Syngene

Putting Science to Work

ENTERPRISE ZERO TRUST TRANSFORMATION

PROJECT LAKSHYA

Securing Science. Safeguarding Trust.

Where scientific innovation meets enterprise-grade cyber resilience



Syngene International Limited

Protecting Scientific Innovation in an Expanding Threat Landscape

BEFORE TRANSFORMATION

A trusted network with a single gate



- ✕ Periodic assessments
- ✕ VPN dependency
- ✕ Broad network trust
- ✕ Fragmented visibility

TODAY'S REALITY

A borderless ecosystem across India and the United States



5000+
employees incl. 2000+ scientists

~400
active global customers

4
locations across India & the US

~3 mn
sq. ft. of R&D and manufacturing

- **Science is borderless. Security had to become borderless too.**

Syngene
Putting Science to Work

Cybersecurity as an Enabler of Scientific Growth



- **Five objectives, one outcome: scientists innovate with confidence.**

Syngene
Putting Science to Work

From Fragmented Security to Integrated Enterprise Defence

BEFORE	AFTER · PROJECT LAKSHYA
ACCESS Perimeter-centric controls and VPN dependency	ACCESS **Identity-aware Zero Trust**
INTEGRATION Limited security integration	INTEGRATION **Integrated security controls**
EXPOSURE Periodic assessments	EXPOSURE **Continuous exposure management**
MONITORING Fragmented monitoring	MONITORING **24×7 monitoring**
GOVERNANCE Fragmented visibility for leadership	GOVERNANCE **Risk-based executive governance**

- **Not a tool upgrade – an operating-model shift from perimeter trust to continuous verification.**

Syngene
Putting Science to Work

One Integrated Cybersecurity Ecosystem

Govern & Assure	ISO/IEC 27001:2022 · Cybersecurity governance · Enterprise risk management · Executive oversight
Prevent & Protect	Zero Trust · MFA · PAM/IGA · Endpoint security (EDR/XDR) · Secure web access · CASB · Microsegmentation
Secure Data & Applications	DLP · Encryption · Email security · WAF · Application testing (SAST, VAPT, Red Team) · AI data protection
Detect & Respond	24×7 Cyber Defence Centre · SIEM · SOAR · Threat intelligence · Incident response · Continuous monitoring

PROTECTING EVERY ENVIRONMENT

- **Enterprise IT**
- **Operational technology**
- **Laboratories**
- **Manufacturing**
- **Cloud & SaaS**
- **Global customers**

- **Four layers, one control plane – designed as an ecosystem, not a product list.**

Syngene
Putting Science to Work

A Risk-Based Cybersecurity Model Built on NIST CSF 2.0

Govern

Policies, accountability and risk oversight under ISO/IEC 27001:2022.

Recover

Business continuity, disaster recovery and lessons learned.

Respond

Incident response, containment and forensic investigation.



Identify

Asset inventory, risk assessment and vulnerability identification.

Protect

Identity security, endpoint protection, DLP and Zero Trust.

Detect

24×7 SOC with SIEM, threat intelligence and continuous monitoring.

- **Lessons learned flow back into governance – risk is managed as a cycle, not a checklist.**

Syngene
Putting Science to Work

Modernising Enterprise Protection Through Zero Trust



Identity & conditional access

MFA, Microsoft Entra conditional access and PAM/IGA



Endpoint detection & response

EDR/XDR with asset visibility across endpoints and servers



Secure internet & private access

ZIA, ZPA and ZTNA with remote browser isolation



Cloud & SaaS protection

CASB visibility and policy for cloud applications



IT/OT microsegmentation

Contains lateral movement between IT and OT networks



Data Loss Prevention

Classification, DLP and encryption for research, client and personal data



Web application protection

WAF, API security and SAST; 45 applications on WAF*



AI security governance

Controls stop confidential data reaching unauthorised AI services

- **Verify explicitly. Grant least privilege. Assume breach – enforced as one integrated platform.**

Syngene
Putting Science to Work

*Application count subject to final confirmation.

24×7 Intelligence-Driven Cyber Defence



SECURITY EVENTS MONITORED

~1.0 bn

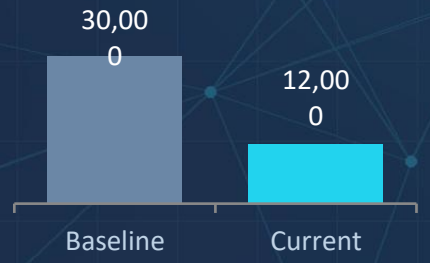
per day (~12,000 events per second)

SUBJECT TO FINAL EVIDENCE VALIDATION

OPERATING MODEL

- Deloitte-supported 24×7 Cyber Defence Centre
- QRadar SIEM with XSOAR response workflows
- Mandiant IR retainer; CERT-In six-hour reporting built in

SOC EVENT VOLUME (EPS)



60% lower

SOURCE-REPORTED · TO BE VALIDATED

- **From raw telemetry to Board-level reporting – one accountable, always-on loop.**

Syngene
Putting Science to Work

Transformation Backed by Measurable Results

EXTERNAL SECURITY RATING

99 /100



SecurityScorecard Grade A – independent view of Syngene's external security posture

SECURE-ACCESS REGISTRATION

96.8%



5,753 devices registered on the secure-access platform; 192 remaining

ENDPOINTS & SERVERS COVERED

~7,500

Protected by Lakshya security controls across India and the US

CYBERSECURITY MONITORING

24×7

Continuous, intelligence-driven monitoring by the Cyber Defence Centre

SOC TICKETS WITHIN SLA

568

Resolved within SLA in May 2026

MAY 2026 · POST-PERIOD

APPLICATIONS PROTECTED BY WAF

45*

Internet-facing applications protected by web application firewall

TO BE CONFIRMED

Nomination period: April 2025 – April 2026. Scores shown as reported at submission; May 2026 SOC volume is post-period supporting evidence. *WAF application count subject to final confirmation.
Source: Project Lakshya programme data.

