

No single tool stops everything, so we layer them.

Real security assumes any one defense can fail. Your tools are arranged in three lines of defense: keep threats out, catch and stop what gets through, and recover cleanly when the worst happens. Each layer backs up the one before it.

LINE 1

Prevent

MICROSOFT DEFENDER

Workstation protection

Blocks known malware on every PC and server before it can run.

DEFENDER FOR OFFICE P2

Email & file filtering

Screens inbound mail, links, and attachments — the number one entry point.

HUNTRESS SAT

Trained people

Phishing simulations and training so staff don't click what slips past filters.

CONNECTWISE RMM

Patching & monitoring

Keeps systems updated, closing the holes attackers exploit most.

ZONEWATCHER

DNS monitoring

Alerts on domain and DNS changes that would reroute your mail or site.

BRACKET

Email encryption

Protects sensitive data in transit so it can't be read if intercepted.

↓ IF A THREAT GETS PAST PREVENTION ↓

LINE 2

Detect & Respond

HUNTRESS EDR

Endpoint response

SOC analysts watch Defender's output and isolate a device the moment a real threat acts.

HUNTRESS ITDR

Identity response

Catches stolen-login attacks in Microsoft 365 — account takeover, MFA fatigue — before data moves.

HUNTRESS SIEM

See the whole picture

Correlates logs across endpoints, firewalls and Microsoft 365 to show what happened and how far it spread.

↓ IF DAMAGE IS DONE — DATA DELETED, ENCRYPTED, OR LOST ↓

LINE 3

Recover

VEEAM — M365 BACKUP

Immutable cloud copies

Encrypted, tamper-proof backups of Email, Teams, SharePoint and OneDrive — restorable even after ransomware. Tested monthly.

MSP360 — ENDPOINTS

PCs, Macs & Workspace

File- and system-level restores for workstations, laptops, and Google Workspace. A lost or wiped device isn't lost work.



Why layering matters. An attacker only has to win once; a single tool only has to fail once. Stacked defenses mean a miss at one layer is caught at the next — and even a total breach ends in recovery, not ruin. We **manage** every layer: tuning alerts, acting on what the tools find, and verifying backups actually restore. TANSTAAFL: there's no free lunch in security, so we'd rather show you exactly what each layer buys you.