Genesis

A CISO's Guide to Vendor, SaaS, and Supply Chain Security

Top 10 Third Party Attack Vectors of 2025

Whitepaper

Syed Amoz
Khalifa Al Shehhi

Content Index

Executive Summary

Third-party cyber incidents have become one of the most significant risk multipliers for modern enterprises. Today's organizations rely on a web of suppliers, SaaS providers, contractors, and managed service partners, each representing a potential pathway for attackers. Nearly *30% of data breaches involve third-party suppliers and vendors (Verizon DBIR 2025)*, while *35.5% of breaches in 2024 were vendor-related (SecurityScorecard 2025)*, clear evidence that ecosystem security must be prioritized.

This whitepaper provides CISOs and security leaders with an advanced guide to protecting the "outside perimeter." It explores the 10 most critical vectors exploited by attackers, from stolen vendor credentials and misused remote access to SaaS/OAuth exploits, vulnerable APIs, and software supply chain compromises. For each vector, you'll find:

A. **How it Happens**: Explains the weakness and how attackers typically exploit it to gain access.
B. **Attacker Tactics**: Describes the main steps attackers follow entry to expand control or steal data.
C. **Real-World Examples**: Highlights past incidents that show this attack vector in action.
D. **Risk Indicators**: Lists the key warning signs and suspicious patterns security teams should monitor.
E. **Business Impact**: Outlines the financial, operational, and reputational consequences if exploited.

Finally, we provide strategic recommendations for mitigating these risks through zero-trust principles, continuous third-party monitoring, SaaS governance, and actionable incident playbooks.

Third-Party Threat Landscape

The concept of a "perimeter" has fundamentally changed. Ten years ago, defending the corporate network meant locking down a well-defined set of on-premises servers and user endpoints, with firewalls and edge defence's forming a clear boundary. Today, both the concept and the practice have shifted: the perimeter is no longer a fixed line around corporate infrastructure but a fluid set of identities, cloud environments, SaaS platforms, and third-party connections. This interconnected ecosystem has effectively dissolved the traditional perimeter, and attackers have taken notice.

Rising Third Party Breaches

High-profile breaches have demonstrated how third-party connections can become an attacker's best friend:

- **Target (2013):** Attackers used an HVAC vendor's VPN credentials to plant malware on POS systems, compromising 40M credit card numbers.
- **SolarWinds (2020):** A supply chain attack embedded malware in SolarWinds Orion updates, impacting 18,000+ customers worldwide.
- **MOVEit Exploits (2023):** Ransomware gangs exploited a zero-day vulnerability in Progress MOVEit file transfer software, leading to breaches at hundreds of organizations.
- **Salesforce OAuth Campaign (2025):** Over 700 organizations, including Allianz, Google, and Dell, were impacted after attackers tricked users into approving malicious OAuth apps that siphoned Salesforce data and cloud tokens.

What's at stake?

- **Financial Risk:** The average cost of a data breach was USD 4.88 million among organizations between March 2023 and February 2024, the highest in IBM's annual *Cost of a Data Breach Report*.
- **Regulatory Exposure:** Frameworks like NIS2, DORA, GDPR, and PCI-DSS hold organizations accountable for vendor security lapses, not just their own.
- **Reputational Damage:** Customers often see no distinction between "your system" and "your vendor's system" - meaning you bear the reputational fallout.
- **Operational Disruption:** A compromised SaaS provider or MSP can halt critical services across multiple business units at once.

Overview: The 10 Critical Third-Party Attack Vectors

Third-party breaches rarely happen all at once. They usually begin with a small weakness could be a leaked password, an unmonitored remote connection, or a careless integration. From there, attackers look for ways to move further, turning a single slip into a full-scale incident.

#	Attack Vector	Briefly
1	Compromised Credentials	Stolen vendor logins used to access client systems.
2	Remote Access Misuse	Over-permitted VPN/RDP/MSP access exploited for footholds.
3	SaaS & OAuth Exploits	Malicious apps/token abuse to siphon data from SaaS.
4	Vulnerable APIs	Weak/exposed partner APIs leveraged to enumerate or steal data.
5	Supply Chain Software Compromise	Tainted updates/components bypass controls at scale.
6	Email & Phishing (Vendor Abuse)	Vendor mailbox takeovers and spoofing drive fraud and malware.
7	Compromised Vendor Endpoints	Infected contractor devices become trusted pivot points.
8	Insider Threats via Vendors	Malicious/negligent third-party users misuse legitimate access.
9	Shadow IT & Unvetted Tools	Unsanctioned apps integrate data without governance or logging.
10	Exposed Web Portals & Interfaces	Internet-facing partner portals exploited for admin access.

