HUNTRESS

Where Huntress Fits in Your Security Stack

Our platform aligns with the NIST Cybersecurity Framework to keep you protected.

The NIST Cybersecurity Framework (CSF) illustrates how layers of security solutions should work together to minimize the risk of cyberthreats. It's a straightforward and easy-to-understand model that focuses on five core components: identify, protect, detect, respond and recover. Let's break down these core components and see which security stack items fit in each.

Our goal is to help you resolve the conundrum of:

- What do I currently have?
- Where are my gaps?
- What can I get rid of or swap out?

Identify

Identify entails determining what the critical functions are and what cybersecurity risks could disrupt them. Understanding what you are protecting is the first step!

- Inventory Management
- Governance, Risk, Compliance

Protect

Protect supports the ability to limit or contain the impact of a potential cybersecurity event (which is where most security budgets are focused today).

- AV/NGAV
- Firewalls
- DNS Filtering
- MFA
- Email Filtering
- Phishing Training
- Encryption
- Application Whitelisting

Detect

Detect includes having the relevant measures in place to quickly uncover threats and other risks. This includes continuous monitoring and threat hunting to identify unusual activity and potential attacks.

- EDR/XDR
- SIEM/SOAR
- IDS
- Honeypots
- Sandbox Analysis
- Global Threat Feeds

Respond

Respond focuses on implementing relevant measures to take action against threats that have made it past preventive tools. This includes response planning, threat analysis and mitigation.

- EDR/XDR
- SOAR
- Ticketing System

Recover

Recovery includes having the tools and strategic plan in place to restore any capabilities or services after a cybersecurity incident.

- Backup Solutions
- Disaster Recovery Plans

We've broken out **where Huntress' various product components fit inside the NIST CSF core functions** so you can see exactly how you will be covered.

Identify

- External Recon
- Phishing Simulation

Protect

- Managed Antivirus
- Security Awareness Training

Detect

- Persistent Footholds
- Ransomware Canaries
- Managed EDR
- MDR for Microsoft 365

Respond

- SOC
- Assisted Remediation
- Host Isolation
- Managed Remediation
- Identity Isolation

Recover

- Huntress may provide guidance on recommended recovery actions

Fun fact ✓

AV is not enough to catch all malicious activity. Attackers are often using legitimate tools to carry out attacks. Last year, Huntress reported more than 350 incidents where attackers had installed commonly used remote management tools.

What a typical SMB security stack looks like:

- Firewalls, email filtering, and website filtering
- Zero Trust models (ex: ThreatLocker)
- Password Manager/MFA (ex: Okta, Duo)
- Antivirus/NGAV solution and/or EDR/MEDR solutions (Defender is a preferred AV for compatibility with MAV)
- Vulnerability Scanner (ex: Rapid7, Tenable)

Huntress agents can work alongside your security stack without blocking or impeding functionality!

What does Huntress offer that other solutions don't?

24/7 SOC

Huntress can augment your team with our Security Experts that are trained and focused specifically on catching hackers using the tools we've built for them. No need for you to be experts, manage the tools, or hire an expert to manage the tools—we got this!

Incident Reports

Other vendors leave a level of ambiguity in their reports, which means your team has to do research and verification on your own. Huntress' reports are actionable intelligence packages, so the work is already done—you just need to approve. We share what we see and provide guidance for you to make the best decision for your company.

Start your free trial today.

HUNTRESS.COM