VENCER GROUP

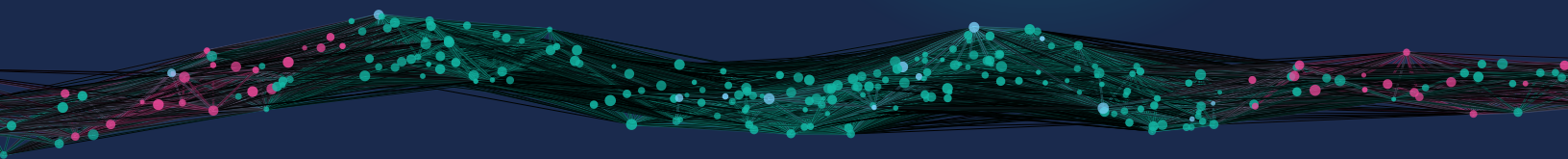
A FREE EDUCATION EBOOK

A CYBERSECURITY GUIDE FOR MID-MARKET OIL & GAS OPERATORS

The Twelve Controls

The twelve cybersecurity controls Canadian cyber insurance underwriters now require evidence on for 2026 renewals - named, scoped, evidenced, with a deployment sequence that actually gets them in place.

Bolted on. **Built in.**



Published by Vencer Group Inc.
Calgary, Alberta · July 2026

vencergroup.com
1-888-271-6230 · Leave a message
connect@vencergroup.com

CHAPTER 00 · FOREWORD

Why mid-market is the target.

For most of the 2010s, mid-market oil and gas operators in Canada operated on a quiet assumption: cyber threats targeted the supermajors. Pipeline operators. Refineries. National oil companies. **That assumption was always wrong. By 2024-25, it became dangerously wrong.**

In July 2025, Zscaler published their ThreatLabz annual report. The headline number for the energy sector: **ransomware attacks against oil and gas companies increased 935% year-over-year**. In August 2024, Halliburton, the largest oilfield services firm in the world, was hit by ransomware and forced to take systems offline for several days. Industrial sector ransomware attacks involving energy companies increased 46% quarter-over-quarter from Q4 2024 to Q1 2025.

Why mid-market is targeted specifically.

Attackers learned three things during 2023-24, and that math does not get better in 2027. It gets worse, because generative AI is becoming a force multiplier.

- Mid-market operators have meaningful revenue, meaningful production data, and meaningful regulatory consequences if disrupted, but most do not have Fortune 500 security budgets or 24/7 security operations centers.
- The IT-to-OT bridge in mid-market is often less segmented than in supermajors, meaning a successful IT intrusion can reach SCADA, historians, and production telemetry in hours rather than days.
- Mid-market cyber insurance payouts are predictable, traceable, and profitable for ransomware groups. The supermajors fight harder. The mid-market pays faster.

The math of opportunistic ransomware now works against mid-market oil and gas. Zscaler’s 2026 predictions explicitly warn that AI-augmented attacks will become standard. **The rest of this ebook is the twelve controls that address that math.**

CHAPTER 01 · THREAT PICTURE

The threat picture, honestly stated.

Most cyber writing aimed at mid-market operators makes one of two mistakes: overstating the threat, or dismissing the reader as too small to matter. **Both are wrong.** Here is the threat picture, as it actually sits for a 30-300 person Canadian operator.

Three categories of threat actor.

- **Opportunistic ransomware groups.** The largest category by volume. Automated scans for vulnerable services, exposed ports, and known CVEs. You get hit because your Fortinet VPN has an open CVE, not because they know your name.
- **Targeted criminal groups.** Smaller category, more dangerous. They identify you specifically, mine your LinkedIn, study your public filings, and build a plan. Energy operators are increasingly on their list.
- **Nation-state actors.** Smallest by volume, most sophisticated. They target energy infrastructure for intelligence gathering and pre-positioning. Rare, but not zero for Canadian operators with cross-border exposure.

What attackers actually want.

