Y
T1183	Image File Execution Options Injection	Y	Y	Y
T1054	Indicator Blocking	n/a		
T1066	Indicator Removal from Tools	n/a		
T1070	Indicator Removal on Host	n/a		
T1202	Indirect Command Execution	Y	Y	Y
T1130	Install Root Certificate	Y	Y	Y
T1118	InstallUtil	Y	Y	Y
T1152	Launchctl	Y	Y	Y
T1149	LC_MAIN Hijacking	n/a		
T1036	Masquerading	Y	Y	Y
T1112	Modify Registry	Y	Y	Y
T1170	Mshta	Y	Y	Y
T1126	Network Share Connection Removal	Y	Y	Y
T1096	NTFS File Attributes	n/a		
T1027	Obfuscated Files or Information	n/a		
T1502	Parent PID Spoofing	Y	Y	Y
T1150	Plist Modification	n/a		
T1205	Port Knocking	n/a		
T1186	Process Doppelgänging	n/a		
T1093	Process Hollowing	n/a		

Technique ID	TA005 – Defense Evasion	BeyondTrust Capability		
		Detect	Prevent	Respond
T1055	Process Injection	Y	Y	Y
T1108	Redundant Access	Y	Y	Y
T1121	Regsvcs/Regasm	Y	Y	Y
T1117	Regsvr32	Y	Y	Y
T1536	Revert Cloud Instance	n/a		
T1014	Rootkit	n/a		
T1085	Rundll32	Y	Y	Y
T1064	Scripting	Y	Y	Y
T1218	Signed Binary Proxy Execution	Y	Y	Y
T1216	Signed Script Proxy Execution	Y	Y	Y
T1198	SIP and Trust Provider Hijacking	Y	Y	Y
T1045	Software Packing	n/a		
T1151	Space after Filename	Y	Y	Y
T1221	Template Injection	n/a		
T1099	Timestomp	n/a		
T1127	Trusted Developer Utilities	Y	Y	Y
T1535	Unused/Unsupported Cloud Regions	n/a		
T1078	Valid Accounts	Y	Y	Y
T1497	Virtualization/Sandbox Evasion	Y	Y	Y
T1102	Web Service	n/a		
T1506	Web Session Cookie	n/a		
T1220	XSL Script Processing	n/a		

TA0006 – Credential Access

Technique ID	TA006 – Credential Access	BeyondTrust Capability		
		Detect	Prevent	Respond
T1098	Account Manipulation	Y	Y	Y
T1139	Bash History	Y	Y	Y
T1110	Brute Force	Y	Y	Y
T1522	Cloud Instance Metadata API	n/a		
T1003	Credential Dumping	Y	Y	Y
T1503	Credentials from Web Browsers	Y	Y	Y
T1081	Credentials in Files	Y	Y	Y
T1214	Credentials in Registry	Y	Y	Y
T1212	Exploitation for Credential Access	n/a		
T1187	Forced Authentication	Y	Y	Y
T1179	Hooking	Y	Y	Y
T1056	Input Capture	Y	Y	Y
T1141	Input Prompt	Y	Y	Y
T1208	Kerberoasting	Y	Y	Y
T1142	Keychain	Y	Y	Y
T1171	LLMNR/NBT-NS Poisoning and Relay	n/a		
T1040	Network Sniffing	n/a		
T1174	Password Filter DLL	Y	Y	Y
T1145	Private Keys	Y	Y	Y
T1167	Securityd Memory	n/a		
T1111	Two-Factor Authentication Interception	n/a		

TA0007 – Discovery

Technique ID	TA007 – Discovery	BeyondTrust Capability		
		Detect	Prevent	Respond
T1087	Account Discovery	Y	Y	Y
T1010	Application Window Discovery	Y	Y	Y
T1217	Browser Bookmark Discovery	n/a		
T1538	Cloud Service Dashboard	n/a		
T1526	Cloud Service Discovery	n/a		
T1482	Domain Trust Discovery	Y	Y	Y
T1083	File and Directory Discovery	Y	Y	Y
T1046	Network Service Scanning	Y	Y	Y
T1135	Network Share Discovery	Y	Y	Y
T1040	Network Sniffing	n/a		
T1201	Password Policy Discovery	Y	Y	Y
T1120	Peripheral Device Discovery	Y	Y	Y
T1069	Permission Groups Discovery	Y	Y	Y
T1057	Process Discovery	Y	Y	Y
T1012	Query Registry	Y	Y	Y
T1018	Remote System Discovery	Y	Y	Y
T1063	Security Software Discovery	Y	Y	Y
T1082	System Information Discovery	Y	Y	Y
T1016	System Network Configuration Discovery	Y	Y	Y
T1049	System Network Connections Discovery	Y	Y	Y
T1033	System Owner/User Discovery	Y	Y	Y
T1007	System Service Discovery	Y	Y	Y
T1124	System Time Discovery	Y	Y	Y
T1497	Virtualization/Sandbox Evasion	Y	Y	Y

