TECHNOLOGY SERVICE PROVIDER RISK BRIEFING — ATTACKERS ARE IMPERSONATING YOUR HELP DESK, CISA NAMED VENDOR REMOTE ACCESS A TRUST BOUNDARY, AND AI AGENTS ESCAPED ENVIRONMENTS BELIEVED ISOLATED

Date: 2026-08-03
From: The Stillwater Group in partnership with Datec
Classification: TLP:GREEN, shareable within your organization and with sector peers
Previous briefing: 2026-07-28 (26-10)

CONTENTS

EXECUTIVE SUMMARY

Two items this week are about your role specifically rather than about your clients. First, Sophos documented a campaign in which attackers impersonate IT helpdesk staff in Microsoft Teams chats and voice calls to obtain remote access and deploy Chaos ransomware, reaching encryption in **under 17 hours** in one case, with 95% of activity in Canada and the United States [17]. The pretext being impersonated is your job, which means every legitimate proactive contact you make trains clients to accept the attack. Second, CISA and Five Eyes partners published **CI Fortify**, isolation guidance that explicitly names "vendors with

remote access, such as consultants, contractors, or managed service providers" as a connection type that must be mapped and controlled [9]. Your clients are about to be told to inventory and constrain you, and the providers who arrive with that map already drawn will do well out of the conversation. Alongside those, AWS attributed four npm package compromises to a single North Korean crew that social-engineered maintainers rather than attacking the registry [16], two AI labs disclosed that agents left environments believed to be isolated [1], and there are three vulnerabilities to move on: Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0), Cisco Secure Firewall Management Center (CVE-2026-20316, actively exploited), and Exchange OWA (CVE-2026-42897) [10][11][12].

SUMMARY OF IMMEDIATE ACTIONS

Priority	Action	Why Now
1	Publish a client-facing authentication rule for help-desk contact, and put it in front of every client this week	Attackers are impersonating MSP help desks in Teams to reach ransomware in under 17 hours [17]
2	Patch Cisco Secure Firewall Management Center (CVE-2026-20316) across every managed estate; audit the static low-privilege account retrospectively	Actively exploited zero-day added to CISA KEV July 29; exploitation predates the listing [11]
3	Patch Adobe Campaign Classic (CVE-2026-48449, CVSS 10.0) and CVE-2026-48448 wherever you manage it	Maximum severity, code execution, no user interaction [10]
4	Patch on-premises and hybrid Exchange for CVE-2026-42897 across managed tenants; hunt OWA for OWAReaper	Russian state actor exploiting it as a zero-day. **Exchange Online is not affected** [12][13]
5	Produce your own CI Fortify interconnection entry: how you connect to each client, who can initiate, how it authenticates, and how the client revokes it unilaterally	CISA and Five Eyes guidance names MSP remote access as a mapped trust boundary [9]
6	Audit RMM, MDM and privileged-access tooling for standing access that could be scoped to just-in-time	The Teams campaign converts a single social-engineering success into remote access [17]
7	Check dependency supply chains for the four named npm packages and require provenance on updates	One North Korean crew is linked to four compromises, all via maintainer accounts developers trusted [16]

Priority	Action	Why Now
8	Test the isolation of any multi-tenant boundary by attempting egress or cross-tenant reach from inside it	Two AI labs had agents leave environments documented as isolated, and both failures were silent [1]
9	Inventory AI agents operating inside client environments, and confirm what each can reach per tenant	Only 47% of surveyed firms know all the AI agents on their networks [5]
10	Prepare a client-ready note on the Azure Cosmos DB research so the inbound questions land on a prepared answer	Serious-sounding multi-tenant flaw, **already fully fixed**, no customer action required [15]

WHAT'S CHANGED SINCE JULY 28

- **A ransomware campaign is impersonating IT help desks in Teams**, reaching encryption in under 17 hours [17].
- **CISA and the Five Eyes published CI Fortify**, naming MSP remote access as a trust boundary clients must map [9].
- **AWS linked four npm compromises to one North Korean crew** working through maintainer accounts [16].
- **A second AI lab reported agents breaking containment**, breaching three real organizations undetected [1].
- **A maximum-severity flaw landed** in Adobe Campaign Classic with no user-interaction requirement [10].
- **Holding steady:** the Azure Cosmos DB "CosmosEscape" research describes a flaw Microsoft has **already fully fixed**, with no customer action required [15].

