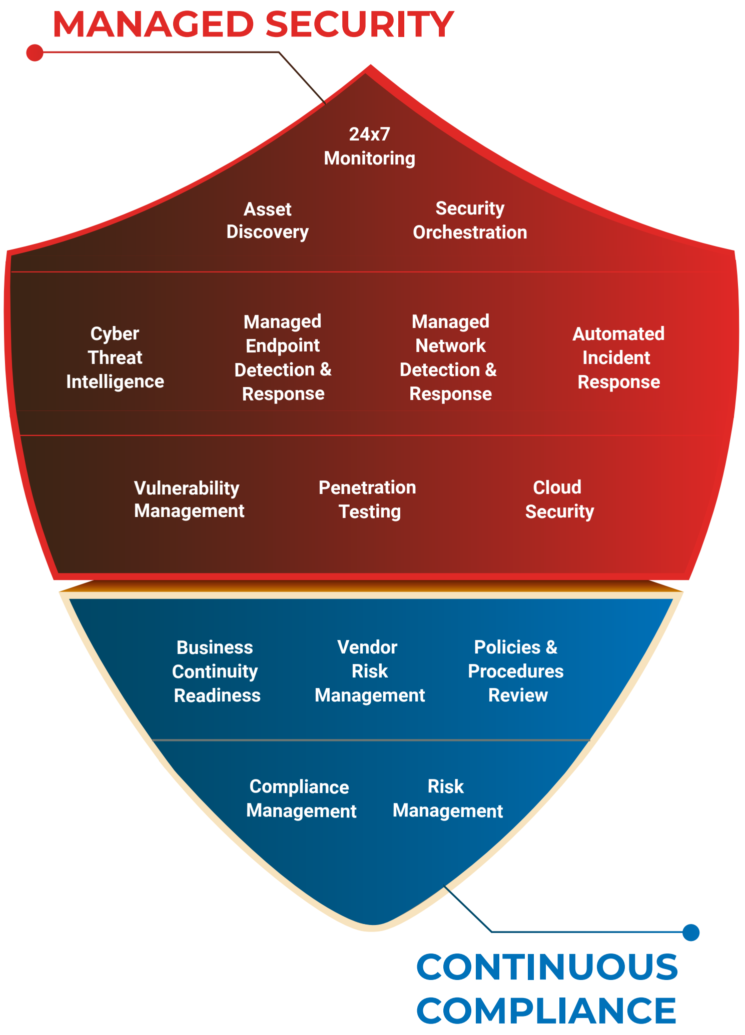
Hunt, Detect, Protect: Advanced

Keeping cyber-safe in the constantly changing threat landscape starts with identifying what IT assets you have and setting up an appropriate monitoring and protection plan. We can help you get in place a proactive cybersecurity and compliance plan that's built for your business and helps you stay compliant.

The Threat Landscape is Growing



MANAGED SECURITY

24x7 Monitoring

Asset Discovery

Security Orchestration

Cyber Threat Intelligence

Managed Endpoint Detection & Response

Managed Network Detection & Response

Automated Incident Response

Vulnerability Management

Penetration Testing

Cloud Security

Business Continuity Readiness

Vendor Risk Management

Policies & Procedures Review

Compliance Management

Risk Management

CONTINUOUS COMPLIANCE

Because a business relies on its assets, having a monitoring and alerting system helps protect your IT environment by keeping you in a proactive position to respond to each potential risk before a vulnerability becomes an issue.

Solution: Proactive Cyber Strategies

Why You Need an Integrated, Ongoing Cybersecurity Program

- Cyber-attacks are on the rise; particularly among small- and mid-sized businesses.
- Data and information systems are accessed through internal networks and wireless devices. Monitoring activities and vulnerabilities can protect against unwarranted events or behaviors.
- An effective, ongoing internal security awareness program can help reduce your company's vulnerability by making your employees the first line of defense.
- Regulatory requirements might require compliance, which can be met by continuously monitoring and identifying risks in defined areas.

Managed Security

Our managed security provides 24/7 monitoring with management and review. Our security analysts provide actionable insights to improve your security posture, and they have rapid response identification and reaction to cyber threats.

Continuous Compliance

Our IT compliance specialists are experienced with HIPAA, PCI DSS, ISO 27001, CCPA, GDPR, and DFARS to keep your business compliant no matter how you are regulated.

$8.19M is the average cost to a U.S. company of a data breach.

Risk Mitigation Platform - Advanced

Advanced Set of Risk Mitigation Entitlements for Up to 100 IP Addresses

Asset Discovery & Management

We work with you to validate & track your assets.

- Discovery of all Assets in the Environment
- 24/7 maintenance of Asset List
- One Asset Inventory Report Per Month

Remote Monitoring & Alerting

We track and analyze behaviors, patterns and security trends on your network, then alert when needed to keep your network safe.

- 24/7 × 365 Remote Monitoring & Alerting
- One Report per Month of Logs, Events & Alerts

Network Security

To track security-related issues: we monitor events or changes on your network and wireless devices, analyze hardware and software settings, assess vulnerabilities, and analyze network traffic.

- 24/7 × 365 Remote Monitoring & Alerting
- One Report per Month of Logs, Events & Alerts

Endpoint Security

We remotely analyze the security of endpoints connected to the network and outside the network. Includes monitoring endpoint devices and analyzing hardware and software configurations.

- 24/7 × 365 Remote Monitoring & Alerting
- One Report per Month of Logs, Events & Alerts

Vulnerability & Penetration Testing

We conduct regular vulnerability scans and penetration tests, and make recommendations based on the analysis of the reports.

- One Vulnerability Scan per Month
- One Penetration Test per Quarter

Policy Creation or Revision

We work with you to determine what kinds of policies you need and get them produced.

- Up to Two Custom IT Policy Creation(s) or Revision(s) of Existing Policies per Year

Risk Management

We give you and your third party vendor a risk assessment to understand the risk posture of all the assets, policies, processes and security controls. Then we analyze the risk identified and apply the security control to reduce the risk.

- One Risk Assessment per Year

Phishing Campaigns

With ever-changing threats present, it is important that your employees are exposed to all the latest phishing traps set by criminals.

- One Campaign per Quarter
- One Report with set of Recommendations per Quarter

Continuous Compliance Management

Identify risks and correlate to the required compliance of two of the following sets of regulatory requirements: HIPAA, PCI DSS, ISO 27001, CCPA, GDPR, and DFARS.

- One Report with set of Recommendations per Month (limited to two compliance standards)

File Integrity Monitoring (FIM) Capabilities

Our File Integrity Monitoring (FIM) solution detects changes to files and directories effectively in near real time, and trigger events based on specific criteria. These events are monitored 24/7 to ascertain if there is any malicious or suspicious activity.

- 24/7 × 365 Remote Monitoring & Alerting
- One Report per Month of Logs, Events & Alerts

Cloud Security

Cloud assets are monitored by installed agents and any security events that arise are analyzed.

- 24/7 × 365 Remote Monitoring & Alerting
- One Recommendations Report per Month

centrexIT™ Taking Care of Business. That's **IT**.