MORPHISEC

5 COST-FREE WAYS FOR ENTERPRISES **TO IMPROVE SECURITY**

INTRODUCTION

One of the common misnomers in cybersecurity planning is that every organization has the budget necessary to deploy the most advanced tools and the highest-end countermeasures to secure their critical infrastructure. The reality is almost exactly the opposite. Most companies don't have unlimited resources when it comes to their cybersecurity posture. If anything, these resource-constrained or "lean" security teams need to protect themselves against attacks without spending beyond their means. Sometimes these lean teams don't even have dedicated security staff, but instead make cybersecurity a responsibility of an IT generalist.

The cybersecurity skills shortage in the United States doesn't help matters. Research shows the US has less than half the trained cybersecurity professionals it needs to keep up with demand. One survey found that 70% of respondents think their company suffers from talent shortages in terms of cybersecurity. Shortages could apply to the number of staff, a lack of advanced/specialized skills, or both. In all cases, though, limited talent and tight budgets put defenders at a distinct disadvantage against a growing army of cybercriminals.

71%
of executives surveyed think a cybersecurity talent gap causes them "**direct and measurable damage**"

Despite some indications the talent shortage is getting better, it will take time to train the millions of professionals currently missing from the job market. Due to a relatively small supply of trained cybersecurity workers--estimates suggest there's only one trained professional for every 10 businesses in the US--lean security teams with only one or even no dedicated security resources are common. Even when companies have the resources to potentially hire an in-house team or expand their current one, the demand for talent far exceeds the supply and will for years to come. Lean, resource-constrained security teams aren't going anywhere, calling pointed attention to the need for other ways to solve for the increasing risk.

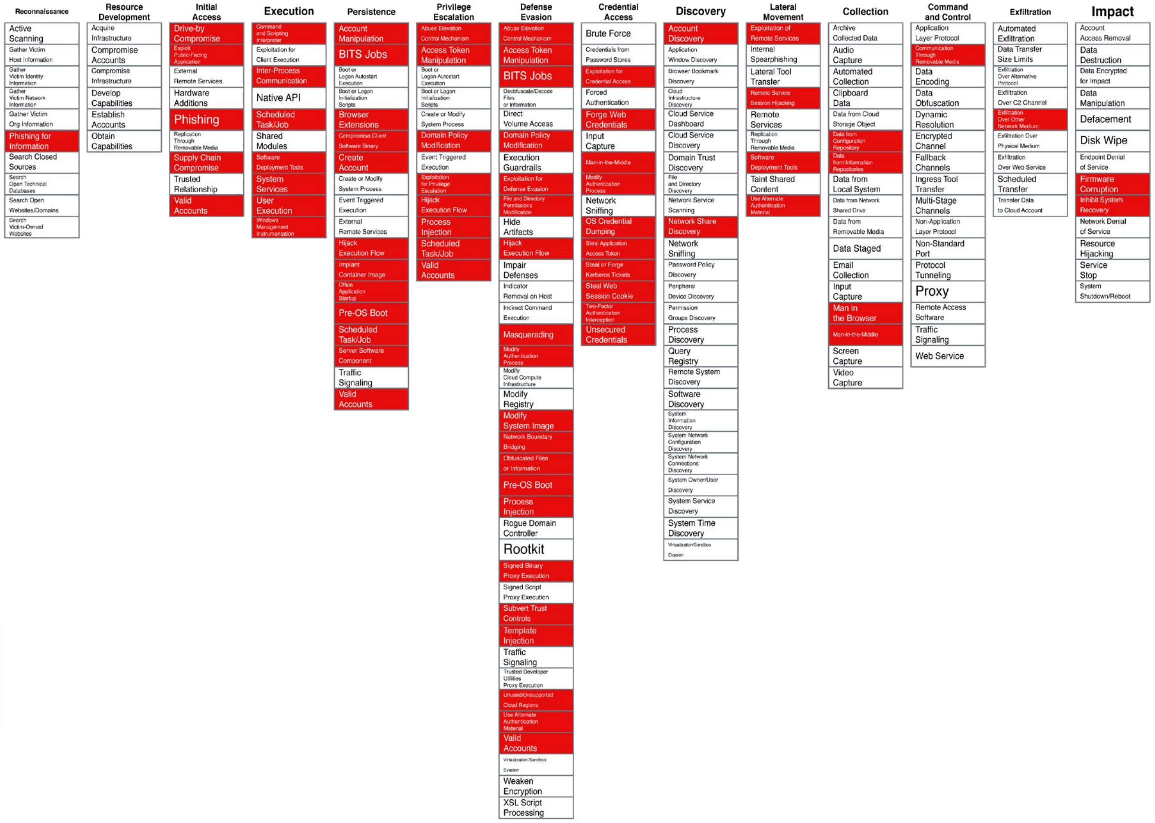
Despite the reality of budget shortfalls and talent shortages, the requirements to secure a business continue to grow. Traditional solutions designed to enhance security, such as EDR, require "eyes on the glass" to triage alerts as soon as they appear. At a fundamental level, this means that better security has historically meant throwing more people at the problem. No wonder 71% of executives surveyed think a cybersecurity talent gap causes them "direct and measurable damage."

That damage will only cut deeper as cyber threats become more ruthless. But the situation isn't hopeless. Lean security teams may not be able to increase their ranks anytime soon or take their attention away from security alerts (many of them false). They can, however, do far more with what they already have. An analysis of the MITRE ATT&CK framework, in fact, shows just how many techniques are prevented through the application of no- or low-cost security tools.

An impressive 34 percent of attack techniques in the MITRE framework are mitigated by taking security actions that require no extra cost. Of the 178 techniques MITRE includes, this means 60 specific threat actor techniques are addressed, substantially reducing attack risk for lean security teams.

