todyl

_Iran Conflict: Middle East Cyber Threat Landscape & Risk Outlook

For North American SMBs and Mid-Market

TLP: White Unlimited Disclosure

March 13, 2026 | Todyl Threat Intelligence

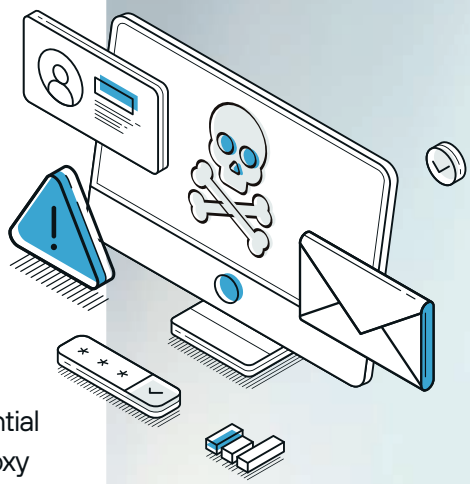
_Table of Contents

This is part two of our assessment into the Iran conflict. For technical detail including threat actor profiles, and industry specific intel, you can access our companion report here:
Iran Conflict and Cyber Risk: What North American Organizations Need to Know.

_Executive Summary

The Iran conflict should now be understood as a combined business-risk event, not simply a foreign-policy issue or a critical-infrastructure concern. Since June 2025, the conflict has moved through successive phases of military escalation, cyber signaling, and growing economic disruption. For organizations in North America, the practical consequence is a sharper convergence of three risks: physical escalation in the region, commercial disruption tied to energy and shipping, and a cyber environment that favors deniable, opportunistic, and scalable attacks.

Iran's cyber playbook does not require immediate, large-scale destructive effects to create meaningful impact. The likely early pattern is a rise in credential theft, password spraying, phishing, exposed-device exploitation, DDoS, leak activity, and quiet access development by a mix of state operators, contractors, proxies, and aligned hacktivists. That matters because many organizations still measure risk by visible damage rather than by access conditions. In this environment, low visible activity should not be mistaken for calm. It may simply mean attackers are probing, staging, or waiting for a better moment to act.



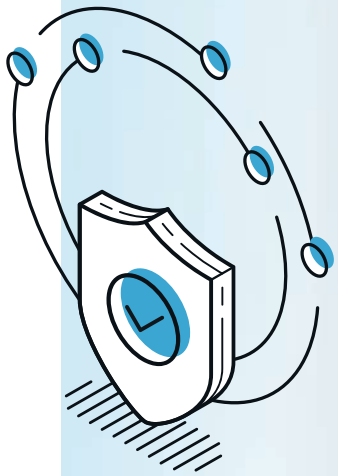
For SMB and mid-market organizations, the main risk is not geopolitical importance; it is accessibility and adjacency. Regional manufacturers, healthcare providers, utilities, logistics firms, local governments, defense-adjacent suppliers, and shared-service providers such as MSPs, MSSPs, SaaS operators, and IT service providers are all exposed because interconnected environments and trusted access can turn a single compromise into broader downstream or multi-tenant impact.

What has changed since our March 1 brief is not the appearance of a radically different Iranian cyber playbook. The more likely pattern remains familiar: credential theft, exposed-system exploitation, DDoS, hack-and-leak activity, disruptive proxy operations, and pressure campaigns amplified through public claims and influence messaging. The mistake is to treat novelty as the signal of seriousness.

The conflict does not need to create a new cyber playbook to create new business risk. It raises the consequence of common gaps, lowers the margin for error, and makes accessible, interconnected organizations more exposed. Iran's broader objective is not limited to technical disruption. Its cyber and influence activity has repeatedly aimed to retaliate, intimidate, undermine support, and create friction through visible or economically consequential targets. That is why businesses across these segments matter. Regional providers, suppliers, healthcare and industrial organizations, technology intermediaries, and service partners can all become useful targets if disruption creates operational pain, public anxiety, or pressure on leadership.

