HUNTRESS

What's Now & Next:
How Huntress is Advancing to Stay Ahead of Adversaries

What We'll Cover

NEED

The trends and threat landscape impacting organizations

NOW

Our platform and how it has advanced in the age of AI

NEXT

New products built to shrink the endpoint & identity attack surface

What We'll Cover

NEED

The trends and threat landscape impacting organizations

NOW

Our platform and how it has advanced in the age of AI

NEXT

New products built to shrink the endpoint & identity attack surface

HACKERS DON'T JUST TARGET THE FORTUNE 500

They prey on the vulnerable

HUNTRESS | 2026 CYBER THREAT REPORT

The TL;DR

The business of cybercrime is booming, and it's never been more efficient.

In 2025, we analyzed hacker activity across more than 4.6 million endpoints and 9.4 million identities. One theme was clear: cybercrime is running better than most businesses. What was once a chaotic patchwork of isolated attacks and disorganized groups has transformed into a sophisticated, global supply chain. Cybercriminals are exploiting the same tools we depend on every day, and they're competing against your business with a standardized playbook.

Our 24/7 human-led, AI-assisted Security Operations Center (SOC) shuts down these threats, giving us a front-row seat to the shifting threat landscape. In the Huntress 2026 Cyber Threat Report, we break down how cybercriminals are abusing legitimate tools, launching complex identity attacks, and pulling off clever social engineering scams to bypass traditional defenses and avoid noisy exploits.

To scale your business securely in the year ahead, here's the TL;DR on the most critical threats.

Industry

Attacks against the manufacturing industry were up by 88%

Malware

ClickFix accounted for 53.2% of all malware loader activity

Identity

18.9% of all identity-based threats were linked to adversary-in-the-middle (AiTM) attacks (a tactic that bypasses MFA controls)

Phishing

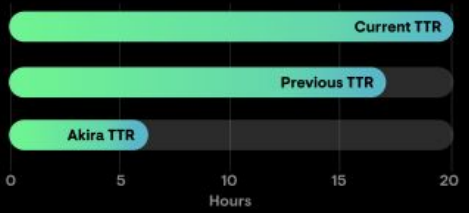
57.7% of phishing attacks used malicious PDF attachments

Ransomware

Over 51% of all ransomware incidents were linked to Akira, Medusa, Qilin, and Ransomhub

Average time-to-ransom (TTR) jumped from 17 to 20 hours because attackers:

- Focused more on extortion and data theft
- Prioritized staying hidden over moving fast
- Took their time between initial access and the next steps in the attack path



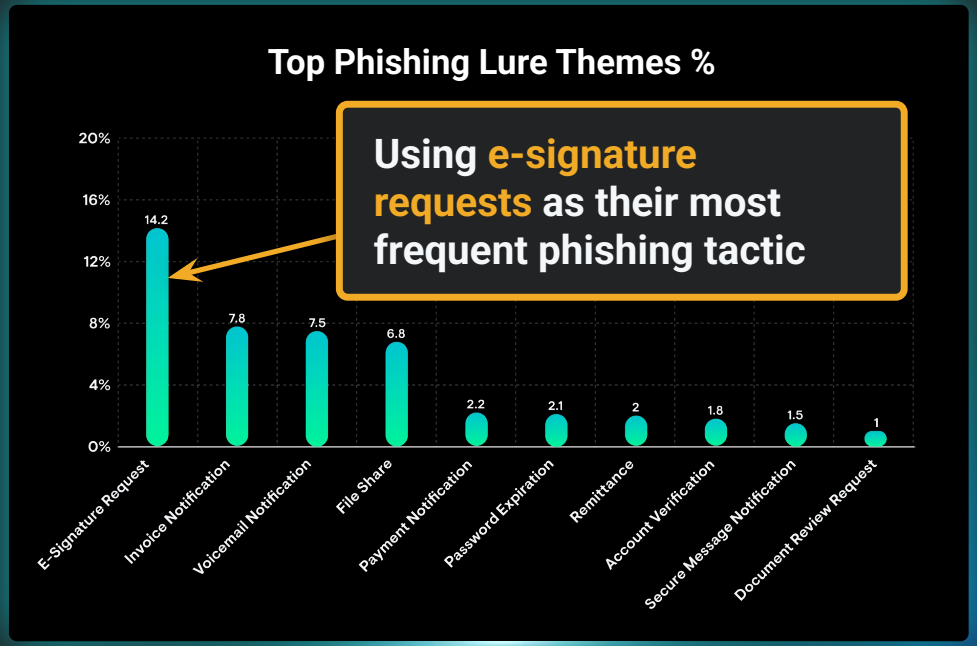
Akira, the top ransomware group, had a TTR of 6.58 hours and was linked to 22% of all ransomware incidents