60 TECHNIQUES
mitigated with
no-cost actions

MITRE ATT&CK Coverage



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	Acquire Infrastructure	🟥 Drive-by Compromise	🟥 Command and Scripting Interpreter	🟥 Account Manipulation	🟥 Abuse Elevation Control Mechanism	🟥 Abuse Elevation Control Mechanism
Gather Victim Host Information	Compromise Accounts	🟥 Exploit Public-Facing Application	Exploitation for Client Execution	🟥 BITS Jobs	🟥 Access Token Manipulation	🟥 Access Token Manipulation
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	🟥 Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	🟥 BITS Jobs
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information
Gather Victim Org Information	Establish Accounts	🟥 Phishing	🟥 Scheduled Task/Job	🟥 Browser Extensions	Create or Modify System Process	Direct Volume Access
🟥 Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Shared Modules	🟥 Compromise Client Software Binary	🟥 Domain Policy Modification	🟥 Domain Policy Modification
Search Closed Sources		🟥 Supply Chain Compromise	🟥 Software Deployment Tools	🟥 Create Account	Event Triggered Execution	Execution Guardrails
Search Open Technical Databases		Trusted Relationship	🟥 System Services	Create or Modify System Process	🟥 Exploitation for Privilege Escalation	🟥 Exploitation for Defense Evasion
Search Open Websites/Domains		🟥 Valid Accounts	🟥 User Execution	Event Triggered Execution	🟥 Hijack Execution Flow	🟥 File and Directory Permissions Modification
Search Victim-Owned Websites			🟥 Windows Management Instrumentation	External Remote Services	🟥 Process Injection	Hide Artifacts
				🟥 Hijack Execution Flow	🟥 Scheduled Task/Job	🟥 Hijack Execution Flow
				🟥 Implant Container Image	🟥 Valid Accounts	Impair Defenses
				🟥 Office Application Startup		Indicator Removal on Host
				🟥 Pre-OS Boot		Indirect Command Execution
				🟥 Scheduled Task/Job		🟥 Masquerading
				🟥 Server Software Component		🟥 Modify Authentication Process
				Traffic Signaling		Modify Cloud Compute Infrastructure
				🟥 Valid Accounts		Modify Registry
						🟥 Modify System Image
						🟥 Network Boundary Bridging
						🟥 Obfuscated Files or Information
						🟥 Pre-OS Boot
						🟥 Process Injection
						Rogue Domain Controller
						Rootkit
						🟥 Signed Binary Proxy Execution
						Signed Script Proxy Execution
						🟥 Subvert Trust Controls
						🟥 Template Injection
						Traffic Signaling
						Trusted Developer Utilities Proxy Execution
						🟥 Unused/Unsupported Cloud Regions
						🟥 Use Alternate Authentication Material
						🟥 Valid Accounts
						Virtualization/Sandbox Evasion
						Weaken Encryption
						XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Brute Force	🟥 Account Discovery	🟥 Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	🟥 Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
🟥 Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Forced Authentication	Cloud Infrastructure Discovery	🟥 Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
🟥 Forge Web Credentials	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	🟥 Exfiltration Over Other Network Medium	Defacement
Input Capture	Cloud Service Discovery	Replication Through Removable Media	🟥 Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
🟥 Man-in-the-Middle	Domain Trust Discovery	🟥 Software Deployment Tools	🟥 Data from Information Repositories	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
🟥 Modify Authentication Process	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	🟥 Firmware Corruption
Network Sniffing	Network Service Scanning	🟥 Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	🟥 Inhibit System Recovery
🟥 OS Credential Dumping	🟥 Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
🟥 Steal Application Access Token	Network Sniffing		Data Staged	Non-Standard Port		Resource Hijacking
🟥 Steal or Forge Kerberos Tickets	Password Policy Discovery		Email Collection	Protocol Tunneling		Service Stop
🟥 Steal Web Session Cookie	Peripheral Device Discovery		Input Capture	Proxy		System Shutdown/Reboot
🟥 Two-Factor Authentication Interception	Permission Groups Discovery		🟥 Man in the Browser	Remote Access Software		
🟥 Unsecured Credentials	Process Discovery		🟥 Man-in-the-Middle	Traffic Signaling		
	Query Registry		Screen Capture	Web Service		
	Remote System Discovery		Video Capture			
	Software Discovery					
	System Information Discovery					
	System Network Configuration Discovery					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion					

In this whitepaper, we will share five specific strategies that security teams of any size can employ and the coverage they provide. It doesn't take a massive staff or a coterie of specialists to effectively defend against many of today's worst cyber threats. Managed security providers aren't necessary either (though they can still be helpful). With a series of proactive steps, any company can build an effective (or impactful) security posture that looms much larger than the team behind it. Powerful enough, even, to contend with today's worst threats.

1 HOW LOCKING DOWN ADMIN PRIVILEGES OFFERS EXPANSIVE MITRE COVERAGE

The MITRE ATT&CK framework provides a critical roadmap for lean security teams. It meticulously breaks down the tactics and techniques that hackers utilize regardless of what attack they employ. By exposing the pathways that hackers take to reach their final target and the tricks they use along the way, MITRE helps security teams of any size defend their critical systems.

Privilege escalation is one of the tactics the framework highlights, referring to any attempt by hackers to ultimately achieve administrative privileges. Bad actors can use privilege escalation to move vertically through an IT infrastructure and seize greater control or access. This tactic also enables hackers to enter through a weak point and move horizontally to reach other parts of the infrastructure. MITRE identifies dozens of different techniques that hackers may use to escalate privileges. Collectively, these techniques function like a skeleton key that hackers can use to move through locked doors at will and reach whatever target they please.

To put into perspective the importance of privilege escalation, estimates suggest as many as 80% of all attacks utilize this technique in some form. Examples include when hackers jump from a virtual machine into the hypervisor it runs on, seize domain administrator access on a workstation, or root out misconfigurations in public clouds they can use to change settings. In all cases, the barriers meant to keep hackers out prove more porous than expected. But that can (and must) be prevented.