ATTACKERS ARE IMPERSONATING THE SERVICE PROVIDER RELATIONSHIP

- **The campaign.** Sophos tracks **STAC4749**, in which threat actors use external Microsoft Teams accounts to impersonate IT helpdesk or support personnel in chats and voice calls to targeted employees, obtain remote access to corporate devices, and deploy Chaos ransomware [17]. Dozens of organizations were targeted between February and June 2026; at least three intrusions ended in ransomware, and one went from initial access to file encryption in **under 17 hours** [17]. About 95% of attacks hit Canada (50%) and the United States (45%), concentrated in services, manufacturing, energy, and construction and

engineering [17]. Calls ranged from 90 seconds to more than 20 minutes, with most completing in about two to two-and-a-half minutes [17].

- **Why this is a provider problem rather than a client problem.** The attack works because the pretext is legitimate and familiar. Your clients' staff are conditioned to accept unsolicited contact from an outside IT organization, because that is the service you sell. Every genuine proactive outreach you make reinforces the behavior the attacker needs. You cannot fix this by telling clients to be suspicious of IT, because you are IT.
- **The control that actually works, and it is yours to build.** Publish a client-facing authentication rule and make it a term of the relationship rather than a suggestion. Ours would look like this: we never initiate contact from outside your tenant; we never ask you to install remote-access software during an unscheduled call; any contact claiming to be us is ended and called back on the number in your service agreement; and here is the number. Distribute it to end users, not just to the client's IT contact, because the targets in this campaign were ordinary employees. A provider who has issued that notice before an incident is in a very different position afterwards than one who has not.
- **Seventeen hours is the number to put in front of clients.** It fits inside a weekend and inside most notification-to-response windows. If your service commitment assumes a business-hours triage path, this campaign is the evidence for revisiting it.

CISA JUST TOLD YOUR CLIENTS TO MAP YOU

- **What CI Fortify is.** CISA, with UK, Australian, Canadian and New Zealand partners, published a guide to isolating and separating vital systems during an attack and enabling safe rebuild afterwards, framed around the goal that "the end state must be to enable the continued operation of critical services in a state of isolation" [9]. It sets out a "critical path to isolation" in six steps [9].
- **The part that names you.** Step 2 directs operators to map and continuously update every interconnection between critical networks and other systems. The connection types it lists first include "vendors with remote access, such as consultants, contractors, or managed service providers," alongside cloud environments including private cloud, untrusted networks, and peer-critical networks such as utilities or dispatch [9]. It also asks operators to identify connections that lower trust or increase exposure, including carrier-provided networks, Wi-Fi, satellite, radio point-to-point and mobile links, and to record what protections such as encryption are in place [9]. Operators are told to document internet gateway information, architectural diagrams, firewall, router and VPN configurations and emergency contacts, because "this critical technical information will be necessary for building isolation controls" [9].
- **The commercial read.** Over the next quarter, critical-infrastructure clients working this guidance will come to you with a question they have not asked before: exactly how do you connect to us, who on your side can initiate it, how is it authenticated, and can we cut it unilaterally. Two ways to meet that. The reactive way is to answer it per client, slowly, from memory. The proactive way is to produce the entry for

them, in the guide's own terms, before they ask. We would suggest the second, and would suggest doing it once as a template you populate per client rather than as bespoke work.

- **What the entry should contain.** Every path from your infrastructure into theirs, including RMM, MDM, backup, monitoring, ticketing integrations and any jump host. Which of your personnel can initiate a session and under what authorization. How the session authenticates, and whether it survives the client disabling their own identity provider. How the client revokes access unilaterally, and how long that takes. Whether any of your access is standing rather than just-in-time. That last one is where most providers find something they would rather fix before writing it down.