_Key Insights:

- Three risks, kinetic, economic, and cyber, are now converging and reinforcing one another.
- The most likely near-term cyber effects are access operations, DDoS, leak activity, and opportunistic compromise, not necessarily immediate catastrophic attacks.
- Quiet or uneven cyber activity should be treated cautiously; low noise can indicate prepositioning rather than de-escalation.
- SMB and mid-market organizations are exposed through supply-chain adjacency, third-party trust, and weak identity or remote-access controls.
- MSPs and other shared-service providers are force multipliers and therefore attractive targets.
- Additional investment in identity, external exposure reduction, third-party access controls, and incident readiness can materially reduce both the likelihood and severity of an incident in the current environment.



_Situation Snapshot

The conflict visible today is best understood in two phases. The first began in June 2025, when strikes on Iranian nuclear and military targets pushed the confrontation into open interstate escalation and triggered missile retaliation. During that phase, public-sector warnings and private-sector reporting reinforced a familiar cyber pattern: heightened vigilance was warranted even before any broad, catastrophic cyber effects appeared.

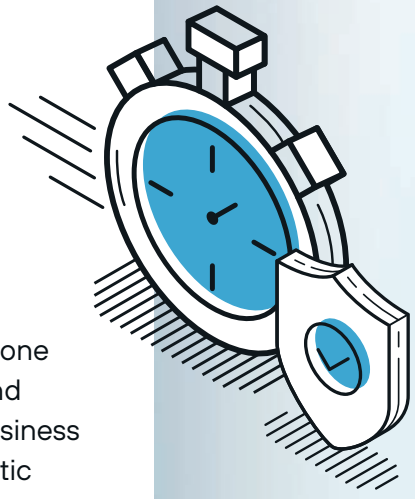
The second phase began in late February 2026 with renewed strikes inside Iran and a broader regional escalation. Since then, the conflict has become more operationally dangerous for businesses because military action, maritime disruption, energy volatility, proxy activity, and cyber pressure are now moving together. The most important implication is not that every forecasted cyber scenario has already occurred. It is that the environment now rewards asymmetric, deniable, and selectively disruptive actions against governments, companies, supply chains, and symbolic targets.

_Timeline

- June 2025: The conflict moves from long-running tension to open military escalation following Israeli strikes and Iranian retaliation.
- Mid June, 2025: The United States strikes key Iranian nuclear sites at Fordow, Natanz, and Esfahan, making the nuclear dimension of the conflict explicit and significantly widening escalation risk.

- Late June 2025: U.S. and allied authorities raise the warning posture for Iranian cyber activity, with specific concern around vulnerable networks, critical infrastructure, and poorly secured internet-exposed systems.
- Mid to late 2025: Visible cyber effects remain uneven, but the threat picture stays elevated; limited public disruption does not reduce the relevance of Iranian access-oriented tradecraft.
- February 28, 2026: Renewed U.S.-Israeli strikes open a broader and riskier phase of the conflict.
- Early March 2026: Shipping, aviation, and energy disruption intensify, turning Hormuz-related instability into a direct business-risk multiplier.
- March 2026: Cyber activity continues alongside kinetic operations through a mix of observed disruptions, proxy and hacktivist signaling, and heightened indirect risk for organizations with regional or supply-chain exposure.
- Current assessment: this should be treated as a sustained period of elevated business and cyber risk, not a short-lived headline event.

While there have already been notable disruptive incidents, including the Stryker event discussed later in this briefing, there has not yet been a single broad cyber event that defines the conflict. In Iranian cyber operations, quiet access, probing, credential theft, and deniable proxy activity can matter as much as immediate spectacle.



_Why This Matters to Businesses

_Three Interconnected Risks

This conflict matters because three forms of risk are now reinforcing one another at the same time: kinetic escalation, economic disruption, and cyber pressure. Each can exist on its own. Together, they create a business environment in which operational strain, uncertainty, and opportunistic targeting compound quickly.