NOT JUST ONE STORY. IT'S HAPPENING AT SCALE.

Users are up against constant threats, and hackers are innovating *fast*.

AI is Accelerating Attacks

They aren't just hacking endpoints — they're **hacking people**

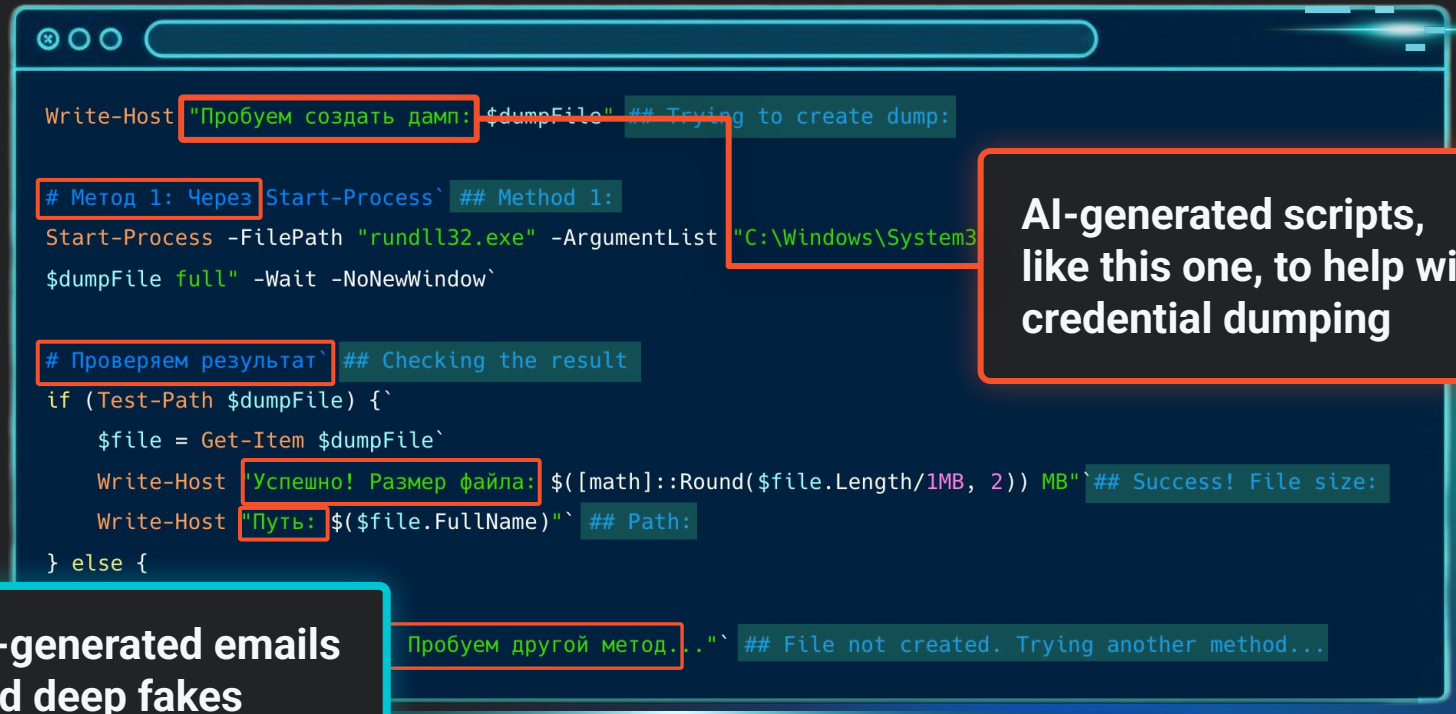


Real-world patterns we see:

- AI-generated scripts that automate credential dumping and other tradecraft
- AI-polished phishing campaigns; e-signature lures and business-lookalike emails dominate
- Malware loaders, like ClickFix, accounting for ~50%+ of observed loader activity in 2025

Attackers Also Use AI

to work smarter and faster



AI-generated scripts, like this one, to help with credential dumping

AI-generated emails and deep fakes

HUNTRESS

Huntress Exists Because Companies of ALL Sizes Deserve a Fighting Chance

The Problem

Hackers don't just target the Fortune 500.