- **Ransom payment.** Average payments for mid-market energy sit in the $500K to $3M USD range. Encrypt your systems, threaten data publication, demand payment.
- **Stolen data with market value.** Production data, partner statements, financial records. Even if you don’t pay ransom, the data ends up sold or published.
- **Operational leverage.** Some attackers explicitly target production disruption, for political reasons, market manipulation, or to demonstrate capability.

> **THE PATTERN**
>
> You are not in the threat picture because you are big or interesting. You are in it because you exist, you are reachable, and you have something worth taking. **The controls that defeat opportunistic attacks are not exotic, they are well-known and well-priced.**

CHAPTER 02 · THE TWELVE CONT

The twelve controls, at a glance.

Twelve controls, organized into four groups. **The order is not arbitrary.** Controls 1-4 (identity) create the foundation. Without them, everything else can be bypassed. The rest layer on top.

01 – 04 Identity & Access

Phishing-resistant MFA on all users. **Conditional access** policies by role. **Privileged access management** for admin accounts. **Documented offboarding** with evidence.

05 – 06 Endpoint & Email

EDR (Gartner Leader) on every endpoint, humans in the loop. **Email security (Gartner Leader)** protecting every inbox: BEC detection, social engineering defense, post-delivery remediation.

07 – 08 Resilience & Segmentation

Immutable backups, tested quarterly, air-gapped copies on different infrastructure. **Network segmentation** between IT, OT, and management planes. The bridge is where breach becomes catastrophe.

09 – 12 Operations

24/7 monitoring & detection (NOC/SOC). **Tested incident response plan**, board-endorsed. **Vendor cyber attestation** for every third-party with system access. **Cyber governance** and tabletop discipline.

WHY THIS ORDER

Controls 1-4 lock the door. 5-6 detect what gets past. 7-8 make sure you survive it. **9-12 make it institutional.** Skip the order, and each control does less than it should.

CHAPTER 03 · CONTROLS 1-4

Controls 1-4: Identity, MFA, access.

The foundation. Every other control assumes these four are in place. **Get the identity layer wrong and the rest is decoration.**

CONTROL 01 Phishing-resistant MFA on everything

Hardware keys (FIDO2, YubiKey), device-bound passkeys, or number-matching MFA on Microsoft Authenticator. **What doesn't pass:** SMS, voice, or email-based MFA - all defeated by SIM-swap, phishing, and credential stuffing.

CONTROL 02 Conditional access policies

Block impossible-travel logins, unmanaged devices, and high-risk countries. Enforce compliant device state for privileged apps. **The invisible layer that catches what MFA misses.**

CONTROL 03 Privileged access management (PAM)

Just-in-time admin elevation. Session recording for admin actions. Break-glass accounts inventoried, rotated, and evidenced. **Standing admin rights are the single largest lateral-movement enabler.**

CONTROL 04 Documented offboarding with evidence

Every departing employee's access killed within 24 hours, evidenced. Contractor cadence: quarterly review, quarterly attest. **Zombie accounts are how most attackers stay resident.**

UNDERWRITER TEST

2026 cyber insurance renewals require evidence, not attestation, on all four. Screenshots, log exports, and written offboarding procedures. **Attestation-only carriers are exiting the Canadian energy market.**

CHAPTER 04 · CONTROLS 5-6

Controls 5-6: Endpoint and email.

The detection layer. Once identity is locked, attackers move to endpoints and inboxes. **These two controls decide whether you catch it in minutes or find out from your bank.**

CONTROL 05 EDR (Gartner Leader) on every endpoint

Behavioural detection, not signature-only. Automatic isolation on high-confidence detection. Human-in-the-loop analyst response. **The same tier of EDR used by Fortune 500 SOCs is accessible to mid-market operators at reasonable per-seat pricing.**

CONTROL 06 Email security (Gartner Leader) on every inbox

Business email compromise detection. Post-delivery remediation, catching what got through and landed in the inbox. Social engineering pattern recognition. **Email is still the #1 initial-access vector across all three threat actor categories.**

What passes and what does not.