Kinetic

The physical conflict remains the core driver. Military action, proxy retaliation, shipping attacks, and regional spillover create direct exposure for any organization with personnel, assets, customers, suppliers, or logistics dependencies tied to the region. Even organizations far from the battlefield are affected when carriers reroute, insurers reprice risk, governments issue new advisories, and leadership teams are forced to make decisions under incomplete information.

Economic
The economic disruption is a force multiplier. Instability tied to the Strait of Hormuz and broader Gulf shipping has immediate downstream consequences for fuel, freight, insurance, parts availability, delivery times, and customer behavior. That matters to security because organizations under cost and continuity pressure often defer projects, extend the life of aging infrastructure, accelerate vendor substitutions, or tolerate more operational shortcuts than they otherwise would. In practice, economic friction often translates into more exposed systems, more fragile workflows, and less room for disciplined response.

Cyber
Cyber offers Iran and aligned actors a scalable form of retaliation that can be calibrated more easily than direct military action. It supports signaling, psychological pressure, disruption, intelligence collection, and access development without requiring immediate overt attribution. The most likely near-term pattern is not necessarily a single catastrophic attack. It is a broadening of access operations, leak activity, DDoS, web compromise, and selective disruptive actions against reachable targets, symbolic targets, or shared-service providers.

Why the convergence matters
The real issue is not which risk appears first. It is that each one lowers the threshold for the others to matter. Kinetic escalation raises business stress. Economic stress weakens resilience and increases tolerance for technical debt. Cyber operations exploit exactly those conditions. That is why the right framing for leadership is not "war risk" or "cyber risk" in isolation. It is resilience risk under geopolitical pressure.

_Why SMB and Mid-Market Organizations Are Exposed

SMB and mid-market organizations are often wrongly treated as peripheral to geopolitical conflict. In practice, they are frequently the most available targets and, in many cases, the easiest route to something larger.

Accessibility over prestige
Iran-linked activity has long favored practical access paths: weak identity controls, exposed remote access, internet-facing appliances, and under-resourced environments. Smaller and mid-sized organizations frequently have exactly this combination. They do not need to be strategically famous to be operationally attractive.

Supply-chain adjacency
Many mid-market firms sit inside larger organizations' delivery chains. Manufacturers support defense and industrial customers. Regional healthcare providers connect into insurers, labs, and device ecosystems. Logistics firms sit between importers, warehouses, and retailers. Professional-services firms hold sensitive communications and documents. Attackers do not need to breach the most hardened enterprise first if a smaller partner offers trust, connectivity, or privileged access.

Identity and SaaS concentration
Modern mid-market environments are highly identity-centric. Administrators often manage email, collaboration, CRM, file sharing, VPN, endpoint tooling, and sometimes cloud infrastructure through a relatively small number of privileged accounts. That makes account takeover, session theft, MFA fatigue, help-desk manipulation, and delegated-admin abuse especially dangerous.

MSP and IT service provider multiplier effect
MSPs, MSSPs, resellers, outsourced IT teams, and cloud service providers deserve special attention. A single compromised remote monitoring tool, support account, tenant integration, or privileged technician workflow can create a multi-customer incident. For that reason, shared-service providers are not just another vertical; they are access multipliers.

Public-facing and OT-adjacent weak points
Hospitals, local utilities, water systems, building-management environments, manufacturers, transportation operators, and regional public-sector entities often combine symbolic value with practical security gaps. These organizations do not need to represent national strategic command and control to be disruptive, visible, or useful to an adversary.

_Cyber Threat Model

_How Iran Operates in Cyberspace

Iran's cyber ecosystem is best understood as layered. Core state organizations, intelligence services, military-linked units, contractors, access brokers, proxy personas, and hacktivist brands can all contribute to the same operating environment. That layered model gives Tehran flexibility: it can collect intelligence quietly, create public pressure noisily, and preserve deniability when useful.