Syngene
Putting Science to Work

Delivering Transformation Without Disrupting Science





- **Phased implementation**
- **Legacy technology integration**
- **User adoption**
- **Cross-functional coordination**
- **Supplier collaboration**
- **Security validation**

TRANSFORMATION JOURNEY

Governance & identity → **Secure access & endpoints** → **Data & app protection** → **Detect & respond at scale** → **Assure & optimise**

NOMINATION PERIOD · APR 2025 – APR 2026 | POST-PERIOD

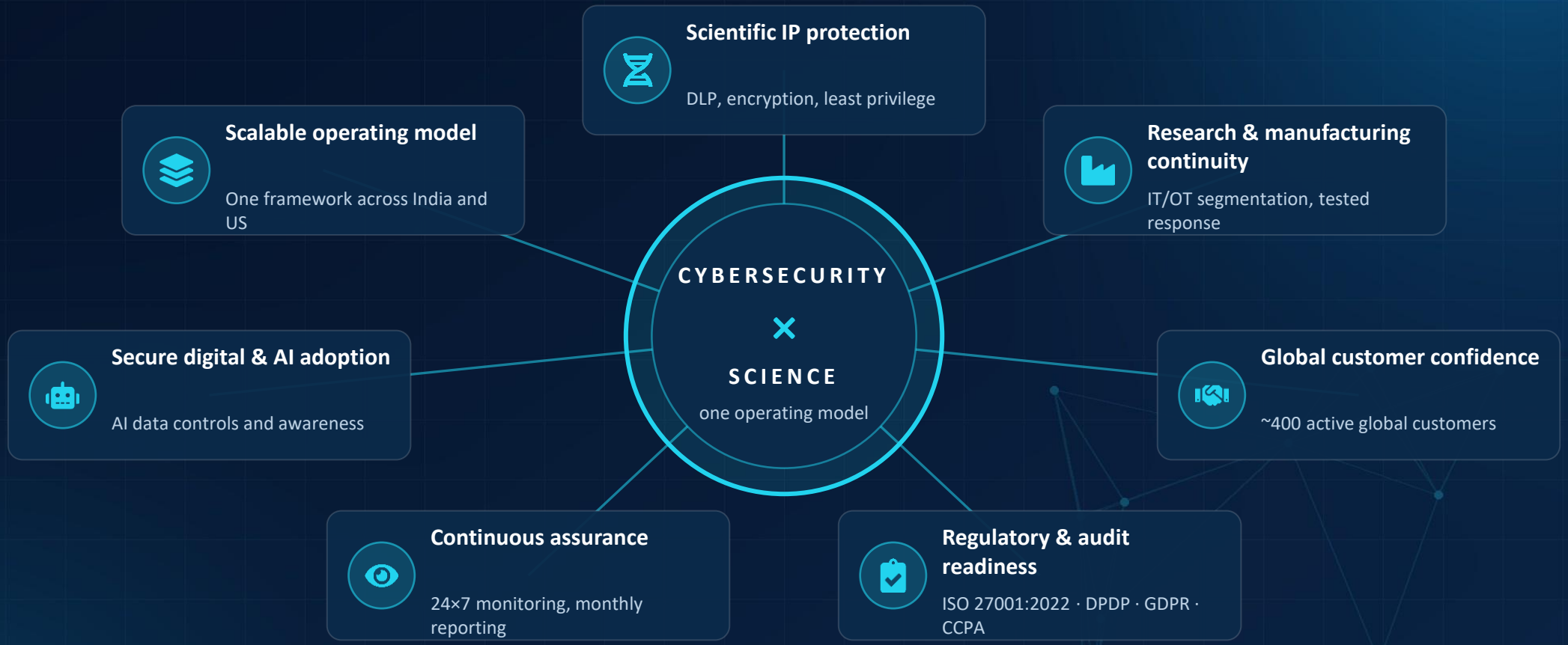
Apr 2025	Mar 2026	Apr 2026	May 2026
Nomination period begins	ISO/IEC 27001:2022 surveillance audit passed	Nomination period ends	568 SOC tickets within SLA

Workstream sequence is indicative – validate against the programme plan. Dates shown are those stated in the nomination and source deck only.

- **Security was re-engineered underneath live science – without stopping it.**

Syngene
Putting Science to Work

Why Project Lakshya Is Different



- **Security designed around the scientist – not around the technology stack.**

Syngene
Putting Science to Work



Syngene

Putting Science to Work

PROJECT LAKSHYA

Securing Science. Safeguarding Trust.

Project Lakshya demonstrates how cybersecurity can become a strategic foundation for scientific innovation, operational resilience and trusted global collaboration. By integrating Zero Trust, continuous monitoring, data protection and accountable governance, Syngene has established a scalable security model designed to protect the science of today and enable the innovations of tomorrow.

Syngene International Limited