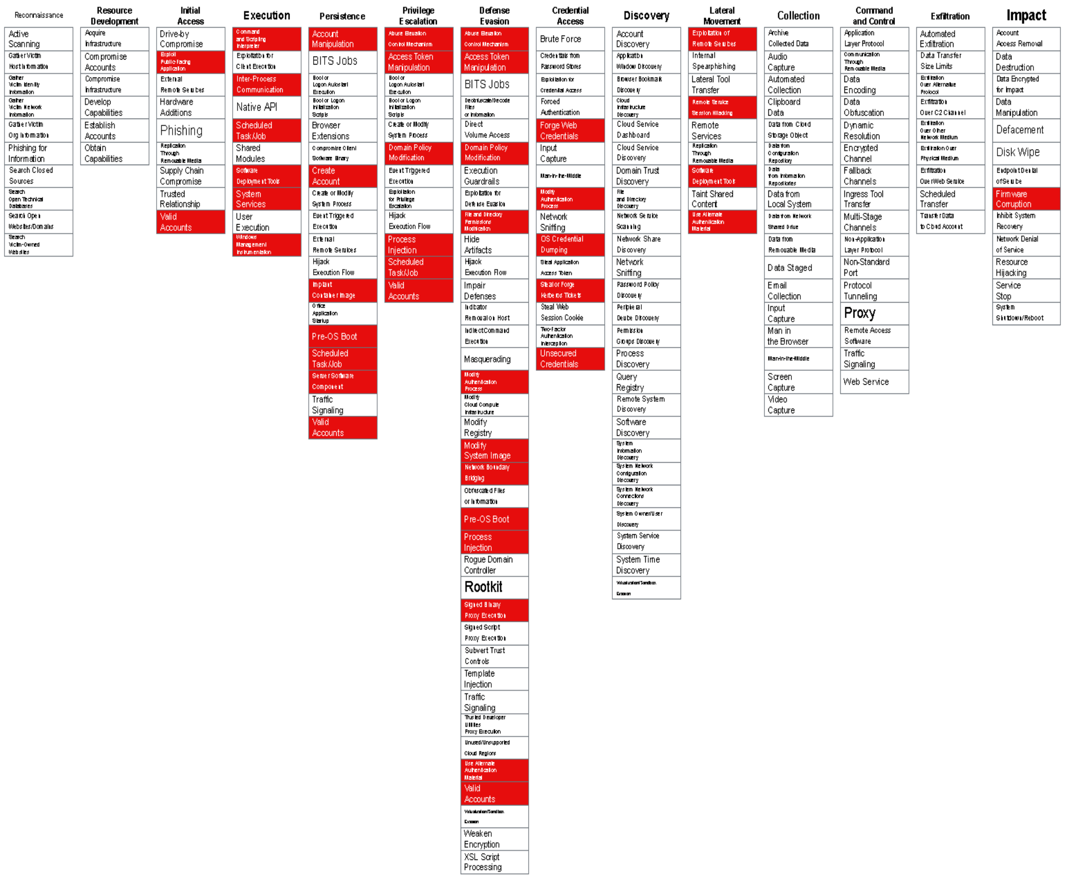
But reduced risk of privilege escalation isn’t the only benefit of careful privileged account management. Using MITRE’s free ATT&CK Navigator, privileged account management can mitigate dozens of techniques across most tactics, including initial access, execution, persistence, and more. The best part about this is that privileged account management is a free action that every company can take right now.

It’s also incredibly effective. Lean security teams can throw roadblocks in front of attacks (up to 80% of them) by carefully managing administrative privileges. This doesn’t take into account that 30 techniques in the MITRE framework are mitigated by properly managing administrative privileges.

30 TECHNIQUES
mitigated by limiting
administrative privileges

The image below shows the coverage gained by managing administrative privileges according to MITRE ATT&CK Navigator.

MITRE ATT&CK Coverage



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

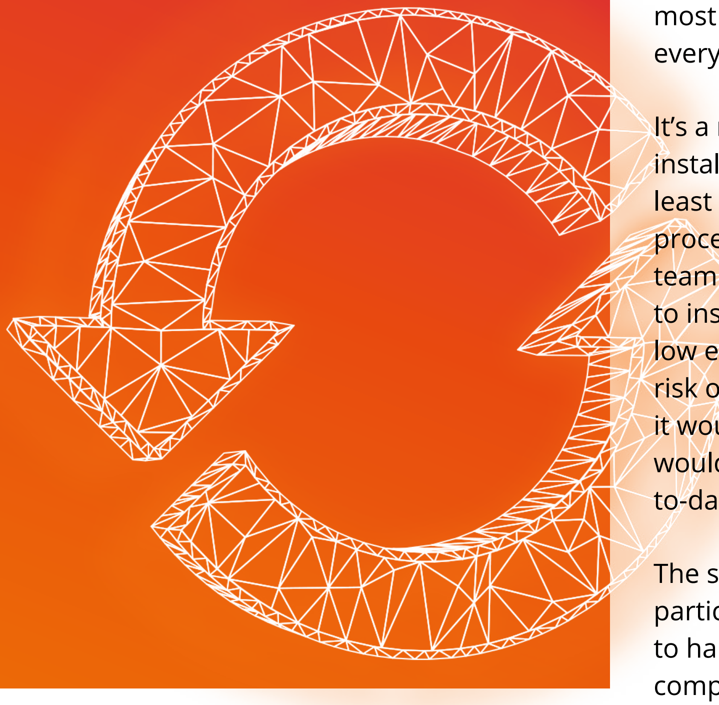
Stripping admin rights away from anyone who doesn't need them means one less privilege for hackers to escalate. Granted, they might find another avenue to exploit – but more likely they will abandon the attack as soon as they encounter an unexpected obstacle and seek out a simpler target instead. Multi-factor authentication can also help prevent privilege escalation, as can an effective employee training/education campaign about how to avoid opening the door for hackers. Above all, though, lean security teams need a systematic approach.

Managing administrative privileges across all of IT can be complex for security teams with a small staff. Things get even more complicated when locking down administrative privileges has the unintended consequence of interrupting operations; cybersecurity can't compromise business continuity.

For lean security teams to juggle all these competing forces, it helps to map the IT infrastructure. Identify all assets involved, determine how they affect business continuity, and investigate what risks they create in terms of privilege escalation. Having a clear understanding of how users and systems impact the risk of an organization will help prioritize prevention controls and remediation efforts. Said differently, a good map makes it clear where to put the biggest defenses in place so that lean security teams can make the most of the resources they have available.

2 INCREASE THE EFFICACY OF VULNERABILITY RESOLUTION WITH VIRTUAL PATCHING

14 TECHNIQUES mitigated by regularly patching software



A study from 2019 found that in 60% of the attacks examined, hackers took advantage of a vulnerability that could have been patched... but wasn't. The 2017 Equifax attack started this way, along with countless others over the years. That won't stop anytime soon because exploiting unpatched vulnerabilities is one of the easiest yet most effective exploits – an unlocked door that everyone knows about.

