

Safeguard your data and reputation

with Cybersecurity solutions.



How can a Cybersecurity strategy safeguard information and ensure the confidentiality and integrity of data?

By integrating advanced technologies, robust processes, and best practices, businesses can leverage services like Risk and Compliance, Managed Services, Incident Response, and Security Assurance to address vulnerabilities, manage security posture, and remain resilient and secure in the face of potential threats.

Deploying these comprehensive cybersecurity solutions, including network security, content security, endpoint security, and identity and access management, will result in enhanced protection of sensitive data, maintenance of business continuity, compliance with regulations, preservation of reputation, and a competitive advantage in the market.

Understanding the importance of Cybersecurity

Cybersecurity

Practice of protecting computer systems, networks, programs, and data from digital attacks, unauthorized access, damage, or theft. It encompasses a range of technologies, processes, and practices designed to safeguard information and ensure the confidentiality, integrity, and availability of data. With the increasing reliance on digital technologies and the internet, cybersecurity has become critical for businesses.

SECURE DEVELOPMENT

Secure Development Practices

Set of measures taken during the development process to prevent vulnerabilities and cyber-attacks. These are based on the idea that security should be integrated into all development stages.

DevSecOps Practices

Set of measures to integrate security into the software development lifecycle. Combines DevOps practices with information security to create secure and reliable software quickly and efficiently.

MONITORING AND PREVENTION

SOC: Security Operations Center

Physical installation where security monitoring and management are centralized. This provides timely identification of vulnerabilities for incident prevention.

Fixes

Allocation of development hours to correct and mitigate vulnerabilities. Addressing a backlog of identified vulnerabilities as part of the continuous monitoring by the SOC.

INCIDENT RESPONSE

Incident Response

Allocation of hours for intelligence and incident response. This enables rapid identification and evaluation of threats, incident containment, and recovery of affected data and systems.

