20 Safeguards, Mapped to the NIST Cybersecurity Framework.

Every safeguard in the Complete plan, grouped by its NIST CSF 2.0 function and delivered to CIS Controls IG2 maturity. Capabilities are described by function, not product name — the specific tools that deliver each are configured per the signed service agreement.

Govern
Own and steer the security program

Identify
Know what you have and where you're exposed

Protect
Stop attacks before they land

Detect & Respond
Catch and contain trouble fast, 24/7

Recover
Get back to business fast — via add-on modules, page 3

Safeguards 01–10

01 DNS / Web Filtering
STAY OPEN

Blocks connections to known-malicious and risky sites at the network level — a safety net that stops malware downloads and phishing sites even after a bad click.

02 Full-Disk Encryption
KEEP TRUST

Encrypts data on laptops and devices so a lost or stolen device can't expose its contents — preventing a lost laptop from becoming a reportable breach.

03 Managed Patching & System Management
RISK REDUCTION

Keeps operating systems and software automatically updated and centrally managed, closing the most common preventable route to compromise.

04 MFA — Endpoints & Business Apps
KEEP TRUST

Requires asecond proofofidentityto sign in, blocking the large majority of account-takeover attempts even with a stolen password.

05 Dark-Web Credential Monitoring
RISK REDUCTION

Monitors criminal marketplaces for the team's leaked usernames and passwords and alerts so they can be reset before misuse.

06 Continuous Vulnerability Scanning
RISK REDUCTION

Regularly scans systems for known weaknesses and misconfigurations, finding flaws before attackers do.

07 Email Authentication (Anti-Spoofing)
STAY OPEN

Configures and maintains SPF,DKIM, and DMARC to stop criminals from sending email that appears to come from your domain.

08 MFA — Email & Microsoft 365
KEEP TRUST

Extends second-factor protection to email and M365, closing the side doors left open when only endpoints are protected. Subject to licensing.

09 EDR + Next-Gen AV
RISK REDUCTION

Detects and blocks malware and ransomware behavior on every device and can automatically isolate a compromised endpoint before it spreads.

10 Security Awareness Training & Phishing Simulation
RISK REDUCTION

Trains staff to recognize and report scams and runs simulated phishing to build and measure that instinct.

Safeguards 11–18 — Govern, Identify & Protect, continued

11 Security Risk Assessment (NIST-Based, Annual)

INFORMED DECISIONS

A formal annual assessment against the NIST framework that prioritizes gaps and produces the cyber insurance and PCI-DSS ASV documentation carriers ask for.

12 Security Policies & Governance Reviews

STAY ELIGIBLE

Maintains written security policies and a regular governance cadence for the evidenced program insurers and regulators expect.

13 Continuous Asset & Endpoint Inventory

STAY ELIGIBLE

Automatically discovers and tracks every device and endpoint connected to the business, so nothing is unknown or unmanaged.

14 Sensitive-Data Discovery

STAY ELIGIBLE

Locates where regulated data lives to limit breach impact and support privacy and payment-card obligations. Provided on request.

15 Basic Firewall Management

RISK REDUCTION

Configures, maintains, and monitors the network firewall so the boundary stays a controlled, defensible edge.

16 Password Management

RISK REDUCTION

A managed vault that generates and stores strong credentials, with tiered admin controls and clean offboarding — ending password reuse.

17 AI Data Protection

RISK REDUCTION

Scans chat input to LLMs for sensitive data — financial records, source code, health data — and blocks it before it leaves the browser.

18 Advanced Email Security

KEEP TRUST

AI-driven detection of impersonation and payment-fraud email that slips past standard filtering — the costliest small-business attack.

Detect & Respond — safeguards 19–20

19 24/7 Managed Detection & Response

STAY OPEN

A human security team monitors device alerts around the clock and investigates and responds to genuine threats.

20 SOC + Centralized Log Monitoring (SIEM)

STAY ELIGIBLE

Collects and correlates activity across the whole environment so a multi-system attack is seen as one picture, 24/7.

Recommended add-ons — extend to full CIS IG2 and the Recover function.

These optional modules round out Complete's coverage—layered in as risk, compliance, or environment warrants. Not included in the base plan.

GOVERN ownership & oversight

Fractional Security Leadership (vCISO)
Part-time executive security and IT leadership that owns your roadmap, risk decisions, budget guidance, and vendor strategy — accountability without a full-time hire.

PROTECT stop attacks before they land

Microsoft 365 Hardening
Applies and continuously monitors a hardened M365 baseline and enforces Conditional Access — risk-based rules for who can sign in, from where, and on which device.

Zero-Trust Remote Access (ZTNA)
Replaces broad VPN access with identity-verified, least-privilege connections to only the resources each user needs.

Firewall-as-a-Service (FWaaS)
A fully managed firewall with current licensing — recommended when existing hardware is out of support or under-licensed .

DETECT & RESPOND catch and contain trouble fast, 24/7

Microsoft 365 Identity Threat Detection & Response
Watches M365 sign-ins and account activity for takeover behavior, catching the root of most business email compromise.

RECOVER get back to business fast

Managed Backup & Disaster Recovery
Independent, encrypted backup of M365, servers, and critical systems with regular restore testing — rapid recovery and compliant archiving.

See how Complete maps to your risk picture.

We'll walk your team through the safeguards, the framework alignment, and where your environment stands today — no obligation.

Start a Strategy Session

Bradenton · Sarasota · Fort Myers · Naples · Bonita Springs · Fort Lauderdale

entechUS.com · 239-539-2433 · Together, we can do what matters.