It's a race against time to lock those doors by installing patches, but lean security teams are the least equipped to sprint. A systematic patching process involves extensive input from the security team. That helps explain why the average time to install patches ranges from 60 days on the low end to 150 days on the high end. Given the risk of infection from an unpatched vulnerability, it would seem that more IT and security teams would focus on ensuring all their software is up-to-date. The numbers suggest otherwise.

The same 2019 study showed that 69% of participants planned to hire at least five people to handle patching at a cost of $650,000 to each company. But many companies can't afford that expense, let alone find that much available talent. Those are often the ones taking close to four months to get patches installed – making them low-hanging fruit in the eyes of hackers eager to exploit unpatched vulnerabilities.

Too often, security teams spend their time managing, configuring, and dealing with alerts from expensive detection tools. The irony is that if the time was spent on maintaining a proper patching regimen, they could prevent the same attacks that those tools are designed to detect. As the MITRE ATT&CK Navigator shows (next page), applying software updates can address several possible attack vectors. In total, 14 techniques are mitigiated by regularly patching software.

Some will rely on staff for patching, but lean security teams have another option: virtual patching. Unlike traditional patching, which makes changes to vulnerable code, virtual patches protect around the code. They implement various rules designed to deflect attacks and shield vulnerabilities, which buys the security team some time until it can implement a traditional patch. Compared to emergency patching, which can be highly disruptive when it means suddenly suspending operations, the virtual alternative offers superior speed, flexibility, and cost-effectiveness.

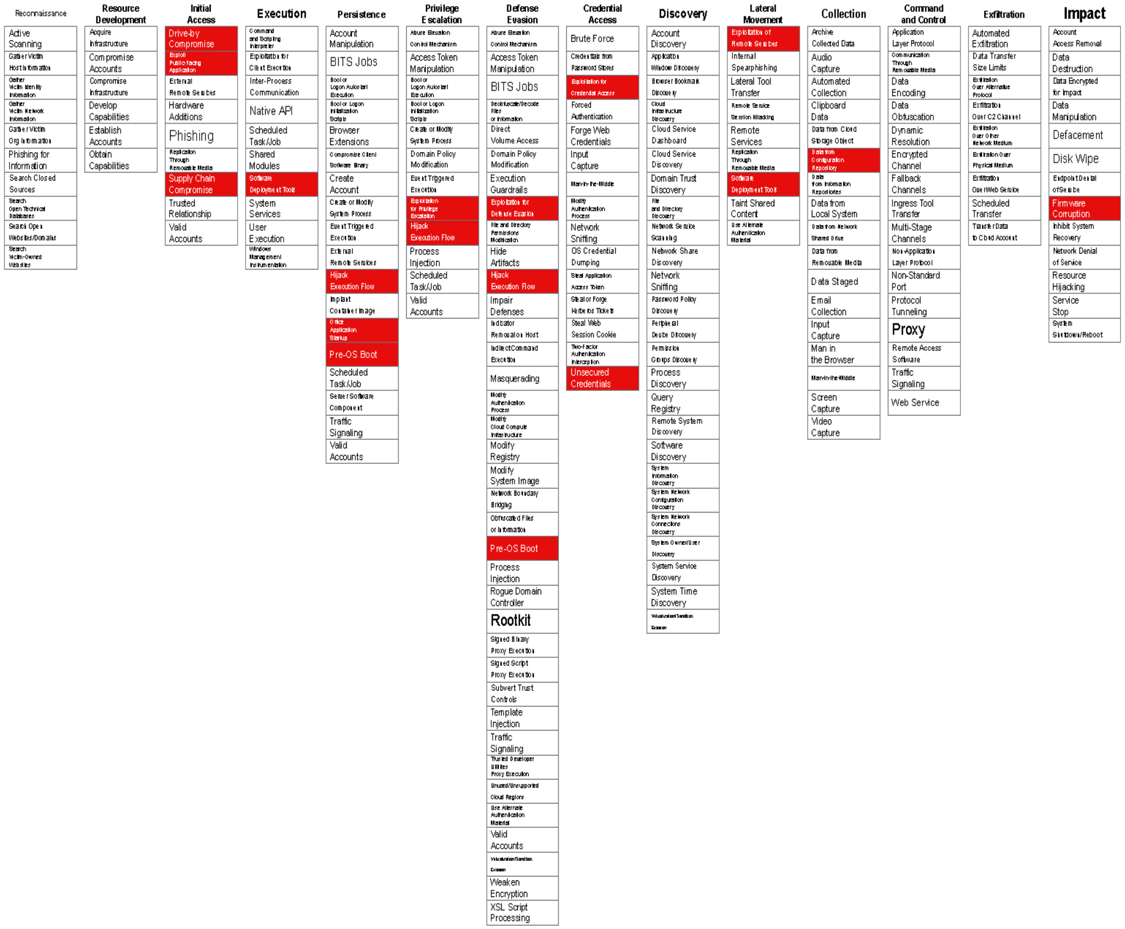
There are numerous ways to apply virtual patches. Some solutions compare network packets against a list of known vulnerabilities or rely on detection paired with vulnerability scanning. In both cases, these options can't recognize (or stop) zero-days that haven't been updated into the system yet. Worse, they can't stop threats that have gone months or years without being discovered. These virtual patches shrink the security gap without sealing it all the way.

Morphisec Guard takes a different approach to virtual patching – one that's ideal for lean security teams. Instead of building rules around an unpatched endpoint, Morphisec Guard alters the attack pathway and obscures the final target: the application memory. A vulnerability may remain unpatched or even unrecognized. Neither matters, though, because even if an attack (new, old, or otherwise) gains entry, it gets lost on the way to its intended destination. Most virtual patches build a bunker around vulnerabilities; Morphisec Guard applies evasive maneuvers.

In the process, Morphisec Guard gives lean security teams two things: time and confidence. Time to patch things when the resources allow instead of under emergency conditions. And confidence that unpatched vulnerabilities, whether known or not, won't create unexpected problems. To put it differently, patching runs according to the security team's schedule instead of the attacker's agenda.

> Too often, security teams spend their time managing, configuring, and dealing with alerts from expensive detection tools

MITRE ATT&CK Coverage



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

3 CAREFULLY EXAMINE SPEND TO ELIMINATE REDUNDANCIES AND MAXIMIZE VALUE

Cybersecurity spending (and staffing) varies widely depending on a company's size, industry, and digital footprint. It's unclear how much the average security team spends and on what. But that's fine. Benchmarking one team against another matters less than scrutinizing every dollar of spending within a specific budget.