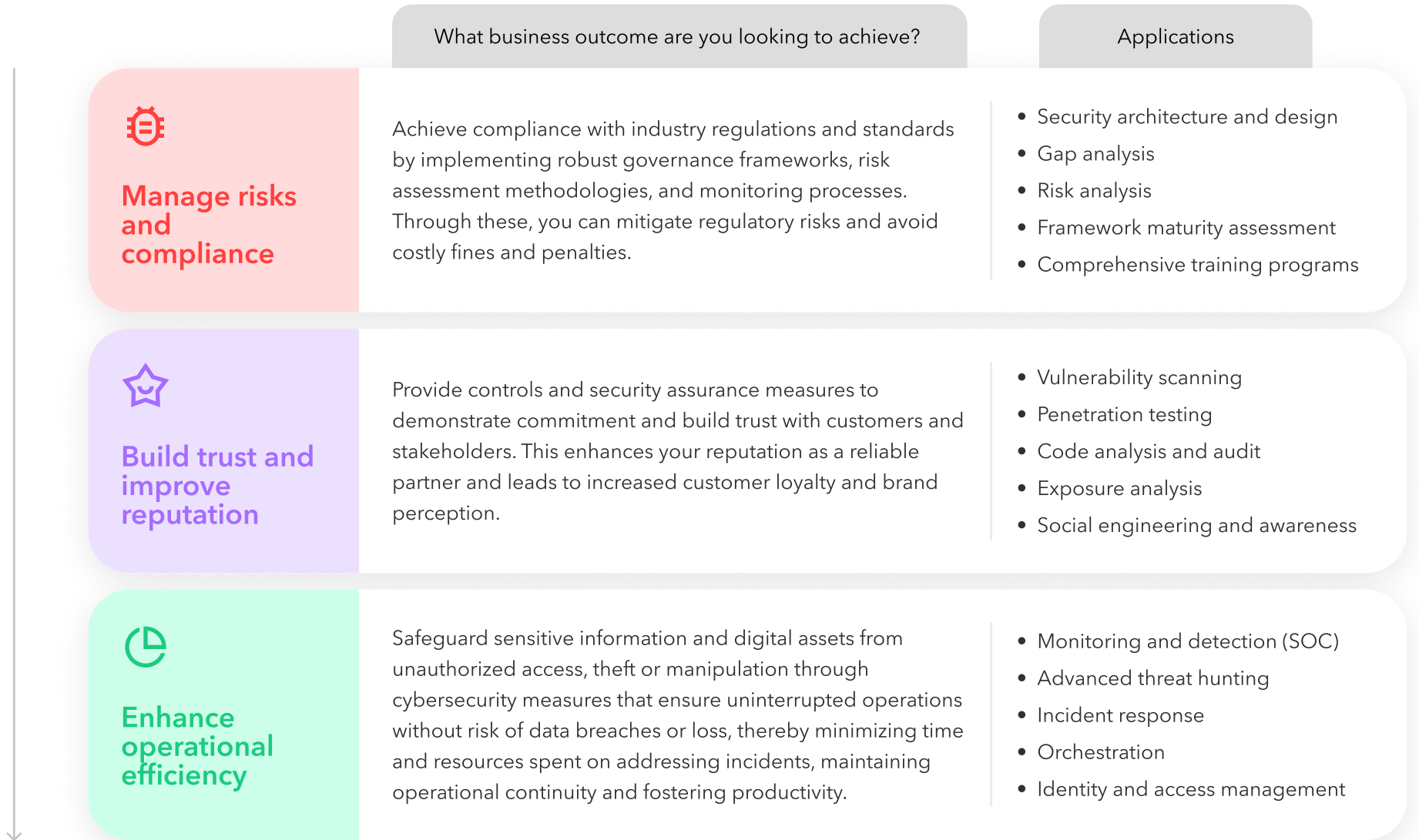
Insurance Policy

Financial coverage for the costs and consequences of cyber-attacks. It may cover incident response, data recovery, breach notification, public relations management, legal claims, etc.

BENEFITS

- Sensitive data protection
- Business continuity maintenance
- Regulations compliance
- Reputation preservation
- Cost savings
- Competitive advantage

Fortifying your business through Cybersecurity



Industry-driven strategies for enhanced protection


From Retail to BFSI, Travel and Hospitality to Manufacturing, industries worldwide are undergoing a paradigm shift in cybersecurity practices, driven by meticulous strategies aimed at safeguarding digital assets. Across diverse sectors, businesses are reimagining traditional security measures, optimizing defenses, and embracing innovative solutions to combat evolving threats.

Through a dedicated focus on Cybersecurity, companies are crafting tailored protection protocols that align with their specific industry needs, ensuring resilient defenses and fostering trust in digital interactions. Let's explore the diverse applications of these strategies across industries:









	Manage risks and compliance <small>Cybersecurity use cases</small>	Build trust and improve reputation <small>Cybersecurity use cases</small>	Enhance operational efficiency <small>Cybersecurity use cases</small>
 <p>Retail</p>	<ul style="list-style-type: none"> • Fraud detection systems • Incident response • Compliance training 	<ul style="list-style-type: none"> • Secure transactions • Customer data protection • Transparent privacy policies 	<ul style="list-style-type: none"> • Supply chain management • Data management • Real-time analytics
 <p>BFSI</p>	<ul style="list-style-type: none"> • Fraud detection • Incident response • Robust compliance 	<ul style="list-style-type: none"> • Secure banking platforms • Secure mobile apps • Personalized security settings 	<ul style="list-style-type: none"> • 24/7 security monitoring • Efficient customer verification • Compliance automation
 <p>Travel & Hospitality</p>	<ul style="list-style-type: none"> • Secure booking platforms • Endpoint security • Incident response 	<ul style="list-style-type: none"> • Secure payment process • Travelers' data protection • Phishing and email security 	<ul style="list-style-type: none"> • Threat detection and response • Supply chain security • Secure collaboration tools
 <p>Sports & Entertainment</p>	<ul style="list-style-type: none"> • Secure venue infrastructure • Sponsorship deals 	<ul style="list-style-type: none"> • Protect fans and players' data • Secure ticketing system • Data integrity in eSports 	<ul style="list-style-type: none"> • Efficient supply chain • Secure media and broadcast distribution
 <p>Manufacturing</p>	<ul style="list-style-type: none"> • Incident response • Access control • Employee awareness 	<ul style="list-style-type: none"> • Data integrity • Secure supply chain management 	<ul style="list-style-type: none"> • Automated threat detection • Supply chain visibility