A layered operating model
At the center are state and state-aligned operators associated with espionage, disruptive operations, credential theft, and long-term access

development. Around that core sit contractors, front companies, and operational clusters that may specialize in phishing, malware delivery, or persistence. Outside them are affiliated or opportunistic personas that present as hacktivists, leak groups, or ideologically motivated disruptors. The result is an ecosystem that can look fragmented in public but still produce coherent pressure in practice.

The consistent access playbook
The methods are familiar because they work. Iranian activity has repeatedly been associated with credential theft, password spraying, tailored phishing, fake login portals, exploitation of exposed edge devices, abuse of remote administration paths, and compromise of poorly secured internet-facing systems. The main lesson is that the front door is usually identity, exposure, or trust and not exotic malware.

Post-access behavior
Once inside, operators often rely on techniques that blend into normal administration. They use legitimate tools, scripts, remote access software, built-in system utilities, PowerShell, browser artifacts, stolen tokens, and cloud platform features to move, persist, and collect. This lowers noise, complicates attribution, and allows them to stay useful even when they are not ready to act.

The two-phase model
A practical way to understand Iranian operations is as a two-phase model. Phase one is access development: gain entry, test credentials, map the environment, preserve footholds, and identify useful accounts or systems. Phase two is flexible operationalization: espionage, leak activity, account abuse, DDoS, wiper-style disruption, extortion-enabling access transfer, or selective OT/ICS interference. Not every intrusion moves to phase two immediately. That is precisely why quiet periods should be treated carefully.

What this means right now
The most likely near-term operating picture is not constant spectacle. It is a mix of probing, access retention, opportunistic compromise, and a smaller number of disruptive or symbolic incidents. That pattern is strategically useful because it preserves options, creates uncertainty, and allows different levels of pressure against different target classes.

_Who Gets Targeted and How

Iran-linked activity is best predicted by target logic rather than by sector labels alone. The three main criteria are accessibility, symbolic value, and downstream leverage.

Accessibility
Organizations with exposed appliances, weak identity controls, unmanaged third-party access, aging VPNs, flat networks, or inconsistent cloud controls are more attractive because they are easier to reach. This includes many smaller businesses, municipalities, clinics, regional operators, and multi-site businesses.

Symbolic value
Targets that create public anxiety or strong headlines can be useful even when they are not technically the most important. Healthcare-adjacent organizations, local services, utilities, public-facing web properties, and financial or payment-related organizations all carry reputational and psychological value.

A disruptive incident against a recognizable brand or sensitive service can create outsized pressure relative to the effort required.

Downstream leverage
Some organizations are attractive because compromise opens doors elsewhere. MSPs, MSSPs, IT outsourcers, SaaS operators, identity providers, payment processors, telecom-adjacent providers, and defense-adjacent suppliers all create leverage beyond a single victim. This is one of the clearest reasons mid-market firms remain exposed during geopolitical surges.

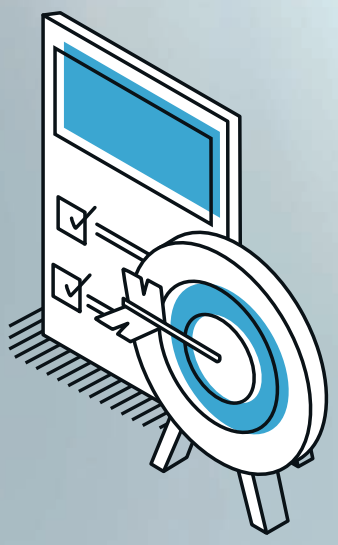
_Documented Targeting Patterns

Historically and in current warning posture, the sectors most relevant to this conflict include energy and industrial environments, water and wastewater systems, telecom, transportation and logistics, public sector entities, defense-adjacent suppliers, healthcare-adjacent organizations, and shared-service technology providers. The common thread is not prestige alone. It is a combination of reachability, disruption value, and indirect access.