Since lean security teams have tighter budgets, both in terms of size and scalability, each investment needs to count. Wasted spending doesn't just result in unnecessary or inadequate protection—it also diverts money away from tools and solutions that could upgrade security. In many cases, lean security teams don't need money to buy more software. They just need to make better use of their existing budget by swapping in cost-free alternatives where possible, eliminating reiterative or ineffective solutions, and investing in what works in areas of remaining risk.

Start by taking a hard look at every line item in the security budget. Is every cost justifiable? Is any cost ambiguous? Excluding items in the budget for compliance reasons, any uncertain spending should be singled out for further review. As part of that review, try to quantify the risk reduction each solution provides. Does it outweigh the cost? If the value of any line item is underwhelming or unclear compared to a cost-free alternative, then it's not an asset.

Similarly, lean security teams should explore opportunities to consolidate or integrate existing solutions rather than adding niche products to an increasingly atomized security stack. In many cases, solutions abound because each one checks a specific compliance box—e.g., for app control or URL filtering. Many of these solutions are now redundant thanks to OS-native security tools and other solutions with built-in capabilities that check more boxes with fewer products.

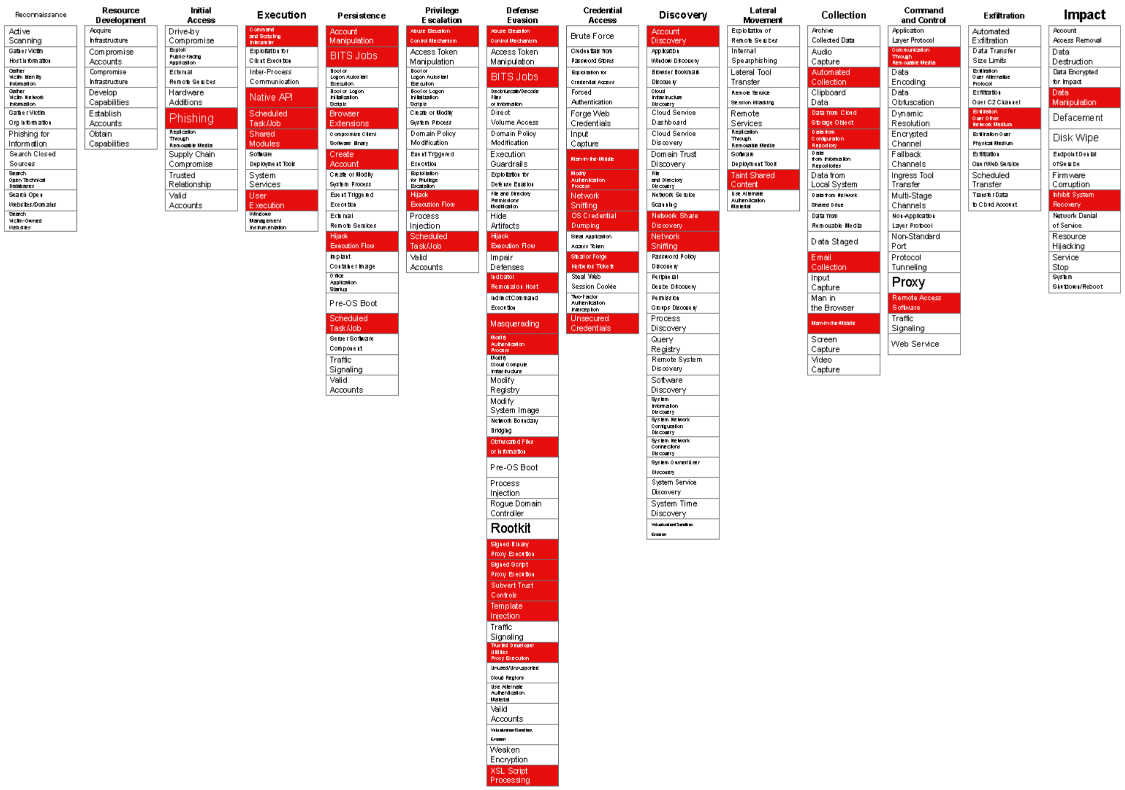
26 TECHNIQUES mitigated by using OS controls

As the budget review continues, focus on the indirect and hidden costs of the tools currently in place or under consideration. They can be substantial. Those costs include deployment, management and operation (especially with EDR), decline in IT performance, and more. For new solutions, evaluate these criteria by asking for a demonstration. If it takes an extensive setup, operating it won't be much easier. Asking other users about their experience can also be a valuable source of first-hand information. SMBs would do well to spend time looking on SpiceWorks forums, and Reddit is a goldmine of community feedback. You can even read reviews at places such as Gartner Peer Insights or IT Central Station.

Don't overlook the obvious, either. Most companies run on Windows, which now comes with a robust suite of OS-native security tools: antivirus, device controls, personal firewall, and disk encryption. Lean security teams don't have to pay for these free tools, and testing agencies have found that free tools like Microsoft Defender are as good as or better than third-party solutions. Making better use of a security budget isn't hard when free, high-quality replacement tools already exist within the physical and virtual walls of the organization. The ATT&CK Navigator shows the benefit of using built-in systems like these to protect your organization, with 26 techniques mitigated through using OS-native solutions.

After moving to free, built-in security tools, the next step should be to prioritize visibility and control. One of the biggest barriers to adoption for OS-native tools like Microsoft Defender AV is that they often don't provide enterprise-level dashboards for centralized administration. Solutions like our own Morphisec Guard, which is tightly interwoven into the Microsoft Windows ecosystem, enhance that visibility and control by adding an enterprise-level management dashboard that allows you deeper insight into Defender events. Additionally, a tool like Morphisec Guard often adds additional protection against evasive malware. The result: cyber risk plummets just as fast as the amount of work required of the security team.