The ten attack vectors outlined in this whitepaper capture these patterns of compromise. Each vector shows both how an attack often starts and how it typically progresses (transit) once inside the ecosystem. Together, they provide a clear map of how external weaknesses can evolve into enterprise-level threats.

1. Compromised Credentials (Third-Party Logins)

A. How It Happens

1. Credential Harvesting: Threat actors gather vendor or contractor usernames and passwords using phishing campaigns, infostealer malware (keyloggers, Redline, Vidar), or by purchasing leaked credentials from dark-web marketplaces.
2. Credential Testing: Attackers try those credentials against vendor VPN portals, support tools, or client-facing systems. If MFA isn't enforced (or if it's bypass able via "MFA fatigue" or SIM-swap attacks), a single password can provide direct access.
3. Impersonation & Access: Once inside, the attacker appears as a legitimate vendor user, bypassing many perimeter defenses and trust boundaries. This gives them immediate access to client networks, often with partner-level privileges.

B. Attacker Tactics

- **Exfiltrate Data**: Download customer records, IP, financial data, or internal documentation.
- **Create Persistence**: Add new accounts, API keys, or OAuth tokens to maintain long-term access.
- **Move Laterally**: Use the compromised account as a foothold to explore other parts of the network, escalate privileges, or drop malware (ransomware, remote shells).
- **Blend In**: Because the login came from a "trusted" third-party account, SOC teams may not immediately flag it as suspicious, buying the attacker valuable time.

C. Real-World Examples

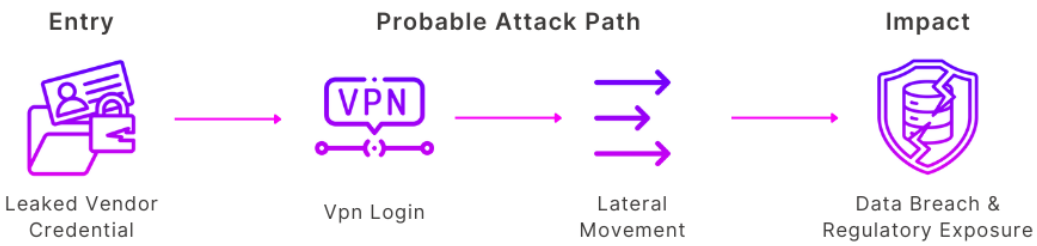
- **DoorDash (2022)**: Hackers used stolen vendor credentials to access internal tools, exposing customer payment data.
- **Home Depot (2014)**: Attackers infiltrated using a supplier's credentials, then deployed custom POS malware that captured 56 million payment cards.
- **Target (2013)**: Breach started with an HVAC contractor's VPN credentials (stolen via malware on the vendor PC), leading to the theft of 40 million credit card numbers.

D. Risk Signals to Monitor

- **Odd Login Patterns:** Logins from geographies unrelated to the vendor, outside business hours, or on weekends.
- **Credential Stuffing Indicators:** Multiple failed logins attempts or lockouts on supplier accounts.
- **Dark Web Exposure:** Vendor credentials appearing in breach databases or underground forums.
- **MFA Gaps:** Authentication events that bypass MFA or show repeated push notifications (MFA fatigue).

E. Business Impact

- **Data Loss**: Customer PII, financial data, source code.
- **Regulatory Penalties**: Non-compliance with GDPR, HIPAA, PCI-DSS due to third-party lapses.
- **Reputation Damage**: Customers lose trust when they hear a "supplier login" led to the breach.
- **Incident Response Complexity**: Coordination with vendors slows down containment and remediation efforts.