They prey on the vulnerable.

The Reality

Elite security was a luxury most couldn't afford.

We're here to change that.

The Promise

Resilience, peace of mind, and a level playing field.

Enterprise-grade security for ALL businesses.

What We'll Cover

NEED

The trends and threat landscape impacting organizations

NOW

Our platform and how it has advanced in the age of AI

NEXT

New products built to shrink the endpoint & identity attack surface

HUNTRESS | Agentic Security Platform

Built to unleash end-to-end protection in the age of AI

Agentic platform fabric

Endpoints | Identities
Human risk | Visibility

All Managed Together

AI-centric SOC

Experts using AI to move faster

AI is the Iron Man suit that lets us outpace attackers

Enterprise-Grade Defense

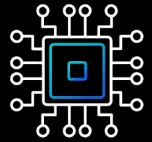
Keep our communities running

Protection without enterprise-grade overhead

Meet Athena

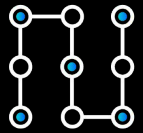
How our agentic investigation system works

Works with Huntress SOC analysts to investigate every threat.



Built on an orchestration engine with specialized AI analysts.

Pulls telemetry across the platform for a picture of the incident.



Uses defined playbooks and guardrails to identify malice.

Writes incident reports and takes action when high confidence is met.

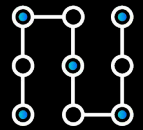
Indeterminate signals go to human analysts review.

Athena Helps Us Shut Down Growing AI-Powered Threats

Instant Pickup

High-priority signals claimed as they appear. Zero wait time.

→ **Faster time to assign**



Zero Shortcuts

Every playbook step runs, every time. No intuition shortcuts.

→ **Improved report quality**

Deterministic Reliability

AI-reasoning + hard-coded guardrails for high accuracy.