Cybersecurity maturity journey

Foundation

 <p>Required</p>	<p>Structured evaluation of cybersecurity processes and practices based on the Capability Maturity Model Integration (CMMI) framework.</p>
--	--

Cybersecurity Journey

 <p>Followers</p>	 <p>Initial</p>	<p>Basic cybersecurity measures are established ad hoc.</p>	<p>Cybersecurity processes are unpredictable, reactive, and poorly controlled.</p>
 <p>Challengers</p>	 <p>Managed</p>	<p>Basic cybersecurity activities are formally managed.</p>	<p>Cybersecurity processes are planned, performed, and controlled.</p>
	 <p>Defined</p>	<p>Cybersecurity policies and procedures are formally defined and managed.</p>	<p>Cybersecurity processes are proactive, documented and followed.</p>
	 <p>Quantitatively Managed</p>	<p>Cybersecurity processes are measured and controlled quantitatively.</p>	<p>Organization is data-driven with quantitative performance metrics that are used to manage and improve cybersecurity effectiveness.</p>
 <p>Industry leaders</p>	 <p>Optimizing</p>	<p>Cybersecurity processes are stable and flexible, based on continuous improvement.</p>	<p>Organization is built to pivot and respond to cybersecurity opportunities and change; stability provides a platform for agility and innovation.</p>

Partnering with Applaudo to strengthen your business through Cybersecurity



Foundation

REQUIRED

Cybersecurity Assessment

Cybersecurity assessment helps organizations understand their current maturity level, identify strengths and weaknesses in their cybersecurity practices, and prioritize improvement initiatives to enhance their cybersecurity posture. This assessment is a structured evaluation of the cybersecurity processes and practices based on the Capability Maturity Model Integration (CMMI) framework.

How can we help?

- Evaluation of current practices
- Maturity level determination
- Identification of improvement areas
- Prioritization of improvement initiatives
- Development of action plans
- Continuous improvement

Managed Services

Safeguard your digital assets by protecting your organization from potential cyber threats with our managed services. With a team of experienced professionals and cutting-edge technology, we provide continuous monitoring and threat detection to ensure your business always remains secure.

How can we help?

- **SOC (Security Operations Center)**
- Monitoring and detection
- Advanced threat hunting

Incident Response

Remain resilient and secure in the face of potential threats by effectively managing and resolving incidents with our rapid response intervention. Our expert team ensures swift containment and mitigation, providing your organization with the necessary measures to quickly and efficiently address any security issues.

How can we help?

 **Applaudo** X  **MANDIANT** |  Google Cloud

- Incident response and orchestration
- Applaudo: Tier I-II
- Mandiant: Tier III

Security Assurance

Elevate your cybersecurity readiness by gaining an in-depth understanding of vulnerabilities and how to address them within your digital assets through a rigorous analysis of vulnerabilities and robust security enhancements. A team of experts will guide you in identifying weaknesses that could compromise your operational integrity.

How can we help?

- Vulnerability scanning
- Penetration testing and API testing
- Code, database, and infrastructure audit
- Exposure analysis (OSINT)
- Social engineering and awareness



Governance Risk and Compliance

The true potential of cybersecurity lies within its strategic support for a robust posture. Stay ahead by showcasing a comprehensive cybersecurity strategy that demonstrates compliance excellence. Applaudo serves as your guiding compass, charting a course towards reinforcing your security fabric or navigating through new regulations seamlessly.

How can we help?

- Cybersecurity strategy
- Security architecture and design
- Gap analysis
- Risk analysis
- Framework maturity assessment
- Infosec frameworks alignment
- Comprehensive training programs

Cybersecurity Journey



Contact us

[APPLAUDO.COM/CONTACT](https://www.applaudo.com/contact)