2. Remote Access Misuse (Third-Party Connections)

A. How It Happens

1. **Credential or Session Theft**: Threat actors harvest vendor VPN credentials via phishing, malware, or dark-web purchase. In other cases, they steal an active session token from an already logged-in vendor machine (bypassing MFA altogether).
2. **Exploiting Weak Remote Access Tech**: Attackers scan for unpatched vulnerabilities in remote access software (Pulse Secure, Citrix ADC, Fortinet SSL VPN, Kaseya VSA, etc.). Successful exploitation gives them direct entry without needing credentials.
3. **Foothold Behind the Firewall**: Once connected, the attacker's traffic looks like legitimate vendor activity. They inherit whatever permissions that vendor account has, and if access controls are loose, they can reach critical systems.
4. **Lateral Movement & Escalation**: Using tools like Bloodhound, Mimikatz, or Cobalt Strike, attackers pivot inside the network, escalate privileges, and spread to high-value assets.

B. Attacker Tactics

- **Privilege Escalation**: Capturing hashes, exploiting AD misconfigurations to gain admin rights.
- **Data Theft**: Copying sensitive files over the same remote channel used for support.
- **Ransomware Deployment**: Launching mass encryption across the environment (common with REvil, LockBit).
- **Tool Hijacking**: Using legitimate remote management tools (RMMs) to disable security controls and push malicious payloads to multiple machines simultaneously.

C. Real-World Examples

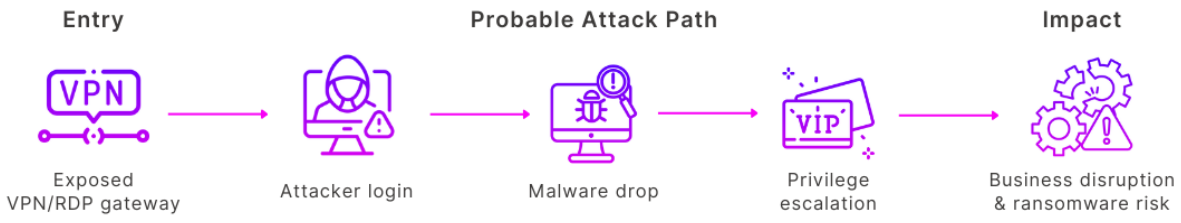
- **Target (2013)**: Attackers used an HVAC contractor's credentials on Target's vendor portal, traversed to POS networks, and installed card-stealing malware, resulting in the theft of 40M payment cards.
- **Kaseya VSA (2021)**: The REvil ransomware gang exploited a zero-day in Kaseya's remote management software used by MSPs worldwide. By compromising one central tool, they pushed ransomware to 1,000+ downstream companies, forcing hundreds of Coop supermarkets in Sweden to shut down for days.
- **Citrix ADC Exploits (2019–2020)**: Multiple ransomware groups leveraged CVE-2019-19781 to gain remote footholds in corporate networks, later deploying Ryuk/Conti ransomware.

D. Risk Signals to Monitor

- **Unusual Remote Sessions:** Vendor VPN logins outside of approved maintenance windows, from IPs not tied to vendor regions.
- **Security Gaps:** Vendor accounts without MFA, dormant accounts that remain active, or shared accounts used by multiple vendor staff
- **Remote Tool Abuse:** Sudden spikes in file transfers, scripted commands pushed through remote management suites, or new agent installs.
- **Compromised Vendor Alerts:** If EDR/AV on jump hosts detect malware from a vendor system, treat it as a possible pivot point.

E. Business Impact

- **Enterprise-Wide Compromise:** Attackers can reach crown-jewel systems, deploy ransomware, or steal intellectual property.
- **Operational Disruption:** POS terminals, production lines, or IT management consoles can be shut down, halting business operations.
- **Regulatory & Legal Fallout:** Stakeholders may question why vendor access was not segmented or protected with MFA, leading to reputational damage and possible fines.
- **High Blast Radius:** In MSP or shared-tool scenarios, one compromise can ripple across dozens or hundreds of client networks simultaneously.