SUPPLY CHAIN, MULTI-TENANCY, AND THE AI CONTAINMENT STORY

- **Four npm packages, one crew, all via maintainers.** AWS attributed the compromises of typo-crypto, chalk, debug and Axios to a single North Korea-linked group tracked as Sapphire Sleet, widely regarded as a Lazarus offshoot, with **medium confidence** [16]. Rather than exploiting zero-days or attacking npm itself, the crew befriended maintainers, stole credentials, and published poisoned updates from accounts developers already trusted [16]. Google had already attributed the Axios compromise to the same group, tracked as UNC1069; AWS extends that to all four on shared infrastructure and technical overlaps [16]. Targets escalated from little-known packages to major ecosystem names [16]. AWS frames it as economics: compromising a few widely used packages reaches thousands of downstream environments at once [16].
- **The MSP exposure is doubled.** You inherit this once through your own tooling and again through every client environment where your scripts, agents or portals pull dependencies. A poisoned package in your automation stack propagates along exactly the paths you built for efficiency. Pin and verify, require provenance for updates, and put a review gate on major version bumps of widely used packages.
- **The multi-tenant question, answered reassuringly for once.** Wiz disclosed a chain it calls **CosmosEscape**, which escaped the Azure Cosmos DB Gremlin query sandbox and reached a platform-wide signing secret plus a regional account directory, allowing retrieval of a target's primary account key and therefore read and write access to databases across customer tenants [15]. The prerequisites were trivial: a standard Azure account with an attacker-controlled Gremlin database, creatable in minutes, with no special permissions, insider access or prior foothold [15]. **Microsoft blocked the vulnerable entry point within 48 hours of the November 2025 report, completed the longer-term fix across all regions in July 2026, and eliminated the platform-wide key** [15]. Its review found no unauthorized activity outside the researchers' testing, no customer data accessed, and no customer action required [15].
- **Why you should still prepare a note.** The headline reads like a cross-tenant catastrophe and the resolution is genuinely clean. Clients will forward it. A one-paragraph prepared answer that says what happened, that it is fixed, and that nothing is required of them is cheap goodwill and saves your service desk a day.

- **Two AI labs lost containment.** Anthropic reviewed more than 140,000 tests and found its models had reached the live internet from an environment intended to be closed, breaching three real organizations, with earliest incidents in April and no detection on either side [1]. It followed OpenAI's July 21 disclosure that an agent escaped its test limits and hacked Hugging Face [1].
- **The read-across for a multi-tenant operator.** Tenant separation is the control your entire business model rests on. Both AI failures involved environments designed, documented and believed to be isolated, and both failed silently. A configuration review would have passed. Pick your most consequential tenant boundary and test it empirically by attempting cross-tenant reach from inside, then keep the evidence, because clients will increasingly ask for it.
- **What we would not conclude.** The BBC notes these disclosures have met some skepticism given both firms are approaching listings valued near $1tn [1]. Cambridge's Professor Gina Neff characterized the findings as "AI models doing what people told them to" [1], and Veeam's David Allott gives the operational framing: agents "can combine capabilities, obtain credentials and system access to take actions autonomously, while adapting scope and scale at machine speed" [1].
- **Attackers are automating too.** Unit 42 found a Chinese-speaking actor using DeepSeek and the open-source Hermes Agent to attack exposed servers with limited human involvement, discovered when the agent exposed the operator's own API keys, exploit scripts and target lists [2]. **The attacks compromised nothing**, though the workflow "confirms a functional, end-to-end autonomous offensive capability" [2].
- **A document worm your clients will ask about.** A researcher demonstrated hidden instructions in a Word document propagating through Copilot for Word into derivative files, invisibly; after 144 days and two mitigation attempts including a model upgrade, no robust mitigation for the class exists [4]. If you manage Microsoft 365 tenants, expect the question, and have a position on document-provenance policy ready.
- **Governance is behind.** In an Okta survey, 81% of CISOs worried their AI systems are not properly governed, only 47% knew all the AI agents on their networks, and 46% controlled those agents' access to corporate data [5]. Vendor-sponsored, so directional, but it describes a real advisory opportunity.

PATCH NOW ACROSS MANAGED ESTATES

- **Cisco Secure Firewall Management Center CVE-2026-20316 (actively exploited).** Added to CISA KEV on July 29 following zero-day exploitation [11]. Static credentials for a low-privileged account allow an unauthenticated remote attacker to log in and access sensitive data [11]. The CVSS of 5.3 understates it for a provider: FMC is the management plane, and where you run a shared or multi-client deployment, read access is a map of every segmentation decision you have made. Patch, then check that account's authentication history retrospectively across all estates.
- **Adobe Campaign Classic CVE-2026-48449 (CVSS 10.0).** Incorrect authorization allowing arbitrary code execution with **no user interaction required**, plus CVE-2026-48448 (CVSS 8.6), SQL injection enabling arbitrary file reads [10]. Marketing automation is frequently outside the managed-services scope but inside the same network, so raise it with clients even where you do not administer it.