- **Passes:** SentinelOne, CrowdStrike, Microsoft Defender for Endpoint P2 (with humans behind it), Proofpoint, Abnormal, Barracuda Sentinel with MDR wrapper.
- **Does not pass:** Any bundled antivirus without behavioural analytics, Microsoft 365 default email filtering alone, EDR without 24/7 human triage.
- **The MDR wrapper matters:** An unmonitored EDR agent is a log producer, not a defence. Human analysts turn logs into interventions.

THE COMPOUND EFFECT

Underwriters increasingly require attested MDR (managed detection & response) not just EDR product licence. **The delta is 24/7 humans, not the software.**

CHAPTER 05 · CONTROLS 7-8

Controls 7-8: Backup and segmentation.

The resilience layer. Even with identity locked and endpoints protected, some incidents get through. **These two controls decide whether an incident is a rough week or an existential event.**

CONTROL 07 Immutable backups, tested quarterly

Immutable means **the attacker who owns your domain admin cannot delete or encrypt your backups.** Air-gapped or object-lock storage. Off-site copies on different infrastructure (different cloud, different account, different credentials). Test restore quarterly with a stopwatch.

CONTROL 08 Network segmentation, IT / OT / management

Three planes. IT: user laptops, corporate apps. OT: SCADA, historians, production. Management: network gear, backup infra, hypervisor consoles. **The management plane is where most catastrophic incidents cross over. Segment it as if it were OT.**

Deployment realities.

- **Backup testing:** Untested backups often fail on the day you need them. Silent corruption, missing dependencies, restore times measured in days not hours.
- **Segmentation is not a project:** It’s an ongoing operational discipline. Every new vendor connection, every new app, every new site tests the boundary.
- **OT segmentation is different:** Level 3.5 industrial DMZ, jump servers, recorded sessions, time-bound access. See Chapter 07 for the full pattern.

THE MATH OF SURVIVAL

Operators with tested immutable backups pay ransoms in ~15% of incidents. Operators without pay in ~65%. **The gap is not luck. It’s a control.**

CHAPTER 06 · CONTROLS 9-12

Controls 9-12: The operating layer.

The operating layer. What turns four control groups into a program that survives contact with reality. **Without these four, the first eight controls decay within eighteen months.**

CONTROL 09 24/7 monitoring & detection (NOC/SOC)

Actual humans in an actual NOC/SOC, on shift, tuned to your environment. Physical location matters: your buyer's M&A diligence team can verify the physical infrastructure and named analyst rosters. **Business-hours-only monitoring is a gap, not a control.**

CONTROL 10 Tested incident response plan

Written IR playbook, board-endorsed. Tabletops twice a year, with real scenarios: ransomware, BEC-triggered wire fraud, insider theft. **An untested IR plan is a document, not a plan.**

CONTROL 11 Vendor cyber attestation

Every third-party with system access, evidenced, at the level of specific controls not "we take security seriously." **Supply-chain attacks are increasingly common because the math works: one vendor compromise, many downstream victims.**

CONTROL 12 Cyber governance & tabletop discipline

Board reporting on cadence: composite cyber score, incident count, control drift. The relationship with carriers, auditors, and regulators is proactive not reactive. **Governance is what makes the first eleven controls compound instead of decay.**

CHAPTER 07 · OT/IT CONVERGENCE

OT/IT convergence and the SCADA boundary.

For energy operators, the IT-to-OT bridge is where breach becomes catastrophe. **A ransomware incident on your laptops is a bad week. The same incident reaching your SCADA layer is regulatory, operational, and existential.**

The Purdue reference model, applied.

- **Level 4-5 (IT):** corporate laptops, email, ERP, corporate apps. Standard IT controls apply.
- **Level 3.5 (Industrial DMZ):** the boundary. Jump servers, historians, patch repositories. **This is where your control point sits.** Everything crossing the boundary is inspected, recorded, and time-bound.
- **Level 0-3 (OT):** PLCs, RTUs, SCADA, historians. Different vendors, different lifecycle, different failure modes. Do not treat like IT.