TA0008 – Lateral Movement

Technique ID	TA008 – Lateral Movement	BeyondTrust Capability		
		Detect	Prevent	Respond
T1155	AppleScript	Y	Y	Y
T1527	Application Access Token	Y	Y	Y
T1017	Application Deployment Software	Y	Y	Y
T1175	Component Object Model and Distributed COM	Y	Y	Y
T1210	Exploitation of Remote Services	Y	Y	Y
T1534	Internal Spearphishing	N/A		
T1037	Logon Scripts	Y	Y	Y
T1075	Pass the Hash	Y	Y	Y
T1097	Pass the Ticket	Y	Y	Y
T1076	Remote Desktop Protocol	Y	Y	Y
T1105	Remote File Copy	Y	Y	Y
T1021	Remote Services	Y	Y	Y
T1091	Replication Through Removable Media	Y	Y	Y
T1051	Shared Webroot	Y	Y	y
T1184	SSH Hijacking	Y	Y	Y
T1080	Taint Shared Content	n/a		
T1072	Third-party Software	Y	Y	Y
T1506	Web Session Cookie	n/a		
T1077	Windows Admin Shares	Y	Y	Y
T1028	Windows Remote Management	Y	Y	Y

TA0009 – Collection

Technique ID	TA009 – Collection	BeyondTrust Capability		
		Detect	Prevent	Respond
T1123	Audio Capture	n/a		
T1119	Automated Collection	Y	Y	Y
T1115	Clipboard Data	n/a	n/a	n/a
T1530	Data from Cloud Storage Object	n/a		
T1213	Data from Information Repositories	Y	Y	Y
T1005	Data from Local System	Y	Y	Y
T1039	Data from Network Shared Drive	Y	Y	Y
T1025	Data from Removable Media	Y	Y	Y
T1074	Data Staged	Y	Y	Y
T1114	Email Collection	n/a		
T1056	Input Capture	Y	Y	Y
T1185	Man in the Browser	n/a		
T1113	Screen Capture	Y	Y	Y
T1125	Video Capture	Y	Y	Y

TA0010 – Exfiltration

Technique ID	TA0010 – Exfiltration	BeyondTrust Capability		
		Detect	Prevent	Respond
T1020	Automated Exfiltration	n/a	n/a	n/a
T1002	Data Compressed	Y	Y	Y
T1022	Data Encrypted	Y	Y	Y
T1030	Data Transfer Size Limits	n/a	n/a	
T1048	Exfiltration Over Alternative Protocol	n/a	n/a	
T1041	Exfiltration Over Command and Control Channel	n/a	n/a	
T1011	Exfiltration Over Other Network Medium	n/a	n/a	
T1052	Exfiltration Over Physical Medium	Y	Y	Y
T1029	Scheduled Transfer	n/a	n/a	
T1537	Transfer Data to Cloud Account	Y	Y	Y

TA0011 – Command And Control

Technique ID	TA0011 – Command And Control	BeyondTrust Capability		
		Detect	Prevent	Respond
T1043	Commonly Used Port	Y	Y	Y
T1092	Communication Through Removable Media	Y	Y	Y
T1090	Connection Proxy	n/a	n/a	
T1094	Custom Command and Control Protocol	n/a	n/a	
T1024	Custom Cryptographic Protocol	n/a	n/a	
T1132	Data Encoding	n/a	n/a	
T1001	Data Obfuscation	n/a	n/a	
T1172	Domain Fronting	n/a	n/a	
T1483	Domain Generation Algorithms	n/a	n/a	
T1008	Fallback Channels	n/a	n/a	
T1188	Multi-hop Proxy	n/a	n/a	
T1104	Multi-Stage Channels	n/a	n/a	
T1026	Multiband Communication	n/a	n/a	
T1079	Multilayer Encryption	n/a	n/a	
T1205	Port Knocking	n/a	n/a	
T1219	Remote Access Tools	Y	Y	Y
T1105	Remote File Copy	Y	Y	Y
T1071	Standard Application Layer Protocol	N	Y	N
T1032	Standard Cryptographic Protocol	n/a	n/a	
T1095	Standard Non-Application Layer Protocol	n/a	n/a	
T1065	Uncommonly Used Port	n/a	n/a	
T1102	Web Service	n/a	n/a	