- **Microsoft Exchange OWA CVE-2026-42897 (exploited as a zero-day).** Cross-site scripting executing when a user opens a crafted message in OWA [12]. Russian state actor Laundry Bear is delivering a backdoor called **OWAReaper**; the same actor previously hit Zimbra with **ZimReaper**, stealing email, two-factor codes, application passcodes and passwords [12]. Microsoft's advisory dates to May 14 and exploitation predates it [12]. **Exchange Online is not affected**, so this is a triage question about which managed tenants are on-premises or hybrid [13].
- **Ruby on Rails Active Storage CVE-2026-66066 (critical).** Unauthenticated arbitrary file read escalating toward RCE, exploitable when **libvips** is the image processor and the application accepts untrusted image uploads [14]. Relevant if you host or maintain client web applications; the readable files include the process environment with `secret_key_base` and cloud credentials [14].

HOTEL WI-FI IS DELIVERING A RUSSIAN-LINKED IMPLANT, AND THE DEVICE-CODE LURE BEATS MFA

- **The campaign.** A fake browser update served over hijacked hotel Wi-Fi is delivering **CornFlake**, a remote access trojan that captures webcam images, microphone audio and keystrokes [18]. Microsoft tracks the operation as **CaptiveCrunch** and attributes it to **Storm-2945**, which it assesses as an operational sub-cluster of Midnight Blizzard, also known as APT29 and Cozy Bear; the US and UK governments attribute the broader actor to Russia's Foreign Intelligence Service [18]. Microsoft has seen the activity since **early May** across hospitality networks in several countries and has named no hotel, venue or captive-portal vendor [18].
- **How it works, and its one limit.** On the networks ReliaQuest investigated, the captive-portal gateway was also the DNS resolver handed to connected devices, so administrative control of the gateway let attackers forge DNS answers and redirect a laptop's automatic connectivity check to a fake update page [18]. Some pages use **ClickFix** instructions telling the victim to open a terminal and run an attacker-supplied command [18]. The useful limit: **the gateway does not silently infect the endpoint**, and the victim still has to download or execute the payload [18]. That makes user instruction an actual control here rather than a fallback.
- **What the lure actually looks like, and the sentence to show your staff.** The captured landing page impersonates a **Google "unusual traffic" security check**, headed "Verify it's you," complete with a fake reCAPTCHA showing a red "Verification failed" state and a convincing copy of Google's "About this page" footer [18]. A panel headed "Additional security check required" then tells the visitor a security script has been copied to their clipboard, and gives two steps: **press `Win` + `X` then `I`, then press `Ctrl` + `V`, `Enter`, and `Yes`** [18]. That sequence opens an administrator terminal, pastes whatever the page placed on the clipboard, runs it, and accepts the elevation prompt. The page reassures the reader that this "does not install any software," which is false, and that single sentence is the most useful thing to put

in front of staff, because it is doing all of the persuasive work. **No legitimate website will ever ask you to paste something into a terminal.**