MITRE ATT&CK Coverage



Reconnaissance
- Active Scanning
- Gather Victim Host Information
- Gather Victim Identity Information
- Gather Victim Network Information
- Gather Victim Org Information
- Phishing for Information
- Search Closed Sources
- Search Open Technical Databases
- Search Open Websites/Domains
- Search Victim-Owned Websites

Resource Development
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Develop Capabilities
- Establish Accounts
- Obtain Capabilities

Initial Access
- Drive-by Compromise
- Exploit Public Facing Application
- External Remote Services
- Hardware Additions
- 🟥 Phishing
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts

Execution
- 🟥 Command and Scripting Interpreter
- Exploitation for Client Execution
- Inter-Process Communication
- 🟥 Native API
- 🟥 Scheduled Task/Job
- 🟥 Shared Modules
- Software Deployment Tools
- System Services
- 🟥 User Execution
- Windows Management Instrumentation

Persistence
- 🟥 Account Manipulation
- 🟥 BITS Jobs
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- 🟥 Browser Extensions
- Compromise Client Software Binary
- 🟥 Create Account
- Create or Modify System Process
- Event Triggered Execution
- External Remote Services
- 🟥 Hijack Execution Flow
- Implant Container Image
- Office Application Startup
- Pre-OS Boot
- 🟥 Scheduled Task/Job
- Server Software Component
- Traffic Signaling
- Valid Accounts

Privilege Escalation
- 🟥 Abuse Elevation Control Mechanism
- Access Token Manipulation
- Boot or Logon Autostart Execution
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Domain Policy Modification
- Event Triggered Execution
- Exploitation for Privilege Escalation
- 🟥 Hijack Execution Flow
- Process Injection
- 🟥 Scheduled Task/Job
- Valid Accounts

Defense Evasion
- 🟥 Abuse Elevation Control Mechanism
- Access Token Manipulation
- 🟥 BITS Jobs
- Deobfuscate/Decode Files or Information
- Direct Volume Access
- Domain Policy Modification
- Execution Guardrails
- Exploitation for Defense Evasion
- File and Directory Permissions Modification
- Hide Artifacts
- 🟥 Hijack Execution Flow
- Impair Defenses
- 🟥 Indicator Removal on Host
- Indirect Command Execution
- 🟥 Masquerading
- 🟥 Modify Authentication Process
- Modify Cloud Compute Infrastructure
- Modify Registry
- Modify System Image
- Network Boundary Bridging
- 🟥 Obfuscated Files or Information
- Pre-OS Boot
- Process Injection
- Rogue Domain Controller
- Rootkit
- 🟥 Signed Binary Proxy Execution
- 🟥 Signed Script Proxy Execution
- 🟥 Subvert Trust Controls
- 🟥 Template Injection
- Traffic Signaling
- 🟥 Trusted Developer Utilities Proxy Execution
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Valid Accounts
- Virtualization/Sandbox Evasion
- Weaken Encryption
- 🟥 XSL Script Processing

Credential Access
- Brute Force
- Credentials from Password Stores
- Exploitation for Credential Access
- Forced Authentication
- Forge Web Credentials
- Input Capture
- 🟥 Man-in-the-Middle
- 🟥 Modify Authentication Process
- 🟥 Network Sniffing
- 🟥 OS Credential Dumping
- Steal Application Access Token
- 🟥 Steal or Forge Kerberos Tickets
- Steal Web Session Cookie
- Two-Factor Authentication Interception
- 🟥 Unsecured Credentials

Discovery
- 🟥 Account Discovery
- Application Window Discovery
- Browser Bookmark Discovery
- Cloud Infrastructure Discovery
- Cloud Service Dashboard
- Cloud Service Discovery
- Domain Trust Discovery
- File and Directory Discovery
- Network Service Scanning
- 🟥 Network Share Discovery
- 🟥 Network Sniffing
- Password Policy Discovery
- Peripheral Device Discovery
- Permission Groups Discovery
- Process Discovery
- Query Registry
- Remote System Discovery
- Software Discovery
- System Information Discovery
- System Network Configuration Discovery
- System Network Connections Discovery
- System Owner/User Discovery
- System Service Discovery
- System Time Discovery
- Virtualization/Sandbox Evasion

Lateral Movement
- Exploitation of Remote Services
- Internal Spearphishing
- Lateral Tool Transfer
- Remote Service Session Hijacking
- Remote Services
- Replication Through Removable Media
- Software Deployment Tools
- 🟥 Taint Shared Content
- Use Alternate Authentication Material

Collection
- Archive Collected Data
- Audio Capture
- 🟥 Automated Collection
- Clipboard Data
- 🟥 Data from Cloud Storage Object
- 🟥 Data from Configuration Repository
- Data from Information Repositories
- Data from Local System
- Data from Network Shared Drive
- Data from Removable Media
- Data Staged
- 🟥 Email Collection
- Input Capture
- Man in the Browser
- 🟥 Man-in-the-Middle
- Screen Capture
- Video Capture

Command and Control
- Application Layer Protocol
- 🟥 Communication Through Removable Media
- Data Encoding
- Data Obfuscation
- Dynamic Resolution
- Encrypted Channel
- Fallback Channels
- Ingress Tool Transfer
- Multi-Stage Channels
- Non-Application Layer Protocol
- Non-Standard Port
- Protocol Tunneling
- Proxy
- 🟥 Remote Access Software
- Traffic Signaling
- Web Service

Exfiltration
- Automated Exfiltration
- Data Transfer Size Limits
- Exfiltration Over Alternative Protocol
- Exfiltration Over C2 Channel
- 🟥 Exfiltration Over Other Network Medium
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Scheduled Transfer
- Transfer Data to Cloud Account

Impact
- Account Access Removal
- Data Destruction
- Data Encrypted for Impact
- 🟥 Data Manipulation
- Defacement
- Disk Wipe
- Endpoint Denial of Service
- Firmware Corruption
- 🟥 Inhibit System Recovery
- Network Denial of Service
- Resource Hijacking
- Service Stop
- System Shutdown/Reboot

