End-to-end security starts with **Insight**

Build resiliency, reduce risk, and strengthen compliance with an all-in-one security partner.

Comprehensive security with a customized approach

Ransomware, phishing, malware, data breaches, insider threats, evolving AI technology, new regulatory requirements: the need for powerful cybersecurity in today's digital landscape can't be overstated. The wrong security strategy leaves too much at risk, but safeguarding your business is a 24x7x365 job — one that requires an all-hands-on-deck approach.

That's where Insight can help. Our cybersecurity consulting services offer comprehensive solutions to address growing threats, and our team of experts provides tailored services to help prevent and mitigate cyberattacks. From risk assessments and vulnerability testing to incident response and compliance management, we'll work tirelessly to protect your most critical assets.

By leveraging industry best practices and deep partnerships with top cybersecurity solutions providers, we help businesses secure their networks, systems, and data effectively. With a focus on proactive security measures and continuous monitoring, Insight empowers organizations to mitigate risks, enhance their security posture, and achieve peace of mind in an increasingly complex cybersecurity environment.

Keep reading to explore essential aspects of a successful security strategy and how Insight can be your all-in-one partner.

Someone's going to find your security gaps.

Let it be us.

As we lean into modern apps, AI technologies, and Operational Technology (OT)/Internet of Things (IoT) devices, the attack surface is expanding. Cloud security, third-party risk, resource constraints, and employee error are major pain points facing modern business.

A key component in preventing attacks, increasing resiliency, and strengthening your overall security posture? Heightened visibility. It's time to sharpen your view.

Improving cybersecurity maturity can include:

✓ Gaining a comprehensive understanding of security technologies to maximize your investments.

✓ Focusing on processes and policies (like employee awareness training programs), as well as threat visibility and management.

✓ Assessing for vulnerabilities and developing/executing an achievable remediation plan.

✓ Designing and building security solutions based on a Zero Trust architecture, like network segmentation and privileged access management.

Our experts will establish a customized approach for your unique needs. With the right solutions, we'll find threats before they find you. Learn how Zero Trust architecture can boost your security, and learn more about our Zero Trust assessment here.

91%

According to our recent survey report, 91% named threat visibility as a top security modernization priority.[1]

What happens after an attack matters, too.

Bolster your ransomware defense and response strategies.

Cyberattacks are a matter of when, not if. Attackers are more persistent than ever, and as ransomware grows in sophistication, you need ironclad solutions to protect your data, devices, users, and reputation.

A well-crafted incident response plan is a critical component of your security strategy, but risk looks different for every organization. You deserve a partner who knows what your business needs.

Our cybersecurity experts will take the time to understand your business and identify ransomware defense solutions aligned to your specific cybersecurity requirements, data environment, and IT complexity.

In addition to preparation, recovery, and infrastructure solutions, key areas of risk minimization include:

$4.88M

The global average cost of a data breach in 2024.[3]

73%

73% of organizations worldwide paid a ransom to recover critical data in 2023.[2]

Identity

Tools like Multi-Factor Authentication (MFA) and Single Sign-On (SSO) make it easier to manage user access to your internal systems.

Endpoints

Data storage and protection solutions for your devices defend your teams from malicious actors — whenever and wherever employees work.

Networks

Solutions like Zero Trust deliver robust protection with encryption, network detection, response control, and remote access features.

Managed XDR

Simplify security management, scale with ease, collect and analyze data, and leverage AI with our Managed XDR services.

Proper planning can make the difference between a minor disruption and a catastrophic event.

Before, during, and after an incident — Insight is there.

In addition to cybersecurity solutions from top security providers, we offer end-to-end incident response services to both prevent and minimize risk to your business. Aligned to the National Institute of Standards and Technology (NIST) framework, our portfolio of incident response solutions addresses every part of the cybersecurity cycle.

With our incident response services, you'll take advantage of key solutions for ransomware prevention and response, including:

BEFORE: Preparation

- Penetration testing and proactive threat hunting
- Incident response planning
- Tabletop exercises
- Emergency Incident Response Retainer (EIRR)

DURING: Incident Management

- Threat identification, containment, and eradication
- Emergency incident response
- Event remediation support

AFTER: Post Incident

- Managed security
- Lessons learned exercises
- Post-incident gap remediation

See a full view of our ransomware defense offerings here, and dive even deeper with our recent Tech Journal article — From Chaos to Control: The Ultimate Incident Response Playbook.

Stay compliant. Stay secure.

It can be difficult to stay aware of what regulatory compliance your industry requires, but the consequences of falling behind are monumental.

So, you're looking to operate more securely, but you're bound by regulatory requirements? And not abiding by best practices can result in an extensive list of consequences? How can you make sure you're meeting regulatory standards while also supporting your business goals?

You're in luck: Our security teams have helped organizations globally manage security, risk, and compliance for decades.

Our GRC offerings include:

✓ Compliance assessments

✓ Security consulting services

✓ Risk and compliance management solutions

✓ Data protection solutions

✓ Regulatory compliance audits

Plus, we're an authorized HITRUST External Assessor (EA). And for those complying with Payment Card Industry (PCI) standards, we have end-to-end expertise in PCI risk management.

QUICK POP QUIZ:

Which of the following is a potential result of poorly executed Governance, Risk, and Compliance (GRC) activities?

a) Heightened complexity

b) Fines and penalties

c) Reduced performance

d) Limited visibility

e) Organizational vulnerability

f) All of the above

You guessed it: All of the above.

Ready to learn more? Check out these resources:

- Our full GRC capabilities
- Our GRC assessment services
- Client story: Card Assets Drives Transformation with Managed Azure Consumption Model

Why choose **Insight** as your end-to-end partner?

As technology rapidly evolves, innovation is key to remaining competitive. But the key to being innovative? Having a secure foundation and the confidence to take risks — knowing your business, people, and data are protected.

Our team of cybersecurity experts will evaluate the implications of your business activities and find the right solutions aligned to your unique needs and objectives. We provide industry-leading knowledge and experience to help navigate your most complex security challenges and create a solid, secure foundation for growth.

For all your security needs, Insight has you covered.

Is it time to reevaluate your security strategy?

[Talk to an expert to get started today.](#)

About Insight

Insight Enterprises, Inc. is a Fortune 500 Solutions Integrator helping organizations accelerate their digital journey to modernize their business and maximize the value of technology. Insight's technical expertise spans cloud and edge-based transformation solutions, with global scale and optimization built on 35+ years of deep partnerships with the world's leading and emerging technology providers.

‡ Insight.

1.800.INSIGHT | insight.com

[1] Insight and Foundry: An IDG, Inc. company. (2024). The Path to Digital Transformation: Where IT Leaders Stand in 2024. Insight-commissioned Foundry survey.

[2] Petrosyan, A. (2023, Aug. 31). Annual share of companies worldwide that paid ransom and recovered data from 2018 to 2023. Statista.

[3] IBM and Ponemon Institute. (July 2024). Cost of a Data Breach Report 2024. IBM.