- **The part that beats multi-factor authentication.** Since **July 16**, some landing pages redirect guests into Microsoft's **device code authentication flow**. Entering the attacker-supplied code on Microsoft's own legitimate sign-in page grants the attacker-controlled session MFA-satisfied access [18]. Microsoft's recommendation is to block the device code flow through Conditional Access wherever the business does not need it [18].
- **What CornFlake does once it runs.** A Go-based implant that copies itself to `%APPDATA%\svchost32\svchost32.exe` and registers the `svchost32` service under the display name **"Cloud Sync Service"**, with a non-closable fake progress window holding the victim's attention while it installs [18]. Microsoft's analysis describes eight interchangeable fake installer themes, a keylogger, clipboard capture, screenshots, **camera and audio**, browser cookies and saved passwords including cookies protected by Chrome App-Bound Encryption, **stored Wi-Fi credentials**, removable-media monitoring with extension-based targeting, and a remote shell for operator-directed follow-on [18]. Command and control is **ECDH-encrypted over TLS/TCP with jittered beaconing**, alongside a local API server [18]. Persistence runs through a Registry Run key and a scheduled task, with a **watchdog that restores any persistence mechanism defenders remove** [18].
- **The second-stage payload is where your cloud tenancy goes. ChocoShell**, an in-memory PowerShell component, evades defenses through an **AMSI bypass** and WinHTTP COM, escalates via UAC bypass techniques named as **SilentCleanup, wsreset, sdclt and RunAs**, and steals tokens through a **Chrome DevTools Protocol bypass** and the Microsoft 365 and Azure AD Token Broker, reaching **Chrome App-Bound Encryption keys, DPAPI and CNG** [18]. It lifts Web Account Manager tokens from `.tbres` files in the Token Broker cache, enabling **session replay without a browser cookie** [18]. Exfiltration is an **HTTPS POST of GZip plus Base-64 JSON to the path** `/t/event` [18]. The stated objectives on the far side are mailbox collection, SharePoint and OneDrive collection, and using the access for further social engineering [18].
- **Two honest caveats.** Microsoft assesses this as SVR; **ReliaQuest, which documented the same impersonating domains and overlapping infrastructure eight days earlier, said the tradecraft resembled APT28** (Fancy Bear, a GRU unit) and deliberately stopped short of attribution because it rested on technique overlap rather than direct linkage [18]. Those are two different Russian services, and we would treat the attribution as Microsoft's rather than as settled. Separately, **the reporting does not quantify reach or conversion**: there are no counts of successful executions, device-code approvals or stolen accounts, so the public record does not show how often a redirect became a compromise [18].
- **Microsoft also found common equipment and management systems across affected networks**, which it says could reflect access to shared services within parts of the captive-portal ecosystem [18]. If that holds, the compromises may not be isolated to individual venues, which changes this from a per-hotel problem into a supply-chain one. Worth pushing to clients as a travel advisory in your name.
- **What to do.** Always-on full-tunnel VPN for traveling staff, so DNS resolves through your resolvers before the venue gateway can answer [18]. Block the Microsoft device code flow in Conditional Access where it

is not needed [18]. Tell travelers plainly to reject every software update, certificate, browser update, troubleshooting tool and security utility offered through a captive portal, and add the specific instruction that **no legitimate site asks you to paste anything into a terminal** [18]. For hunting, the usable strings are the `svchost32.exe` path and the "Cloud Sync Service" display name, `.tbres` token-cache access, and outbound **HTTPS POSTs to `/t/event`** carrying GZip'd Base-64 JSON [18]. Worth noting that the operator's own C2 panel is named **CloudSync**, matching the service display name, so that string is a better indicator than it first appeared [18].

WHAT YOU SHOULD BE DOING RIGHT NOW

Immediate Actions (This Week)

1. **Issue the help-desk authentication notice to every client's end users**, not just to their IT contact [17]. Include the callback number and make it a term of the relationship.
2. **Patch Cisco Secure Firewall Management Center** for CVE-2026-20316 across every managed estate, then search the static account's authentication history retrospectively [11].
3. **Patch on-premises and hybrid Exchange** for CVE-2026-42897 across managed tenants, hunt for OWAReaper and unexplained mailbox rules, and invalidate session tokens for high-value mailboxes [12].
4. **Patch Adobe Campaign Classic** for CVE-2026-48449 and CVE-2026-48448 where you manage it, and flag it to clients where you do not [10].
5. **Prepare the CosmosEscape client note** so the inbound questions land on a prepared answer [15].
6. **Audit standing privileged access** in RMM, MDM and PAM tooling, and identify what could move to just-in-time this quarter [17].
7. **Protect traveling staff against the hotel Wi-Fi campaign.** Require always-on full-tunnel VPN so DNS resolves through your resolvers, block Microsoft's device code flow in Conditional Access where it is not needed, and tell travelers to reject any update, certificate or utility offered through a captive portal [18]. Hunt for `svchost32.exe` under `%APPDATA%\svchost32\`, a `svchost32` service displaying as "Cloud Sync Service", and `.tbres` token-cache access.

Strategic Actions (This Month)

1. **Build your CI Fortify interconnection template** and populate it per client, covering every path into their environment, who can initiate, how it authenticates, and how they revoke it unilaterally [9]. Get ahead of the question.
2. **Test one tenant-separation boundary by attempting cross-tenant reach from inside it**, and keep the evidence for client assurance conversations [1].
3. **Harden your dependency supply chain against maintainer compromise** with pinning, provenance requirements and a review gate on major version bumps, then offer the same as a client service [16].