Water and OT as proof of method
The Unitronics-related water sector activity remains an important proof point because it shows how internet-exposed industrial control environments can become symbolic and operational targets even outside the largest utilities. Smaller operators with exposed HMIs, default credentials, weak segmentation, or limited monitoring should assume that visibility and simplicity can matter more than scale.

Stryker as proof of concept
The recent Stryker incident is best understood as a proof of concept for the current moment: a high-visibility, healthcare-adjacent target can be disrupted in a way that is operationally meaningful, publicly resonant, and strategically useful even if the broader campaign remains deniable and uneven. The lesson is not that every medical or industrial organization will see the same activity. The lesson is that symbolic, customer-facing disruption is both possible and useful.

IT service providers as access multipliers
Wherever trusted remote access, delegated administration, shared security tooling, or multi-tenant management exists, the impact of compromise expands fast. This is why service providers, outsourced IT teams, and technology intermediaries should be treated as priority hardening and monitoring cases rather than as a supporting footnote.



_What Organizations Get Wrong

The biggest exposure is often conceptual. Many organizations still rely on assumptions that fit a peacetime threat model rather than a conflict-driven one.

"We're too small."
Size is not protection. Smaller organizations are often more exposed, less segmented, and more dependent on a handful of systems and accounts. In conflict periods, accessibility beats prestige.

"Nation-state activity only matters to government and defense."
Nation-state pressure frequently moves through suppliers, regional operators, service providers, healthcare, logistics, and software or identity intermediaries. A private business may never be the political objective and still become the operational victim.

"If we have EDR, we are covered."
This threat model is heavily identity-, cloud-, and access-driven. EDR matters, but it does not by itself stop password spraying, stolen sessions, compromised help-desk workflows, delegated-admin abuse, or exposed remote management paths.

"Cyber war will be obvious."
It may not be. Early indicators are often quiet: repeated login attempts, suspicious OAuth grants, abnormal remote sessions, new admin accounts, unexplained MFA prompts, website probing, or benign-looking changes to administrative tooling. Waiting for a dramatic outage means reacting late.

"If the tactics look familiar, the risk hasn't really changed."
That is the wrong benchmark. The current risk does not depend on a novel technique or a single defining cyber event. Familiar activity such as credential theft, phishing, DDoS, vendor compromise, or quiet access development can carry greater business consequences in the current environment because the margin for error is lower and interconnected organizations are more exposed. The right question is not whether the activity looks new. It is whether existing weaknesses could now produce broader operational, customer, or reputational impact.

"This is mainly a technical problem."
It is also a leadership, continuity, and communications problem. When cyber pressure arrives during a broader geopolitical shock, legal, insurance, PR, customer success, vendor management, and executive leadership all become part of the response path.

What To Do

_Priority Actions for Leaders and IT Teams

The right response is not panic. It is disciplined reduction of the attack paths most likely to matter.

1. Treat identity as the front door

Review privileged accounts, enforce phishing-resistant MFA where possible, tighten conditional access, reduce standing admin privileges, review service accounts, and validate recovery paths for identity platforms, and strengthen ITDR coverage to improve detection of suspicious account activity, privilege abuse, and identity-based intrusion. Focus especially on email administrators, IdP administrators, cloud administrators, remote-management platforms, backup systems, and security tooling.

2. Reduce external attack surface

Inventory internet-facing systems and remote access paths. Remove or restrict unnecessary exposure. Prioritize VPNs, firewalls, edge appliances, remote desktop gateways, support portals, admin consoles, OT-adjacent interfaces, and any legacy systems still reachable from the internet. Where possible, apply IP allowlisting, Zero Trust Network Access, and other access controls that limit who can reach administrative and remote-access infrastructure in the first place.

3. Harden third-party and vendor access

Review all external support paths, delegated admin roles, RMM tools, MSP workflows, and shared credentials. Require named accounts, MFA, just-in-time access where possible, logging, and approval-based elevation. Disable stale vendor accounts and verify who can reach what right now.