→ **Lower rejection rates**

Human Analysts Lead Athena

Human SOC Analysts

Aren't always in the decision-making loop, but are always in the lead

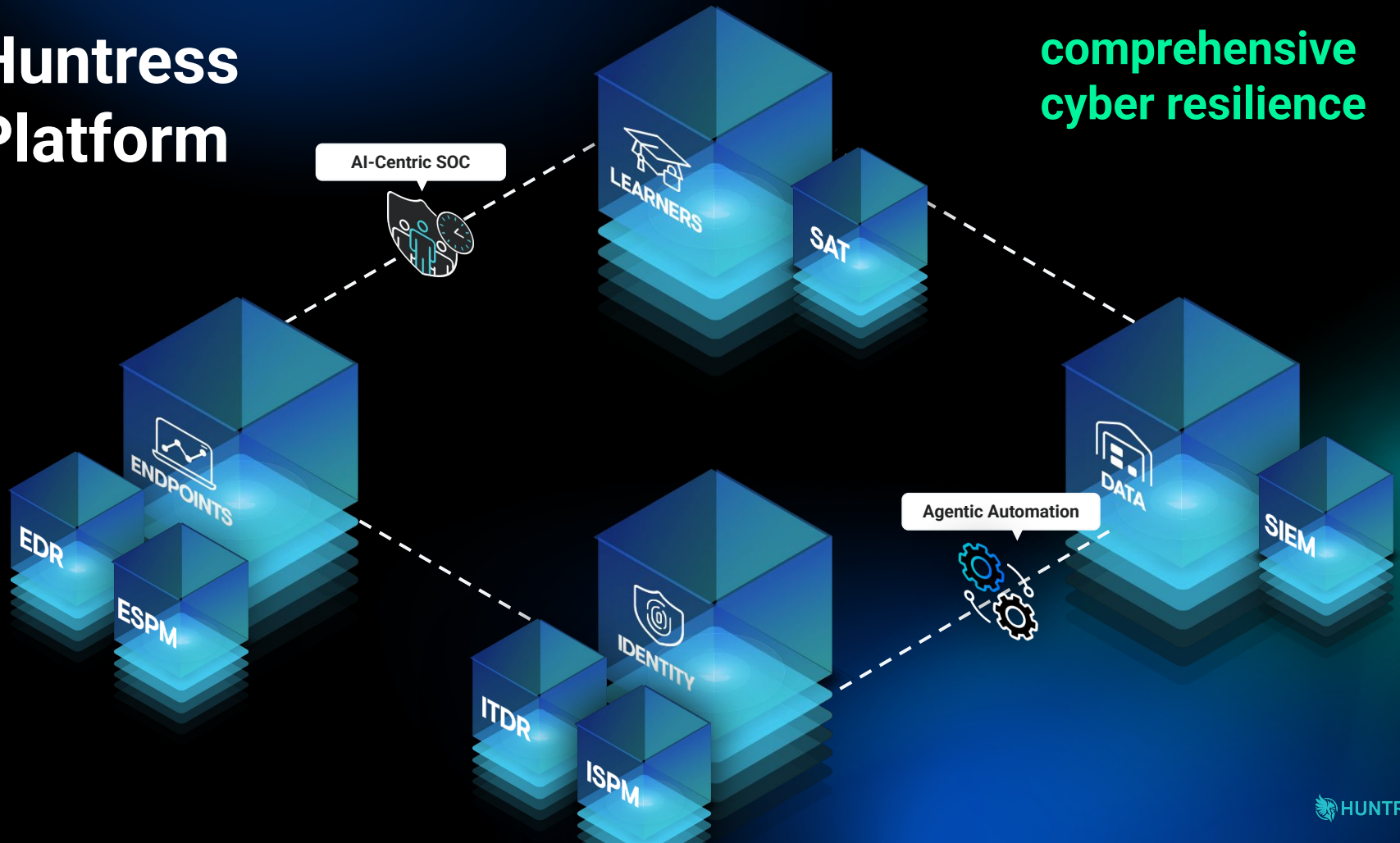
Huntress SOC analysts:

- Own Athena's guardrails and playbooks
- Adjust them as needed
- Reviews any signals Athena views as indeterminate