Vendor access, the way it should work.

- Every vendor session goes through a jump server in the DMZ. No direct access to OT assets.
- Every session is recorded and reviewable, for the same reason surgeons record procedures.
- Every session is time-bound. When the vendor is done, access closes automatically. No permanent standing access.

> **WHY THIS MATTERS**
>
> OT downtime for a mid-market Canadian operator is measured in six figures per day, minimum. A production shutdown that would cost a supermajor $10M costs you $10M too, at your scale. **The SCADA boundary is your most important control.**

CHAPTER 08 · CYBER INSURANCE

Cyber insurance. 2026 renewals.

2026 renewals separate operators into two piles: those with evidence, and those with excuses. **Carriers are asking for the artifacts, not the assurances.**

What carriers now require.

- **Phishing-resistant MFA** on privileged, executive, and email accounts. Not SMS, not voice, not email codes. Evidence via M365 authentication method reports.
- **Attested MDR:** not just EDR licence, but 24/7 human triage. Named provider, SOC location, response time SLA in writing.
- **Immutable, tested backups:** quarterly restore log, off-site copy attestation, recovery-time-objective demonstrated not claimed.
- **Board-endorsed IR plan:** latest tabletop within 12 months, minute-taken, with remediation actions closed out.
- **Vendor cyber posture:** attested at the specific-control level for anyone with system access. “We take security seriously” is not an answer any more.

WHAT UNDERWRITERS WON’T SAY OUT LOUD

Operators who can answer all of these affirmatively get the best rates and the broadest limits. Everyone else pays 30-100% more, or gets non-renewed. Cross-border exposure adds complexity, your Bangkok or Houston exposure may not be covered by a Canadian-issued policy without a rider.

PRACTICAL PLAYBOOK

Start renewal prep 90 days before expiry. Assemble the evidence package. Sit down with your broker four weeks before submission. **The renewal outcome is decided before you fill in the questionnaire.**

CHAPTER 09 · WHITE-LABEL MSP

The white-label MSP problem.

Most regional MSPs do not have their own NOC/SOC. They resell someone else's, often with the labels stripped. **None of this is inherently dishonest. It becomes problematic when the disclosure is unclear and the accountability is elsewhere.**

BUYER BEWARE

In every M&A diligence engagement Vencer has run in the last three years, **white-label cyber has been the single most common finding.** The buyer asks: "Who is actually monitoring your environment at 2am?" The answer is often three levels of subcontractor deep.

The three patterns to recognize.

- **NOC/SOC re-labelling:** The MSP's dashboard shows the MSP's logo. The alerts are triaged by a Bangalore or Manila SOC the MSP has never physically visited.
- **"24/7 monitoring" that is really 9-to-5 with a paging service:** Real analysts respond during business hours. Overnight, an on-call rotation may or may not pick up.
- **EDR product resale with no MDR wrapper:** You get the SentinelOne licence, but no human is watching the console. When the alert fires at 2am, no one sees it.

THE FIVE QUESTIONS THAT SURFACE IT

Where is your SOC physically located? Who are your named on-shift analysts? What's your time-to-first-eyes-on-alert? Do you own or resell the EDR platform? **Can I visit your SOC?** The answers, or the discomfort with the questions, tell you everything.

CHAPTER 10 · CHOOSING YOUR STACK

How to choose your cyber stack.

Mid-market cyber vendor selection is where most operators overspend and underprotect. **The right stack costs less than the wrong one, if you know what you're buying.**

The four criteria that actually matter.

ONE Gartner Leader status at minimum

Not niche vendors, not challengers. The tier the Fortune 500 uses is accessible at mid-market pricing now, and the product roadmap is better funded. Non-Leaders often lose feature parity within 18 months.

