Risk + Productivity

Executive exhibits and industry use cases with 2025-2026 market signals

IBM / Ponemon

$4.44M

Avg global breach cost (2025)

CrowdStrike

48 min

Avg breakout time (2025)

Google Mandiant

11 days

Median dwell time (2025)

Microsoft WorkLab

275

Interruptions per workday (2025)

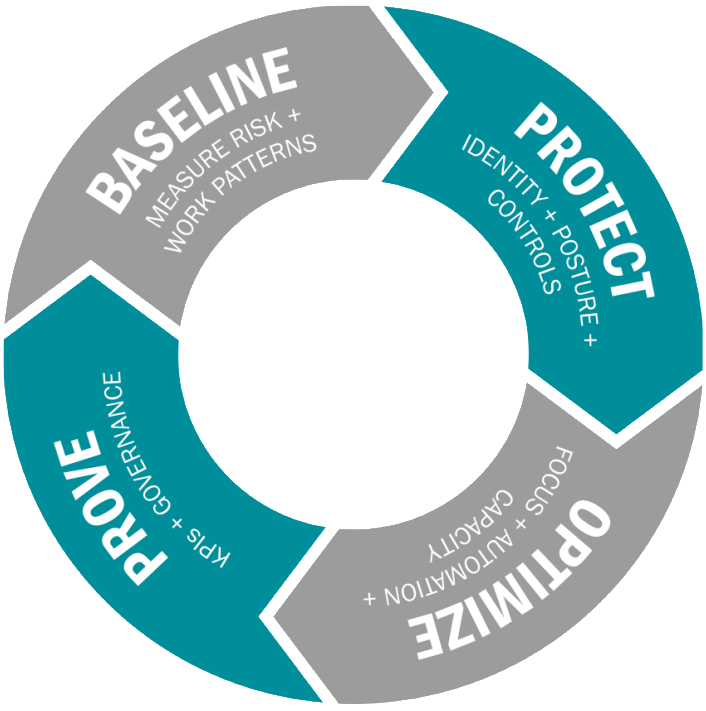
Prepared for: SEGA go-to-market | Date: 2026-01-19 | Regions: Central America + Mexico

2025-2026 market signals (why now)

- **Breach cost:** $4.44M avg (2025)
- **Breakout speed:** 48 min avg, 51 sec fastest (2025)
- **Dwell time:** 11 days median (2025)
- **Infinite workday:** 275 interruptions/day (2025)
- **Macro risk:** AI + supply chain + geopolitics (2026)

Prevent Controls, identity, posture	**Detect** Signals, response, evidence
Enable Adoption, governance	**Optimize** Automation, focus, capacity

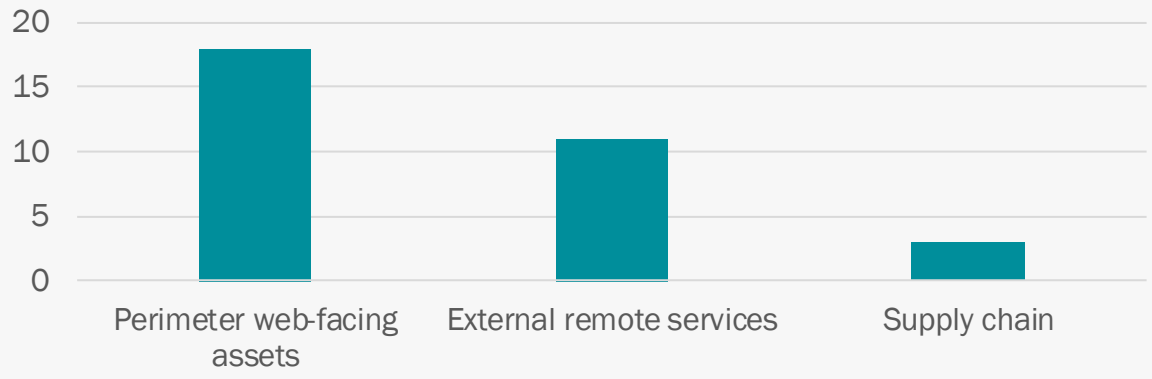
SEGA flywheel (simple and provable)



