birlasoft

WHITEPAPER

BSecure Framework

Birlasoft's Strategic Response to Evolving Cybersecurity Threats

Overview

In an era of increasing digital transformation, cybersecurity is no longer optional - it's foundational. The BSecure Framework offers a comprehensive, AI-augmented approach to securing enterprise environments, ensuring resilience, compliance, and proactive threat mitigation.

Key Challenges in Cybersecurity

Evolving Threat Landscape:
Constantly changing attack vectors and sophisticated cyber threats.

Data Privacy and Compliance:
Navigating complex regulatory environments (e.g., GDPR, HIPAA).

Lack of Visibility:
Difficulty in monitoring and managing distributed IT environments.

Incident Response Delays:
Slow detection and response times increase breach impact.

Talent Shortage:
Shortage of skilled cybersecurity professionals.

Legacy Systems:
Incompatibility with modern security tools and practices.

Cybersecurity Risks and Challenges in 2025

(Gartner-Informed)

1. **Generative AI Risks**
   The rise of GenAI introduces new vulnerabilities, especially around the handling of unstructured data (e.g., text, images, videos). Organizations must secure. AI models, training data, and outputs to prevent data leakage and model manipulation.

2. **Machine Identity Explosion**
   With increased automation, cloud adoption, and DevOps practices, machine identities (credentials for devices and workloads) are proliferating. Poor management of these identities expands the attack surface and increases the risk of credential misuse.

3. **Talent Shortage and Burnout**
   The persistent gap between cybersecurity talent supply and demand is causing burnout among existing teams. This affects incident response times, innovation, and overall security posture.

4. **Cloud Complexity and Ecosystem Risk**
   Rapid cloud adoption is reshaping digital ecosystems, introducing complexity in visibility, control, and governance. Misconfigurations and lack of unified security policies across multi-cloud environments are major risk factors.

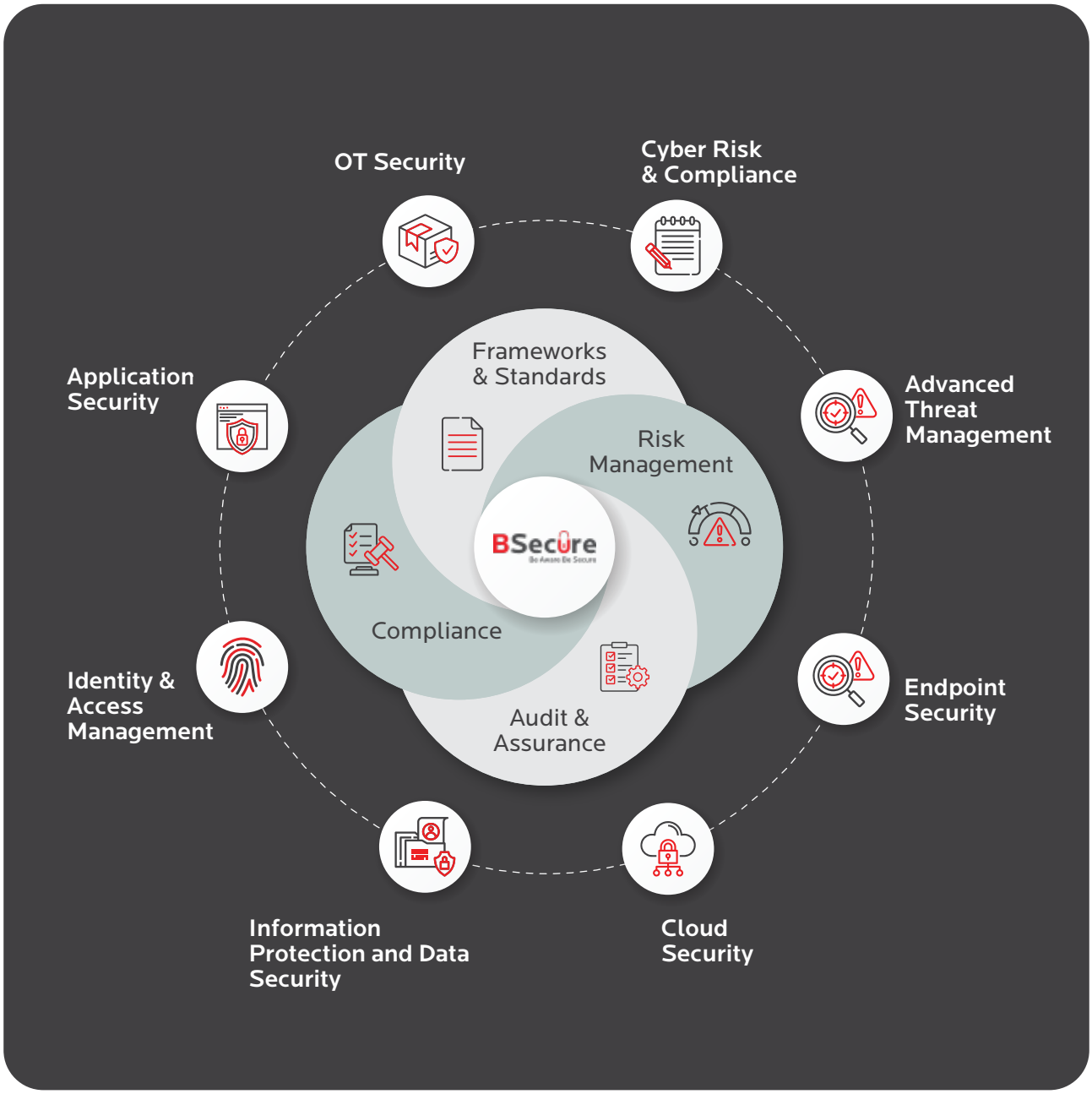
5. **Regulatory Pressure and Compliance**
   Governments are tightening regulations around cybersecurity, privacy, and data localization. Organizations must navigate evolving compliance landscapes while maintaining agility and innovation.