TWO Human coverage that maps to your risk window

24/7 for anyone with OT or customer PII. Extended-hours for pure IT. **Ask where the analysts physically sit. Ask their names.**

THREE Total cost of ownership at 3-year horizon

Year-one pricing is not the number. Renewal-uplift, integration cost, staff time, incident-cost offset. Cheaper year-one often means more expensive year-three.

FOUR Integration with the rest of your stack

Best-of-breed only works if the products talk. Products that share signal (identity, endpoint, email, network) compound. Products that don't are silo'd cost.

THE DISQUALIFYING SIGNALS

"We take security seriously" without specifics. Reluctance to name their SOC location. No demo of your specific integrations. **Vague answers are the tell.**

CHAPTER 11 · MEASURING POSTURE

Measuring cyber posture.

Cyber posture that isn't measured drifts. **Four metrics, computed quarterly, reported to the board. The composite score turns a fuzzy conversation into a defensible one.**

METRIC 01 Composite cyber score (0-100)

Weighted average of the twelve controls, with each scored 0-10 on evidence quality. Track quarterly. **A 47 defended by evidence beats a 78 defended by attestation.**

METRIC 02 Mean time to detect (MTTD)

From attacker action to your SOC seeing it. For mid-market operators with mature MDR, target is under 60 minutes for high-confidence indicators. For unmonitored environments, it is often weeks.

METRIC 03 Mean time to contain (MTTC)

From detection to isolated. Target: under 60 minutes for endpoint incidents, under 4 hours for identity incidents. Tabletops are where you find out if your written plan matches reality.

METRIC 04 Patch latency, critical vulnerabilities

From CVE disclosure to patched on your systems. Target: under 14 days for critical, under 30 for high. Longer than 90 days on a Fortinet critical is a cover letter for the next incident.

REPORT TO THE BOARD

Quarterly, one page. Composite score trend, top-three drift items, remediation status. The board does not want detail. **They want to know whether the number is going up or down.**

CHAPTER 12 · 90-DAY PLANS

Three postures. Three 90-day plans.

Where you are decides where you start. Three postures, three 90-day plans. **Pick the one that describes your environment honestly. Optimism has never survived contact with an incident.**

STARTING < 30 Foundational posture

MFA on identity, EDR deployed, immutable backups in place, offboarding process documented. **Do not skip to advanced controls. Foundational gaps make advanced controls decorative.**

STARTING 30-60 Improving posture

MDR wrapper on EDR, immutability properly evidenced, real 24/7 monitoring not just tooling. PAM deployed. IR plan tested. **The middle 90 days are about turning products into a program.**

STARTING 60+ Insurance-defensible posture

Composite cyber score tracked, board reporting on cadence, vendor attestation program running. OT/IT boundary hardened. Governance layer institutional. **The goal is renewal at flat or better, and diligence-ready.**

THE CYCLE QUESTION

The cyber program you have at $107 oil is the cyber program you'll be defending at $67 oil. Down-cycle cuts to security show up in insurance renewals and M&A diligence within eighteen months. **Foundational controls do not get cut. Ever.**

WHAT WE DO HERE

Vencer runs 90-day cyber deployment programs for mid-market Canadian operators, mapped to your starting posture, with the twelve controls sequenced correctly. **The next page shows what that looks like operationally.**

CHAPTER ∞ · IN CLOSING

The companies still standing.

Zero client breaches in eleven years, across Canadian mid-market operators with combined exposure of hundreds of millions of dollars in production revenue. **The pattern is boring, on purpose. Boring is what survives the next incident.**

What the survivors have in common.

- **They treat cyber as an operational discipline, not an IT category.** Board level accountability. Quarterly cadence. Documented artifacts. Not a project, a habit.
- **They picked Gartner Leader vendors and stayed with them.** Consistency compounds. Switching cyber vendors every 18 months breaks continuity, breaks tuning, breaks response time.
- **They evidenced everything.** Every offboarding, every MFA enforcement, every backup restore, every tabletop. Insurance-defensible on renewal day is a decision made twelve months earlier.
- **They built the twelve controls in order.** Identity first. Endpoint and email second. Resilience third. Operations layered on top. No shortcuts, no parallel work streams that end up half-done.