4 MAKE SECURITY AWARENESS MORE THAN AN ANNUAL TRAINING

14 TECHNIQUES
mitigated through
regular user training

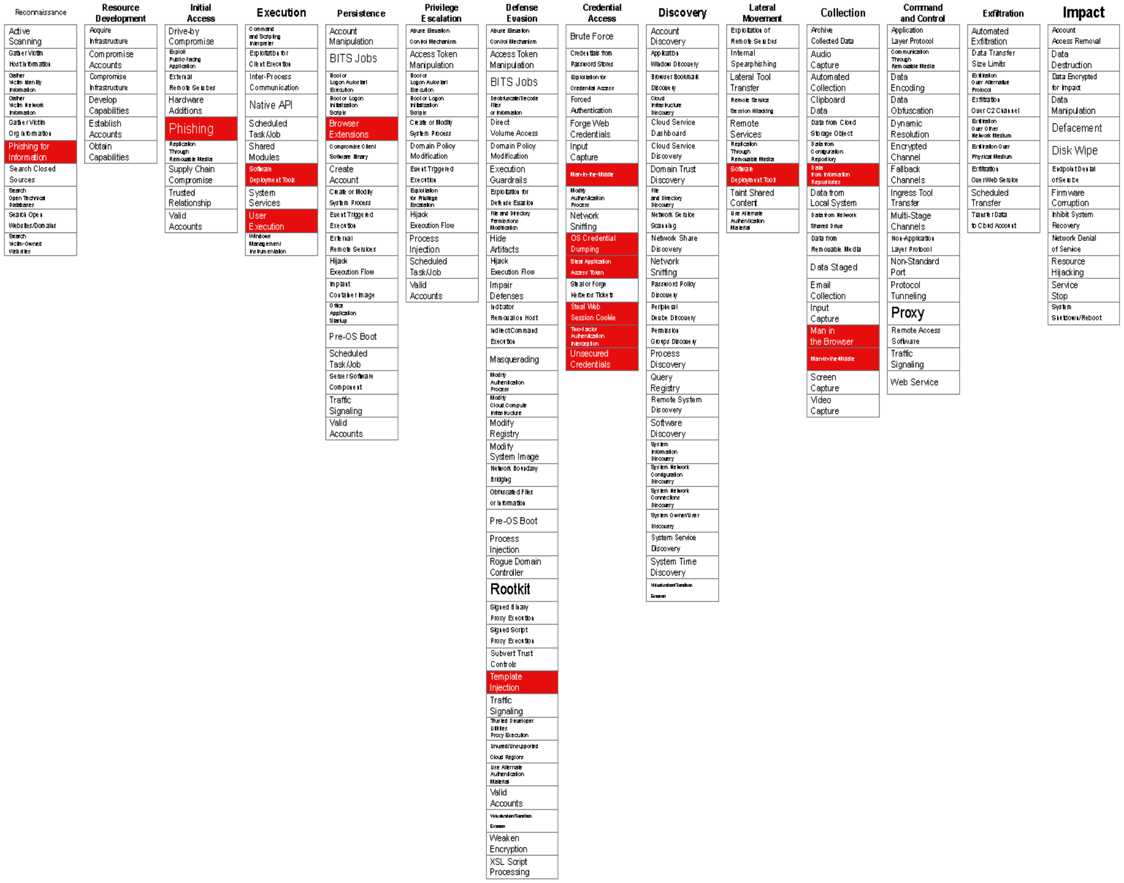
Effective cybersecurity always comes down to your people. The people working for your company who need extensive training to see and stop the cyber attacks targeted at them. And the people on your security team who carry the heavy burden of protecting everyone and everything. If these people break down, so does your cybersecurity.

Supporting employees on the front lines of cybersecurity is both an imperative and a sound investment. If an ounce of prevention is worth a pound of cure, investments in people cost far less than what they return; one study showed that even the least effective security training programs result in a seven-fold ROI. Another study linked these programs with a 70% reduction in cyber risk. Well-trained employees make attacks less likely to succeed and less destructive when they do, just as under-prepared employees do the opposite. Any investment in cybersecurity training is money well spent. Fully 14 threat actor techniques are mitigated with security awareness training.

Supporting employees on the front lines of cybersecurity is both an imperative and a sound investment

How to approach security awareness training is a big enough subject for another whitepaper. That being said, there are two key components: persistence and variety. Employees need to receive training during onboarding and regularly afterwards to keep governance top-of-mind and continuous. Just as importantly, they need diverse training experiences to keep it from becoming a stale exercise with diminishing returns.

MITRE ATT&CK Coverage



Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion
Active Scanning	Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism
Gather Victim Host Information	Compromise Accounts	Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation	Access Token Manipulation
Gather Victim Identity Information	Compromise Infrastructure	External Remote Services	Inter-Process Communication	Boot or Logon Autostart Execution	Boot or Logon Autostart Execution	BITS Jobs
Gather Victim Network Information	Develop Capabilities	Hardware Additions	Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information
Gather Victim Org Information	Establish Accounts	**Phishing**	Scheduled Task/Job	**Browser Extensions**	Create or Modify System Process	Direct Volume Access
Phishing for Information	Obtain Capabilities	Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification	Domain Policy Modification
Search Closed Sources		Supply Chain Compromise	**Software Deployment Tools**	Create Account	Event Triggered Execution	Execution Guardrails
Search Open Technical Databases		Trusted Relationship	System Services	Create or Modify System Process	Exploitation for Privilege Escalation	Exploitation for Defense Evasion
Search Open Websites/Domains		Valid Accounts	**User Execution**	Event Triggered Execution	Hijack Execution Flow	File and Directory Permissions Modification
Search Victim-Owned Websites			Windows Management Instrumentation	External Remote Services	Process Injection	Hide Artifacts
				Hijack Execution Flow	Scheduled Task/Job	Hijack Execution Flow
				Implant Container Image	Valid Accounts	Impair Defenses
				Office Application Startup		Indicator Removal on Host
				Pre-OS Boot		Indirect Command Execution
				Scheduled Task/Job		Masquerading
				Server Software Component		Modify Authentication Process
				Traffic Signaling		Modify Cloud Compute Infrastructure
				Valid Accounts		Modify Registry
						Modify System Image
						Network Boundary Bridging
						Obfuscated Files or Information
						Pre-OS Boot
						Process Injection
						Rogue Domain Controller
						Rootkit
						Signed Binary Proxy Execution
						Signed Script Proxy Execution
						Subvert Trust Controls
						Template Injection
						Traffic Signaling
						Trusted Developer Utilities Proxy Execution
						Unused/Unsupported Cloud Regions
						Use Alternate Authentication Material
						Valid Accounts
						Virtualization/Sandbox Evasion
						Weaken Encryption
						XSL Script Processing