Helping You Achieve Cyber Resilience

Huntress Platform

comprehensive cyber resilience



HUNTRESS

225k Organizations Protected

Trusted across healthcare, manufacturing, government, education, and services

5M+
Endpoints

11M+
Identities

878k+
Learners

715k+
Log Sources

4.9
G2 Rating

98.6%
CSAT

What We'll Cover

NEED

The trends and threat landscape impacting organizations

NOW

Our platform and how it has advanced in the age of AI

NEXT

New products built to shrink the endpoint & identity attack surface

Huntress is moving left of boom into Security Posture Management

HUNTRESS

Security gaps stall the business

The real cost of “good enough” security posture

45%

Had an incident this year caused by a misconfig

55%

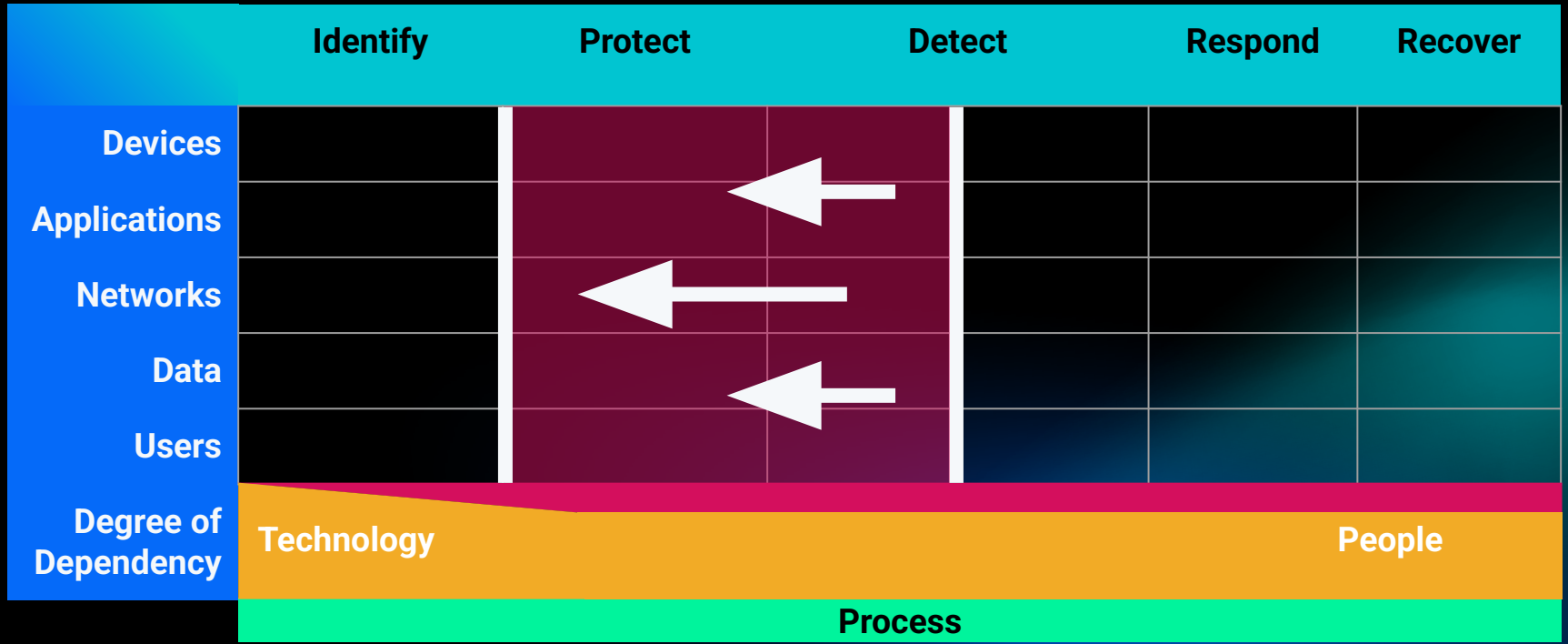
Canceled or delayed initiatives due to posture

47%

Take longer than 24 hours to fix a known misconfig

Market research performed by User Evidence on behalf of Huntress, report to be released spring 2026

It’s time we stop giving attackers easy wins



Huntress ISPM Overview

Huntress Managed ISPM stops attackers getting a foothold

Fortify the environment, prevent the attack

Who can log in

from where

on what devices

with which applications

and approved access levels

Hackers getting a foothold

performing recon

lateral movement

Admin takeover

We secure...

So you avoid...

Huntress Managed ISPM

Continuously audits and enforces configurations, policies, and permissions in Microsoft 365 to shut down the misconfigurations attackers love to exploit.

We don’t leave the door open for hackers to walk in

Fixes weak spots in Microsoft 365 configurations to lock down common hacker attack paths

Fix drift faster than attackers move with always-on identity protection

Enforce an always up-to-date framework tuned to Microsoft guidance, industry standards, and real-world attacker tactics

Harden Microsoft 365, not your workload

Spots policy drift and automatically snaps misconfigurations back to safe defaults

Evidence-Based Controls to Target the Worst Attacker Tactics

- Huntress-managed identity security framework based on SOC insights from 10M+ identities
- Covers the gaps attackers exploit most like risky logins and mailbox manipulation
- Delivers real security, not just better scores

Huntress ESPM Overview

Comprehensive endpoint integrity

Proactive security combined with threat detection and response for full endpoint protection

Managed ESPM

Proactively defend against endpoint attacks

- Application visibility and control
- High-risk vulnerabilities surfaced
- Properly configured OS and security controls
- On-demand demonstrable compliance

Managed EDR

Detect and respond to shut down endpoint attacks

- Threat experts monitoring, assessing, and operationalizing adversary tradecraft and intel
- 24/7 AI-assisted SOC for continuous threat detection, containment, and remediation
- Threat hunting to find stealthy hackers

The value of Huntress Managed ESPM

Proactive defense.
No guesswork or drama.

App control without the headaches

Fast, evidence-based compliance

Built-for *all* businesses