4. Prepare for cyber disruption as a business continuity event

Update BCP and DR planning for scenarios in which the issue is not only ransomware but also account compromise, cloud lockout, DDoS, SaaS disruption, destructive activity, vendor compromise, or public leak pressure. Confirm manual workarounds for essential workflows and verify communications alternatives.

5. Increase monitoring around the behaviors that matter

Use SIEM correlation, MDR monitoring, and behavioral anomaly detection to watch for password spraying, impossible travel, token abuse, suspicious mailbox rules, OAuth grants, MFA fatigue, remote session anomalies, admin-role changes, unusual outbound traffic from internet-facing or OT-adjacent assets, and the emergence of new or commonly abused third-party tools that can blend in with routine administrative activity, especially where remote support, scripting, or unattended access is involved.

6. Rehearse decisions before you need them

Run a tabletop that includes executive leadership, IT, security, legal, communications, and customer-facing teams. Test the first 24 hours of a scenario involving account compromise, public disruption, or vendor-originated intrusion. The goal is not perfection. It is faster coordination.

7. Assess business, political, and public exposure

Identify what makes your organization symbolically attractive. Public statements, regional ties, defense or government adjacency, high-profile customers, healthcare or utility operations, and visible executive profiles can all shape risk. Then put that assessment to work: prioritize additional hardening and monitoring around the systems, vendors, business units, and customer-facing services most likely to draw attention; align communications and escalation plans for the scenarios most likely to create public pressure; and brief leadership on where a routine cyber incident could become a broader business event. The goal is not to change your business profile. It is to understand where attention may land and reduce the blast radius before it does.

8. Verify recovery, not just prevention

Confirm that backups, identity recovery procedures, emergency communications, alternate support paths, and incident-retainer contacts work. In a conflict-driven event, response speed and credibility often matter as much as prevention.

9. What This Means for Executives

This is not a call for open-ended spending or reactive security activity. It is a call to manage a changing risk environment with enough structure and discipline that leadership can understand the tradeoffs, prioritize the right controls, and explain the rationale behind those decisions. The central question is not simply whether to spend more on security. It is whether the organization can identify the risks most likely to matter, evaluate their business impact, and decide which risks to reduce, which to monitor, and which risks it is consciously accepting.

In practice, that means treating cyber as an enterprise risk management issue rather than as a narrow technical issue. GRC tools, best-practice frameworks, and a current risk register can help translate technical exposure into business terms: which scenarios matter most, how likely they are, what the operational, financial, regulatory, and reputational impacts could be, what controls exist today, where the gaps remain, and what each mitigation option costs in money, time, and operational friction. That

structure is what allows leadership and the board to make informed decisions instead of reacting to headlines or vague threat warnings.

The practical implication is that leaders do not need to become experts in Iranian tradecraft. They need a clear view of where the organization is exposed, how those exposures map to business processes, and what the tradeoffs look like between additional control investment, operational burden, residual risk, and recovery capacity. In the current environment, that means understanding whether familiar weaknesses such as weak identity controls, external exposure, third-party trust, or incomplete recovery planning could now produce outsized business consequences.

Risk management priorities

- Use GRC tools and best-practice frameworks to map the most relevant conflict-driven scenarios to business processes, control gaps, and owners.
- Maintain a current risk register that captures the scenarios most likely to matter, the controls already in place, the residual risk that remains, and the decisions required from leadership.
- Prioritize targeted investment where it most directly lowers risk: identity hardening, external exposure reduction, third-party access controls, ITDR, MDR, SIEM, continuity planning, and recovery readiness.
- Distinguish clearly between risks the organization is reducing now, risks it is monitoring more closely, and risks it is consciously accepting based on cost, complexity, or operational tradeoffs.
- Create a reporting cadence that translates technical progress into business language so leadership and the board can track risk reduction without getting lost in raw security telemetry.