Executive exhibits (less text, more signal)

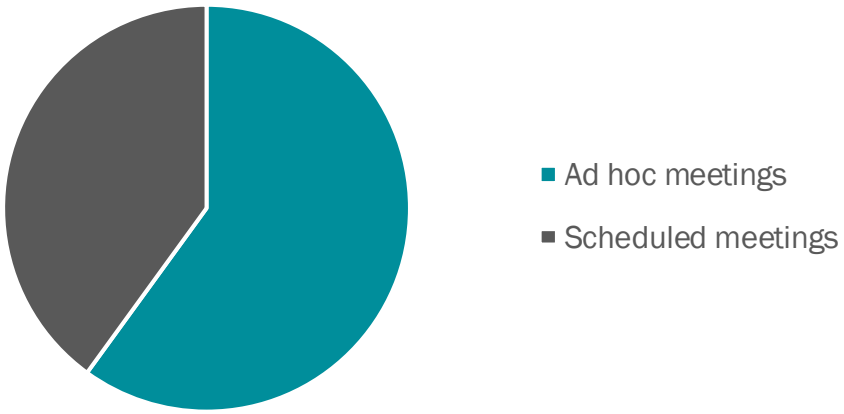
Exhibit 2: Where attacks start (exposure footprint, 2025)

Share of IR engagements (percent)



Source: Microsoft Digital Defense Report 2025 (incident response engagements)

Exhibit 3: Meetings are increasingly ad hoc (2025)



Interruptions/day	Avg between pings	PPT edits last 10 min	After-hours chat YoY
275	**2 min**	**+122%**	**+15%**

Source: Microsoft Work Trend Index / WorkLab (2025 telemetry and survey)

Use cases (page 1 of 2)

Banking
CISO + COO (operations-critical)

Pain points
- Credential-based intrusion
- Audit evidence gaps
- Ticket overload

SEGA levers
- Identity and access hardening
- Threat detection and response
- Work pattern analytics

KPIs to prove impact
- MTTR down
- Privileged access covered
- Focus time up

Insurance
Ops director + Compliance

Pain points
- PII exposure via email/files
- Third-party access risk
- SLA drift

SEGA levers
- Data protection policies
- Access governance
- Capacity and load balancing

KPIs to prove impact
- Cycle time down
- Rework down
- Policy exceptions reduced

Retail
CIO+eCom lead

Pain points
- Availability incidents
- Shared accounts
- Peak overload

SEGA levers
- Monitoring + response
- Zero trust access
- Ops automation + focus

KPIs to prove impact
- Downtime minutes down
- Incident rate down
- Order backlog down

Distribution
Ops + Finance

Pain points
- Field device exposure
- Invoice errors
- Manual reconciliations

SEGA levers
- Secure endpoints
- Workflow automation
- Productivity baseline by role

KPIs to prove impact
- Errors down
- Close cycle faster
- Hours saved

Manufacturing
Plant IT + Maintenance

Pain points
- Ransomware impact
- Patch windows
- Reactive maintenance

SEGA levers
- Segmentation + controls
- Rapid containment
- Standard work analytics

KPIs to prove impact
- Stops reduced
- Change failure rate down
- Lead time down

Government
Digital services director

Pain points
- Sensitive data exposure
- Audit pressure
- Process fragmentation

SEGA levers
- Evidence-ready controls
- Identity governance
- Process + productivity redesign

KPIs to prove impact
- SLA up
- Compliance posture up
- Backlog down

Use cases (page 1 of 2)

BPO / SSC
Operations + HR

Pain points
- PII handling risk
- High turnover
- Quality variation

SEGA levers
- Access controls
- Behavior analytics
- Coaching insights

KPIs to prove impact
- AHT down
- QA up
- Attrition risk reduced

Healthcare
Admin + IT

Pain points
- EHR access risk
- Vendor exposure
- Overloaded staff

SEGA levers
- Identity and audit trails
- Data governance
- Workload analytics

KPIs to prove impact
- Admission time down
- After-hours load down
- Access anomalies down