6. **Tactical AI Integration Challenges**
   Security leaders are facing mixed results with broad AI implementations. There's a shift toward tactical AI use cases that deliver measurable outcomes, such as threat detection, anomaly analysis, and automated response.

7. **Supply Chain Vulnerabilities**
   Interconnected supply chains introduce third-party risks. A breach in one vendor can cascade across the ecosystem, making vendor risk management and continuous monitoring essential.

Birlasoft BSecure Framework Solutions

In response to the escalating cybersecurity threats driven by digital transformation, Birlasoft delivers a robust and structured solution through its proprietary BSecure Framework. This comprehensive, AI-augmented cybersecurity service is designed to proactively safeguard enterprise environments, ensuring operational resilience, regulatory compliance, and rapid threat mitigation. By integrating advanced threat intelligence, cloud security, identity governance, and data protection, the BSecure Framework empowers organizations to confidently navigate today's complex risk landscape and secure their digital future.



Agentic AI in Action - Transforming Security Operation

Agentic AI is ushering in a new era of intelligent enterprise operations, where automation, adaptability, and autonomy converge to redefine how work gets done. By embedding AI agents across core IT and productivity domains, organizations can unlock unprecedented efficiency, resilience, and personalization. These agents operate with contextual awareness and

decision-making capabilities, enabling proactive support, seamless collaboration, and dynamic security enforcement.

Cyber Risk & Compliance

Cyber risk and resiliency form the foundation of the BSecure Framework, ensuring enterprises can anticipate, withstand, and recover from cyber threats.

Key Capabilities:

- Risk assessments and gap analysis
- Cyber risk quantification and compliance alignment
- Business continuity and disaster recovery planning
- Security awareness and training programs
- Regulatory and compliance adherence
  (NIST, ISO 27001, GDPR, etc.)

1

Advanced Threat Management

Proactive threat detection and response mechanisms are crucial to mitigating sophisticated cyber-attacks.

Key Capabilities:

- Security Operations Center (SOC) design and implementation
- Threat intelligence and hunting services
- AI-driven anomaly detection and behavioral analytics
- Security Incident and Event Management (SIEM)
- Incident response and forensic investigation

2

Cloud Security

As enterprises migrate to cloud environments, securing cloud infrastructure and applications is paramount.

Key Capabilities:

- Cloud security architecture and governance
- Cloud security posture management (CSPM)
- Secure DevOps (DevSecOps) integration
- Identity and access security for multi-cloud environments
- Cloud workload protection and compliance monitoring

3

Endpoint Security

Securing endpoints, including workstations, servers, and mobile devices, is critical to preventing cyber intrusions.

Key Capabilities:

- Endpoint Detection and Response (EDR)
- Mobile Device Management (MDM) and security
- Zero Trust Network Access (ZTNA)
- Patch management and vulnerability remediation
- Secure remote access solutions

4

Identity and Access Management (IAM)

Ensuring the right users have the right access at the right time is fundamental to cybersecurity.