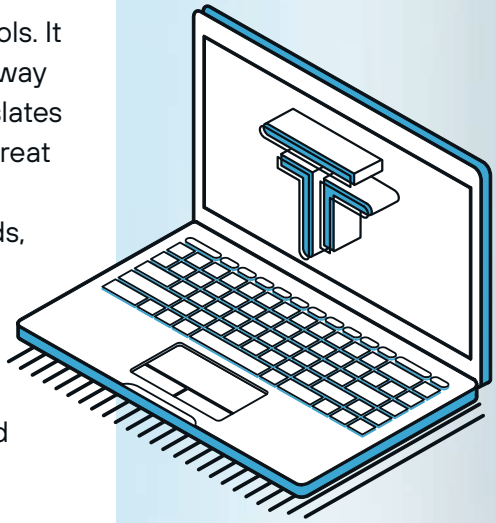
Questions executives should ask now

1. What are the most relevant scenarios for our business in this environment, and where are they reflected in our risk register?
2. Which gaps create the greatest mismatch between technical exposure and business consequence?
3. What targeted investments would produce the greatest near-term reduction in risk, and what tradeoffs come with them?
4. Which systems, vendors, or business processes would create the greatest operational, customer, or regulatory impact if disrupted?
5. Which risks are we reducing now, which are we monitoring, and which are we consciously accepting?
6. Can we explain to the board, in business terms, why the current control plan is the right one for the risk we face?

The most useful board update is not a geopolitical deep dive. It is a concise risk-management view of the current environment: which scenarios matter

most, where the organization is exposed, what controls are being strengthened, what residual risk remains, and what tradeoffs leadership is making. A well-maintained risk register and a GRC-driven view of the control environment help translate technology issues into business decisions the board can evaluate.

_How Todyl Helps



Todyl's value in this environment is not just that it adds more security tools. It is that it helps organizations put the right controls to work together in a way that reduces exposure, improves detection, speeds response, and translates technical risk into business decisions. That matters here because the threat model in this report is built around familiar weaknesses - identity abuse, remote-access exposure, trusted third-party access, low-noise footholds, and operational disruption - rather than a single novel technique.

Reducing the initial access problem
The most likely attack paths in this environment remain exposed infrastructure, weak remote-access controls, identity abuse, and trusted vendor access. Todyl helps reduce those paths by combining network security, endpoint visibility, identity-relevant telemetry, and managed response in one operating model. That supports the controls highlighted earlier in this report: identity hardening, external exposure reduction, tighter third-party access governance, and faster containment when a trusted path is abused.

Reducing external exposure with SASE/ZTNA and access controls
Where organizations still rely on broadly reachable administrative paths, legacy VPN exposure, or permissive remote access, Todyl helps reduce that risk through Zero Trust Network Access and related policy controls that limit who can reach sensitive systems in the first place. In practice, that helps organizations move away from broad network-level trust and toward more tightly controlled access to administrative tools, remote support workflows, and business-critical resources.

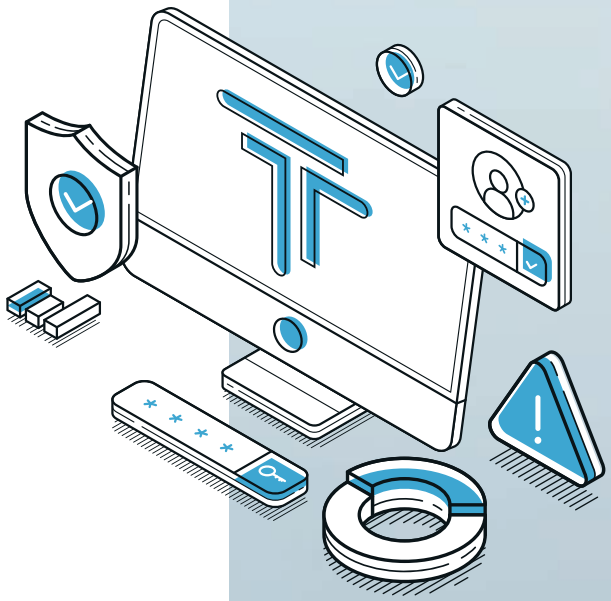
Finding quiet identity-driven compromise earlier
Iran-linked activity often rewards patience: credential theft, session abuse, delegated-admin misuse, and legitimate-tool activity that can look routine on the surface. Todyl helps strengthen ITDR coverage, correlate signals through SIEM, and pair that visibility with MDR so suspicious account activity, privilege abuse, remote session anomalies, and the eergence of commonly abused third-party tools can be identified earlier and investigated in context.