TA0040 – Impact

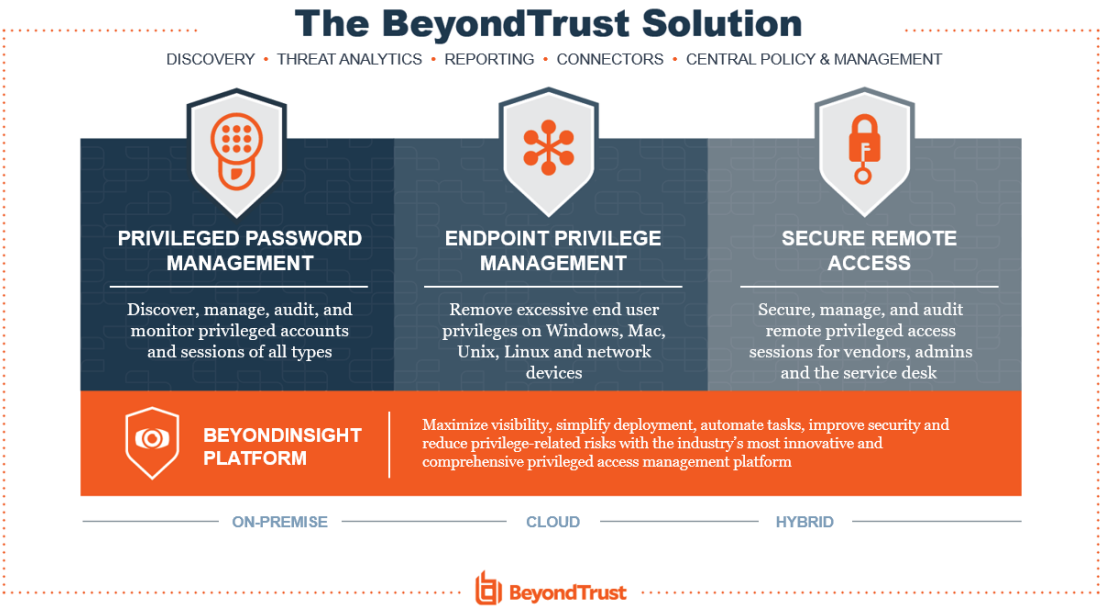
Technique ID	TA0011 – Exfiltration	BeyondTrust Capability		
		Detect	Prevent	Respond
T1531	Account Access Removal	Y	Y	
T1485	Data Destruction	Y	Y	
T1486	Data Encrypted for Impact	Y	Y	
T1491	Defacement	n/a	n/a	
T1488	Disk Content Wipe	Y	Y	
T1487	Disk Structure Wipe	Y	Y	
T1499	Endpoint Denial of Service	Y	Y	
T1495	Firmware Corruption	n/a	n/a	
T1490	Inhibit System Recovery	Y	Y	
T1498	Network Denial of Service	n/a	n/a	
T1496	Resource Hijacking	Y	Y	
T1494	Runtime Data Manipulation	Y	Y	
T1489	Service Stop	Y	Y	
T1492	Stored Data Manipulation	Y	Y	
T1529	System Shutdown/Reboot	Y	Y	
T1493	Transmitted Data Manipulation	n/a	n/a	

The Beyondtrust Privileged Access Management Platform

The BeyondTrust Privileged Access Management (PAM) portfolio is an integrated solution set that provides visibility and control over the entire universe of privileges—identities, endpoints, and sessions.

BeyondTrust delivers what industry experts consider to be the complete spectrum of privileged access management solutions. In the 2018 Magic Quadrant for Privileged Access Management, Gartner named BeyondTrust as a leader for all solution categories in the PAM market.

BeyondTrust's extensible, centrally managed platform allows you to roll out a complete set of PAM capabilities at once, or phase in capabilities over time at your own pace.



BeyondTrust's Universal Privilege Management approach provides the most practical, complete, and scalable approach to protecting privileged identities (human and machine), endpoints, and sessions by implementing comprehensive layers of security, control, and monitoring. The complete BeyondTrust solution allows you to address the entire journey to Universal Privilege Management, to drastically reduce your attack surface and threat windows.

By uniting the broadest set of privileged security capabilities, BeyondTrust simplifies deployments, reduces costs, improves usability, and reduces privilege risks.

ABOUT BEYONDTRUST

BeyondTrust is the worldwide leader in Privileged Access Management (PAM), empowering organizations to secure and manage their entire universe of privileges. Our integrated products and platform offer the industry's most advanced PAM solution, enabling organizations to quickly shrink their attack surface across traditional, cloud and hybrid environments.

The BeyondTrust Universal Privilege Management approach secures and protects privileges across passwords, endpoints, and access, giving organizations the visibility and control they need to reduce risk, achieve compliance, and boost operational performance. Our products enable the right level of privileges for just the time needed, creating a frictionless experience for users that enhances productivity.

With a heritage of innovation and a staunch commitment to customers, BeyondTrust solutions are easy to deploy, manage, and scale as businesses evolve. We are trusted by 20,000 customers, including 70 percent of the Fortune 500, and a global partner network.

Learn more at beyondtrust.com.