THInc. SECURE ™

All-in-one managed cybersecurity solution providing next-gen managed detection, response, and remediation across all client platforms, 24/7 SOC, Microsoft 365 security hardening, and more.

Put your business back ahead of evolving tactics used by today's cybercriminals

Designed from the ground up to address the blind spots of conventional MDR, EDR, and SIEM, THInc. Secure provides over 15 security functions in one unified solution, all backed up by a $500K cyber warranty. This complete security program brings together all of the people, processes, and technology to defend against today's increasingly advanced cyber threats. More than just our superior technology, we're known for our superior client onboarding, proactive communication, and strategic approach.

- 24/7 SECURITY OPERATIONS CENTER
- MANAGED DETECTION & RESPONSE
- ENDPOINT DETECTION & RESPONSE
- M365 SECURITY CONFIGURATION
- INCIDENT RESPONSE READINESS
- STRATEGIC GUIDANCE & ADVICE
- $500K CYBER LIABILITY WARRANTY
- VULNERABILITY SCANNING & REPORTS

DETECTION & RESPONSE

THInc. Secure is built on next-gen monitoring architecture that has protected hundreds of thousands of users with zero ransomware events allowed.

We go beyond log-based analysis and integrate data from end points, networks, and cloud services to correlate activity across environments and detect intruders on your network that might go unnoticed by other MDRs.

Microsoft 365 Detection & Response

Cybercriminals know Microsoft 365 can't detect and shut down threats automatically. THInc. Secure monitors 24/7 to stop malicious activity.

Endpoint Detection & Response

We deploy a kernel level endpoint agent for deeper visibility into device activity and provide a range of added capabilities beyond conventional EDRs.

Network Detection & Response

Continuous monitoring across your on-premise, remote, and cloud systems to detect suspicious activity and disable compromised accounts.

Global Active Response

Neutralize threats with automated response policies, tapping into the global threat intelligence community to safeguard against the latest tactics used by cybercriminals.

SECURITY OPERATIONS

Now you have a complete security operations team in your corner and a strategic partner on your cybersecurity and risk management journey.

24x7 Security Operations Center

Our North-American based security operations team is watching over networks, servers, databases, cloud-based services, and endpoints around the clock 365 days a year.

Microsoft 365 Security Hardening

Enable the native security policies and settings in M365 for increased protection where most attacks originate.

Microsoft 365 Configuration & Policy Backup

After security hardening, we monitor for any drift of your baseline or changes to your policies and settings, with nightly backups and a full audit trail.

External Threat Monitoring

Monitor your external defenses for weaknesses including exposed services public IP addresses and domains known services vulnerabilities and email domain protection.

Proactive Threat Hunting

Proactively identify emerging threats, detecting suspicious or anomalous behavior at scale with contextualized analysis.

Enhanced Threat Analysis

Human analysts search for signs of malicious activity that may have evaded automated detection and perform threat root-cause analysis upon request in response to a security event.

Suspicious Email Analysis

Enable staff to report suspicious emails for immediate analysis, streaming syslog or CEF logs from any source to aid in analysis.

DMARC/DKIM/SPF

Monitoring of configurations and alerts to prevent domain spoofing and Business Email Compromise BEC . A continuous learning model ensures your M365 environment remains up to date with the latest security standards from Microsoft.

Microsoft Defender Antivirus Management

Defender Antivirus policies are configured, audited, and enforced within THInc. Secure for centralized endpoint management.

Dark Web Monitoring

Monthly scanning to identify if your organization's data is appearing on the dark web. Daily scanning also available.

RISK & COMPLIANCE

Stay out in front of emerging risks while also preparing for an effective response and successful recovery in the event of a security incident.

Cyber Liability Warranty

Qualified businesses receive a $500,000 cyber liability warranty included with their THInc. Secure subscription at no cost. See agreement for details of qualification criteria.

Incident Response Readiness

Improve readiness of your organization to respond to a security incident and ensure internal stakeholders know what actions to take for the best possible outcome.

Vulnerability Scanning

Ongoing detection for misconfiguration and risks with reporting on vulnerabilities to support compliance with standards like HIPAA, CIS, ISO, Cyber Essentials, GDPR.

Strategic Advice & Guidance

Consultations with a CISSP on security posture, vulnerabilities, resolved/ongoing security issues, incidents, security mechanism deployment, identity and access management, and planning.

TECH HEADS

AVAILABLE PACKAGES

	Cloud	Core	Complete
DETECTION & RESPONSE			
M365 Detection & Response	✓	✓	✓
Endpoint Detection & Response		✓	✓
Network Detection & Response			✓
Global Active Response	✓	✓	✓
SECURITY SERVICES			
24/7 Security Operations Center	✓	✓	✓
Microsoft 365 Security Hardening	✓	✓	✓
M365 Configuration & Policy Backup	✓	✓	✓
External Threat Monitoring		✓	✓
Proactive Threat Hunting	✓	✓	✓
Enhanced Threat Analysis			✓
Suspicious Email Analysis	✓	✓	✓
Microsoft Defender AV Management		✓	✓
Dark Web Monitoring			✓
White Glove Onboarding	✓	✓	✓
RISK & COMPLIANCE			
Cyber Liability Warranty	✓	✓	✓
Incident Response Readiness	✓	✓	✓
Vulnerability Scanning		✓	✓
Strategic Guidance & Advice	✓	✓	✓
Log Retention	90 Days	90 Days	Up to 7 Years

BUSINESSES THAT EXPECT MORE FROM THEIR CYBERSECURITY PARTNERS TRUST TECH HEADS.

Ready to address the gaps in conventional MDR?

With mean time-to-detect and noise to-signal ratio rivaling the best MDRs on the planet, THInc. Secure s monitoring platform has protected hundreds of thousands of users with zero ransomware events allowed. Contact Tech Heads to learn more.