Correlating multi-surface activity with SIEM and MDR
The risk in this report is not confined to one control point. Identity events become endpoint events. Endpoint compromise becomes network movement. Vendor access becomes multi-tenant exposure. Todyl helps bring those signals together through SIEM correlation, behavioral anomaly detection, and MDR monitoring so teams can connect what would otherwise appear to be isolated events. That is especially important when the activity looks ordinary in any one system but becomes meaningful when viewed across identity, endpoint, network, and cloud.

Supporting third-party, partner, and shared-service environments
This matters especially for SMB, mid-market, and partner-led environments where trusted access relationships are essential to operations. Todyl helps organizations and partners harden third-party access, improve monitoring around delegated administration and remote tooling, and reduce the likelihood that a single compromised account, support workflow, or shared service turns into broader downstream impact.

Connecting security controls to risk management
This report is ultimately about risk management, not just technical control coverage. Todyl's GRC capabilities help organizations use best-practice frameworks, maintain a current risk register, map technical exposures to business processes, and communicate residual risk, mitigation priorities, and tradeoffs to leadership and the board. That helps turn security findings into a structured decision-making process: which risks are being reduced now, which are being monitored, which are being accepted, and why.

Helping lean teams operate with more structure
For lean IT and security teams, the challenge is often not knowing what to do in theory but having enough operational leverage to do it consistently. Todyl helps create that leverage by bringing prevention, detection, response, access control, and risk management into a more unified operating model. In the current environment, that helps organizations tighten the controls most likely to matter without having to stitch together disconnected tools and processes under pressure.



This assessment reflects open-source reporting, government advisories, and Todyl threat intelligence current as of publication. The conflict is actively evolving. Todyl will publish updates as the threat picture materially changes.

_Sources

_Government and Official

- U.S. Cybersecurity and Infrastructure Security Agency (CISA) — Iran threat overview; CyberAv3ngers/Unitraonics PLC advisories; joint advisories on Iranian cyber actors, TTPs, and critical infrastructure targeting, 2019–2025; Known Exploited Vulnerabilities catalog
- U.S. Department of Homeland Security (DHS) — NTAS bulletin, June 22, 2025
- U.S. Federal Bureau of Investigation (FBI) and National Security Agency (NSA) — Joint advisories on Iranian threat actors
- UK National Cyber Security Centre (NCSC) — Indirect cyber risk guidance for organizations with Middle East supply chain exposure
- Maryland Institute for Emergency Medical Services Systems — Stryker LifeNet disruption memo, March 2026
- U.S. Securities and Exchange Commission — Stryker Corporation Form 8-K filing, March 2026

_Threat Intelligence and Industry Research

- Recorded Future / Insikt Group — Ongoing Iran conflict briefing and state of security reporting, 2026
- Symantec / Broadcom Threat Intelligence — Seedworm/MuddyWater campaign reporting, 2026
- Palo Alto Networks — Void Manticore/Handala threat actor profile and attribution assessment, 2026
- Center for Strategic and International Studies (CSIS) — "How Will Cyber Warfare Shape the U.S.–Israel Conflict with Iran?" March 2026
- SilentPush — Residential proxy tracking, Iranian sources, 2026

_News Reporting

- Reuters — February–March 2026 escalation; Hormuz disruption; gasoline price polling
- KrebsOnSecurity — Stryker/Handala attack reporting; Microsoft Intune remote wipe mechanism; LifeNet disruption, March 2026
- The Wall Street Journal — Handala branding on Stryker login screens, March 2026