Key Capabilities:

- Multi-Factor Authentication (MFA) and Single Sign-On (SSO)
- Role-based and attribute-based access control (RBAC/ABAC)
- Just-In-Time (JIT) privileged access management
- User behavior analytics and insider threat detection
- Compliance-driven identity governance

5

Information Protection & Data Security

Data is the most valuable asset for enterprises; its protection is critical against breaches and insider threats.

Key Capabilities:

- Data loss prevention (DLP) solutions
- Encryption for data at rest, in transit, and in use
- Database activity monitoring and access control
- AI-driven data classification and risk assessment
- Secure data sharing and governance frameworks

6

Operational Technology (OT) Security

With IT-OT convergence, industrial control systems (ICS) require strong cybersecurity measures.

Key Capabilities:

- Industrial network segmentation and monitoring
- Secure SCADA and IoT infrastructure
- OT risk assessments and vulnerability management
- Threat detection for critical infrastructure
- Compliance alignment *(NERC CIP, ISA/IEC 62443)*

7

Application Security

Ensuring secure software development and protection against application-layer attacks is a core component of the framework.

Key Capabilities:

- Secure Software Development Lifecycle (SDLC)
- Static and dynamic application security testing (SAST/DAST)
- API security and microservices protection
- Web application firewalls (WAF) implementation
- Runtime application self-protection (RASP)

8

Use Cases for the BSecure Framework

1. **Phishing Detection and Response**
   AI models analyze email metadata, content patterns, and sender behavior to detect phishing attempts in real time. Suspicious emails are automatically quarantined, and users are alerted with contextual risk insights.

2. **Zero Trust Implementation**
   The framework enforces continuous authentication and authorization across users, devices, and applications. AI helps dynamically assess trust levels and adapt access controls based on behavior and risk.

3. **Insider Threat Monitoring**
   Behavioral analytics powered by machine learning detect deviations from normal user activity. The system flags potential insider threats, such as unauthorized data access or unusual login patterns.

4. **Predictive Risk Modeling**
   Generative AI simulates potential attack scenarios and evaluates system vulnerabilities. This helps security teams prioritize mitigation strategies and allocate resources effectively.

5. **Automated Compliance Monitoring**
   The framework continuously checks system configurations and data flows against regulatory standards (e.g., GDPR, HIPAA). AI ensures real-time compliance and generates audit-ready reports.

6. **Threat Intelligence Augmentation**
   AI aggregates and analyzes threat data from multiple sources, identifying emerging risks and correlating them with internal activity. This enables proactive defense and faster incident triage.

7. **Endpoint Protection and Response**
   AI-driven EDR tools monitor endpoint behavior, detect anomalies, and initiate automated containment actions. This minimizes lateral movement and reduces breach impact.

Benefits of the BSecure Framework

Enhanced Threat Detection: AI-driven insights reduce false positives.

Faster Incident Response: Automation reduces mean time to detect (MTTD) and respond (MTTR).

Regulatory Compliance: Continuous monitoring ensures adherence to standards.

Scalability: Adaptable to hybrid and multi-cloud environments.

Conclusion:

The Birlasoft BSecure Framework provides a holistic and structured approach to cybersecurity service implementation and delivery. By integrating risk management, proactive threat intelligence, and compliance-driven security controls across these eight domains, Birlasoft helps enterprises achieve cyber resilience and secure their digital transformation journeys.

References:

https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

https://www.gartner.com/en/newsroom/press-releases/2025-03-03-gartner-identifiesthe-top-cybersecurity-trends-for-2025

Author

Vipin Jamwal

AVP & Global Head of
Cybersecurity Practice,
ICTS

Co-Authors

Bhaskar Kulshrestha,
Asit Verma,
Sameer Khandar,
Abhijit Ghosh,
Vinay Prakash Tiwari,
& Cybersecurity team.

Capt. Vipin Jamwal is an Associate Vice President at Birlasoft, leading the Global Cybersecurity Practice within the Infrastructure Services business unit. A seasoned cybersecurity leader with over 26+ years of experience across diverse sectors including defense, hospitality, banking, retail, and insurance, he brings extensive experience in building and transforming enterprise-wide security programs and governance frameworks for global organizations.

At Birlasoft, Vipin drives the development of intelligent, platform-based cybersecurity solutions that enhance resilience, regulatory compliance, and operational excellence. His focus areas include advanced threat management, cloud security, zero trust architecture, identity and access management (IAM), threat detection and response (XDR/EDR/SIEM), AI-led cyber operations, OT Security, and secure digital transformation initiatives.

He is a strong advocate of automation-first security operations, leveraging SOAR, MITRE ATT&CK mapping, threat intelligence, and AI-driven risk management to enable proactive, scalable, and self-healing cyber defense environments.