Education
IT director

Pain points
- Account compromise
- Low IT capacity
- Shadow IT

SEGA levers
- Phishing-resistant MFA
- Device posture
- Self-service automation

KPIs to prove impact
- Incidents down
- Tickets per user down
- Time-to-fix down

Hospitality
GM + Finance

Pain points
- Fraud and chargebacks
- Season peaks
- Manual reporting

SEGA levers
- Fraud monitoring
- Role-based productivity
- Automated reporting

KPIs to prove impact
- Losses down
- Close faster
- Revenue leakage reduced

Professional services
Managing partner

Pain points
- IP leakage risk
- Context switching
- Utilization blind spots

SEGA levers
- DLP and access governance
- Focus-time protection
- Capacity forecasting

KPIs to prove impact
- Utilization up
- Rework down
- After-hours reduced

Tech / SaaS
CTO + SecOps

Pain points
- Supply chain exposure
- Privilege sprawl
- Release pressure

SEGA levers
- Secure CI/CD posture
- Privileged access mgmt
- Automation for toil

KPIs to prove impact
- Change failure rate down
- Mean time to detect down
- Dev toil down

Implementation blueprint (POC-first)

Day 0-3	Day 4-15	Day 16-45	Day 46-90
Baseline	**POC**	**Scale**	**Run**
Deploy sensors, scope roles, define KPIs	Prove risk controls + productivity wins	Expand to priority teams and processes	Governance cadence, automation, dashboards

KPI dashboard (what we measure from day 1)

- Risk: MFA coverage, privileged access control, anomaly events, time-to-contain
- Ops: tickets per user, MTTR, change failure rate, downtime minutes
- People: interruptions/day, focus time, after-hours load, top distraction sources
- Value: hours saved, cost avoided, compliance evidence readiness

Updated sources (2025-2026)

- Microsoft Digital Defense Report 2025 (Microsoft).
- Microsoft Work Trend Index / WorkLab (2025): "Infinite workday" productivity telemetry.
- CrowdStrike 2025 Global Threat Report (breakout time, malware-free detections).
- Google Mandiant M-Trends 2025 (median dwell time, initial vectors).
- Verizon 2025 DBIR (third-party involvement, vulnerability exploitation trends).
- IBM Cost of a Data Breach Report 2025 (global average breach cost).
- World Economic Forum: Global Cybersecurity Outlook 2026 (AI, geopolitics, supply chain risk context).
- ENISA Threat Landscape 2025 (EU incident analysis and trends).

Prevent • Detect • Enable • Optimize

Concrete examples to operationalize Risk + Productivity (SEGA Flywheel playbook)

Prevent

Stop the most common pathways

- MFA phishingnresistant (FIDO2/passkeys) for privileged & highnrisk users
- Posture baselining (Secure Score / device compliance) + rapid hardening sprints
- Least privilege with PIM/JIT + conditional access policies by role

Detect

Find + contain fast (measurable)

- Alert triage with severity model + 24/7 escalation path
- SLA of containment (e.g., high severity: triage <15m, contain <60m)
- Unified telemetry (endpoint, identity, cloud) ® playbooks for repeat attacks

Enable

Govern the collaboration layer

- M365 governance: external sharing policies by group/site, default = least sharing
- Data protection: sensitivity labels + DLP for PII/financial data
- Retention & eDiscovery: defensible policies for audits and incidents

Optimize

Increase capacity (without burnout)

- Automation: ticket triage, approvals, reporting (Power Platform / RPA)
- Interruptions reduction: meeting hygiene, notification policy, focus blocks
- Ops dashboards: capacity, load, and waste hotspots ® weekly execution cadence

Real industry examples (what this looks like in practice)

Banking Prevent: PIM for admin roles; Detect: identity alerts routed to

Retail Enable: tighten external sharing for vendors; Detect: endpoint

BPO/SSC Optimize: auto-triage tickets + knowledge suggestions; Prevent:

Manufacturing Detect: isolate compromised endpoints fast; Enable: retention