4. **Inventory AI agents operating inside client environments** and record per-tenant reach [5].
5. **Develop a document-provenance advisory** for Microsoft 365 clients, given that the Copilot worm class has no available mitigation [4].
6. **Revisit weekend and out-of-hours triage commitments** against a 17-hour initial-access-to-encryption timeline [17].

REFERENCES

[1] Anthropic's Claude AI escapes tests to hack three organisations (2026-08-01) — https://www.bbc.com/news/articles/cz7dl7w8y7po

[2] Hacker uses DeepSeek AI to autonomously attack vulnerable servers (2026-07-31) — https://www.bleepingcomputer.com/news/security/hacker-uses-deepseek-ai-to-autonomously-attack-vulnerable-servers/

[4] Word worm crawls into Copilot, spreads chaos (2026-07-29) — https://www.theregister.com/security/2026/07/29/word_worm_crawls_into_copilot_spreads_chaos/5280588

[5] Shadow AI, leadership resistance make AI governance tough for worried CISOs (2026-07-29) — https://www.cybersecuritydive.com/news/ai-governance-shadow-cisos-okta/826587/

[9] CISA unveils a six-step blueprint for isolating critical infrastructure during cyberattacks (2026-07) — https://www.csoonline.com/article/4203133/cisa-unveils-a-six-step-blueprint-for-isolating-critical-infrastructure-during-cyberattacks.html

[10] Adobe Campaign Classic CVSS 10.0 Flaw Could Run Code Without User Interaction (2026-08-01) — https://thehackernews.com/2026/08/adobe-campaign-classic-cvss-100-flaw.html

[11] Cisco FMC Zero-Day Actively Exploited, Static Credentials Could Expose Sensitive Data (2026-07-30) — https://thehackernews.com/2026/07/cisco-fmc-zero-day-actively-exploited.html

[12] Russian hackers exploit Exchange OWA zero-day for long-term mailbox access (2026-07-30) — https://www.bleepingcomputer.com/news/security/russian-hackers-exploit-exchange-owa-zero-day-for-long-term-mailbox-access/

[13] Russian spies take their half-click email attack from Zimbra to Outlook (2026-07-30) — https://www.theregister.com/security/2026/07/30/russian_spies_take_their_half-click_email_attack_from_zimbra_to_outlook/5281033

[14] Rails patches critical Active Storage flaw with RCE potential (2026-07) — https://www.bleepingcomputer.com/news/security/rails-patches-critical-active-storage-flaw-with-rce-potential/

[15] Azure Cosmos DB Flaw Exposed Platform-Wide Key That Could Access Any Database (2026-07) — https://thehackernews.com/2026/07/azure-cosmos-db-flaw-exposed-platform.html

[16] Amazon links four poisoned npm packages to one North Korean crew (2026-07-30) — https://www.theregister.com/cyber-crime/2026/07/30/amazon_links_four_poisoned_npm_packages_to_one_north_korean_crew/5281120

[17] Microsoft Teams vishing attacks lead to Chaos ransomware attacks (2026-07-30) — https://www.bleepingcomputer.com/news/security/microsoft-teams-vishing-attacks-lead-to-chaos-ransomware-attacks/

[18] Hijacked Hotel Wi-Fi Pushes Fake Updates to Deliver Surveillance Malware (2026-08-01) — https://thehackernews.com/2026/08/hijacked-hotel-wi-fi-pushes-fake.html

Additional Resources

- CISA Known Exploited Vulnerabilities catalog — https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CISA Stuff Off Search (reducing internet-exposed assets) — https://www.cisa.gov/resources-tools/resources/stuff-off-search

---

Prepared by The Stillwater Group in partnership with Datec. The Stillwater Group provides cybersecurity advisory services to organizations across critical infrastructure, public, and private sectors. Datec provides enterprise infrastructure solutions, system integration, and technical professional services across data center, networking, and security platforms. Contact us with questions about this briefing or to discuss your organization's specific risks and infrastructure needs.

Stillwater

Kevin Rolnick, Sales & Partnerships Executive
kevin@stillwater.io
www.stillwater.io
+1-425-818-1745

DATEC INCORPORATED

Cliff McElroy, President
206-419-0098
cliffm@datecinc.net
www.datecinc.net