> **THE MATH OF THE NEXT INCIDENT**
>
> Companies with the twelve controls in place recover from most incidents in days, without paying ransom, without regulatory disclosure, without losing customer trust. **Companies without them make the news, pay the ransom, and often do not survive the eighteen-month insurance renewal cycle that follows.**

> **ONE CHOICE**
>
> **Eleven years. Zero breaches. Twelve controls. Two sister entities. One choice.** Build the program that survives contact. Or pay for the one you didn’t build. The math is settled.

ABOUT VENCER GROUP

Bolted on.
Built in.

Your IT team, wherever your business operates.

We're builders and operators. **Calgary-rooted. Canadian-reaching. Internationally capable.** With multiple engagement models, 24/7 locally staffed NOC/SOC protection, and field-specific support options.

Founded 2006. Nineteen years operating IT for founders, boards, and operators. Zero client breaches in eleven years. Active client work on four continents right now.

Vencer was built from decades of experience across mergers, divestitures, technology transitions, and daily operations. Every scaling moment, every M&A close, every inflection point, encoded into how we build and how we show up.

19	11	4	24/7
YEARS OPTIMIZING IT	YEARS WITHOUT A BREACH	CONTINENTS DELIVERED	SUPPORT AND MONITORING

Let's talk. One conversation. No pitch.

Thirty minutes. Coffee, Zoom, or however works.

EMAIL
connect@vencergroup.com

PHONE
+1 (888) 271-6230

NOTES, METHODOLOGY & LEGAL

How this ebook was compiled.

CYBERSECURITY DATA AND BENCHMARKS

Threat statistics cited in *The Twelve Controls* are drawn from public reports: Zscaler ThreatLabz 2025 annual report; Canadian Centre for Cyber Security 2025-2026 National Cyber Threat Assessment; Honeywell industrial cyber quarterly data 2024-2025; Claroty operational technology monitoring dashboards. Insurance underwriter requirements reflect published carrier guidance in the Canadian mid-market energy market as of 2026.

OPERATIONAL PATTERNS AND FINANCIAL RANGES

Ranges cited for MSP pricing, engagement models, close cycles, and posture composite scores are drawn from Vencer Group's field engagements across 19 years of Canadian mid-market IT operations, over 30 M&A transactions, and cyber engagements with operators in the 10-to-200 person range. Where relevant, we've cross-referenced against published Service Leadership managed IT benchmarks.

THE SIX LEVERS, FOUR WALLS, THREE POSTURES

The frameworks introduced in *The Crude Truth* are Vencer's, developed through two cycles of field work with Canadian oil and gas operators. They are field observations, not academic constructs. Match them to your situation; they are calibration tools, not prescriptions. The 90-day plans have been executed with real operators; specifics vary by starting posture and organizational context.

ATTRIBUTIONS AND UPDATES

Halliburton, Colonial Pipeline, and RECOPE incidents cited are public reporting. Zscaler predictions for 2026 AI-augmented attacks reflect published forecasts. Cyber insurance market observations reflect Vencer's engagements with Canadian carriers and brokers as of Q2 2026. Content may be updated as market conditions change; consult vencergroup.com/insights for the most current version.

WHERE OUR LAWYERS SMILE

This ebook is a foundational reference. It is educational, not prescriptive. Nothing here constitutes legal, financial, procurement, or IT advice for your specific organization. Where the content cites benchmarks, ranges, or industry patterns, those reflect general market observations at the time of publication and are subject to change. Consult your own advisors and match the frameworks to your situation. Vencer Group is available to help translate the general into the specific under a scoped engagement.

VENCER

GROUP

Bolted on.
Built in.

Based in Calgary · Serving across Canada · International M&A engagements

vencergroup.com · 1-888-271-6230 · connect@vencergroup.com