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Brute Force	Account Discovery	Exploitation of Remote Services	Archive Collected Data	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Credentials from Password Stores	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Forced Authentication	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Clipboard Data	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Forge Web Credentials	Cloud Service Dashboard	Remote Services	Data from Cloud Storage Object	Dynamic Resolution	Exfiltration Over Other Network Medium	Defacement
Input Capture	Cloud Service Discovery	Replication Through Removable Media	Data from Configuration Repository	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Man-in-the-Middle	Domain Trust Discovery	**Software Deployment Tools**	**Data from Information Repositories**	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Modify Authentication Process	File and Directory Discovery	Taint Shared Content	Data from Local System	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Network Sniffing	Network Service Scanning	Use Alternate Authentication Material	Data from Network Shared Drive	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
OS Credential Dumping	Network Share Discovery		Data from Removable Media	Non-Application Layer Protocol		Network Denial of Service
Steal Application Access Token	Network Sniffing		Data Staged	Non-Standard Port		Resource Hijacking
Steal or Forge Kerberos Tickets	Password Policy Discovery		Email Collection	Protocol Tunneling		Service Stop
Steal Web Session Cookie	Peripheral Device Discovery		Input Capture	Proxy		System Shutdown/Reboot
Two-Factor Authentication Interception	Permission Groups Discovery		**Man in the Browser**	Remote Access Software		
Unsecured Credentials	Process Discovery		**Man-in-the-Middle**	Traffic Signaling		
	Query Registry		Screen Capture	Web Service		
	Remote System Discovery		Video Capture			
	Software Discovery					
	System Information Discovery					
	System Network Configuration Discovery					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion					

Above you can see the impact of security awareness training in the MITRE ATT&CK Navigator.

Members of the lean security team also need regular check-ins. Since this team strives to use resources efficiently, especially human resources, investigate how much time people spend on what tasks. The answers may be surprising. Part of being a lean team is making sure staff stay focused on the strategic tasks that collapse risk, not learning a complicated new tool or responding to endless false alarms coming from the EDR. Just because the team seems busy doesn't mean they're working effectively. Too often, low-value tasks consume time and attention because that's what they require: eyes on the screen and hands on the keyboard.

Whether or not labor-intensive solutions are worth keeping should be investigated in the previous step. If they put too much strain on the security team (without delivering adequate value), make sure the replacement doesn't do the same. Introduce as much proven automation and self-prevention hardening as possible while simultaneously evaluating solutions based on the amount of manual input required. Introducing more noise in the form of alerts and alarms doesn't help. Rather, it creates extra stress and wastes important resources, namely time and staff.

5 DEPLOY A ZERO TRUST DEFENSIVE STRATEGY ON THE ENDPOINT (TOO)

Years of cybersecurity failures have taught security teams to trust no one. In 2020, 72% of organizations surveyed planned to either assess their capacity for zero trust or implement this capability in some form. Zero trust shrinks the attack surface to thwart an impressive number of attacks – making it ideal for lean security teams who need to use their resources preventing attacks rather than mitigating the damage, which involves a much larger lift.

A comprehensive zero trust defensive strategy integrates the most important layers of defense: identity, network, and endpoint at run-time. By requiring traffic at all of these points to prove their credentials, zero-trust exposes attacks earlier in the attack pathway and denies entry. The appeal of this approach, in addition to its effectiveness, is how little it requires from the security team. They will need to review an incident response. Otherwise, though, careful access controls do the hard work of keeping hackers out. By implementing a zero trust defensive strategy, lean security teams add the additional hardening they need to reduce their breach risk.

Some form of zero trust may already be in place in terms of identity and access management, as well as network security. The missing piece is to apply zero trust to endpoints. More and more, hackers use endpoints as their access point, in no small part because endpoints have yet to be fortified with zero trust. The sudden shift to remote work because of COVID-19 didn't help the situation either. Massive numbers of new, insecure endpoints became a prime target for hackers.

Zero trust on the endpoint is the most important, yet overlooked, component of a zero trust strategy. Attacks on the endpoint don't have to reveal themselves until they're already loaded in memory and performing the malicious action. Supply chain attacks are a perfect example. A trusted user would bring a trusted process into memory, and only once it's past the "zero trust zones" of identity and network zero trust would the attack proceed. As a result, not applying zero trust on the endpoint creates the risk of an attack progressing once it's able to sneak past network security and identity and access management solutions.

Lean security teams will need to address these endpoint risks, especially as remote work has become part of the new normal. Zero trust on the endpoint does that while "closing the loop" in terms of access. Anyone who wants inside must get permission first. Granted, zero trust can't keep out every single threat. But it can stop enough of them to significantly lighten the load on a security team. And when teams do need to address an attack, they have ample resources on hand to move fast and fight hard.

> In 2020, 72% of organizations surveyed planned to either assess their capacity for zero trust or implement this capability in some form

RISK REDUCTION DOESN'T MEAN COMPROMISING BETWEEN SPEND AND EFFECTIVENESS

The best security teams aren't defined by their size. The amount they spend or the tools they use don't distinguish the elite either. For those that take cybersecurity seriously, only one metric matters: risk reduction. Taking the no-cost (or very low-cost) actions described in this whitepaper can substantially reduce the attack surface for a lean security team, leading to a more secure organization overall.

Effective teams stop more attacks more of the time regardless of whether they're lean or have all the budget, tools and personnel they could ever need. Cybersecurity isn't an arms race; having the most guns or the biggest bombs doesn't equate to the strongest defense. Rather, it's about using the resources at hand to outmatch whatever threat looms on the horizon. Some lean teams excel at this, just as some large teams fail at it.

The point we want to leave you with is that lean security teams aren't at a disadvantage. Talent shortages, budget shortfalls, and hyper-aggressive hackers don't mean the certain failure of small teams. Likewise, it doesn't take a massive influx of money, expertise, or other resources to shore up cybersecurity. Small teams have most of the assets they need already.

All that's missing is a change in mindset: Lean doesn't mean running at a bare minimum; it means running with optimal efficiency.

60 TECHNIQUES mitigated with no-cost actions

ABOUT MORPHISEC

FUNDAMENTALLY ALTERING THE CYBERSECURITY LANDSCAPE

Morphisec is transforming endpoint security with our pioneering Moving Target Defense. Our solutions deliver operationally simple, proactive prevention unbound by the limits of detection and prediction. We protect businesses around the globe from the most dangerous and sophisticated cyberattacks immediately, efficiently and absolutely.