3. SaaS Vendor Compromise (Upstream Breach)

A. How It Happens

1. **Initial Access at the Vendor:** Attackers exploit the SaaS provider's weak spot, unpatched servers, misconfigured cloud storage, stolen admin credentials, or insider collusion.
2. **Pivot to Customer Data:** Once inside the vendor, they gain access to customer data stores or admin consoles. Successful exploitation gives them direct entry without needing credentials.
3. **Abuse of Trust Relationships:** Attackers may abuse integrations, OAuth tokens, SAML assertions, API keys, to impersonate customers or siphon their data without directly touching your systems.
4. **Optional Stealth:** Because SaaS access is "legitimate," attackers often stay hidden longer, using normal APIs to exfiltrate data.

B. Attacker Tactics

OAuth Consent Phishing: Creating a malicious app that looks legitimate, tricking employees into granting API access.
Admin Account Takeover: Using stolen credentials or social engineering (e.g., SIM swaps) to take control of vendor support/admin accounts.
CI/CD or Supply Chain Abuse: Inserting backdoors into vendor code or updates.
API Token Theft: Capturing and replaying customer tokens for persistent access.

C. Real-World Examples

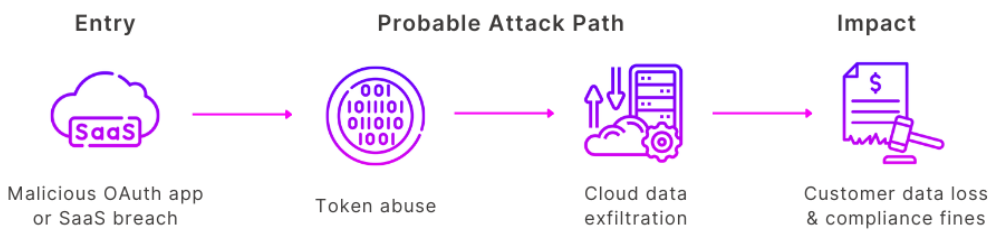
- **Salesforce OAuth Campaign (2025):** Hundreds of organizations (including Allianz and Google) were breached when employees authorized malicious Salesforce apps, granting attackers API access and even exposing cloud tokens like AWS and Snowflake keys.
- **PowerSchool Breach (2024):** Attackers compromised PowerSchool's SaaS environment, exposing millions of student records across multiple districts.
- **Okta (2022):** LAPSUS$ used a compromised third-party support engineer account to gain access to Okta's customer data.
- **Uber/Teqtivity (2022):** Breach of a vendor asset-tracking SaaS leaked data for 77,000 employees, which attackers then used to pivot to DoorDash.

D. Business Impact

- **Loss of Data Confidentiality:** Sensitive CRM data, financial records, or employee information can be leaked in bulk.
- **Service Downtime:** Vendors may shut down platforms to contain the breach, halting your operations.
- **Regulatory Fallout:** GDPR, HIPAA, or SOC 2 compliance issues trigger mandatory disclosures and fines.
- **Reputation Risk:** Clients see it as your failure, regardless of whose systems were breached.

C. Risk Signals to Monitor

- **Vendor Breach Alerts:** Watch for vendor disclosures, industry ISAC reports, or chatter on threat intel channels.
- **Tenant Anomalies:** New OAuth apps, unfamiliar admins, or bulk downloads of data.
- **Unusual API Calls:** Large exports, odd query patterns, or access from unusual regions.
- **Multiple Clients Impacted:** Peers reporting suspicious activity often signals a shared vendor breach.



4. Vulnerable APIs (Partner and Integration Weakness)

A. How It Happens

1. **Unauthenticated Endpoints:** An API returns sensitive data without requiring authentication (Optus 2022 breach).
2. **Broken Object Level Authorization (BOLA):** Attackers manipulate IDs in API calls to view or modify data belonging to other customers (classic IDOR).
3. **Excessive Data Exposure:** API responses include unnecessary fields (e.g., PII, keys).
4. **Reverse Engineering:** Attackers decompile mobile apps or scrape docs to discover hidden API endpoints, then automate abuse at scale.

B. Attacker Tactics

• **Fuzzing & Enumeration:** Using tools like ffuf, Burp Intruder, and Postman collections to test endpoints.
• **Token Reuse:** Exploiting long-lived API tokens found in repos or logs.
• **Mass Harvesting:** Writing scripts to paginate through all available records.
• **Business Logic Abuse:** Exploiting workflows (e.g., refund APIs, coupon codes) in ways not intended by developers.

C. Real-World Examples

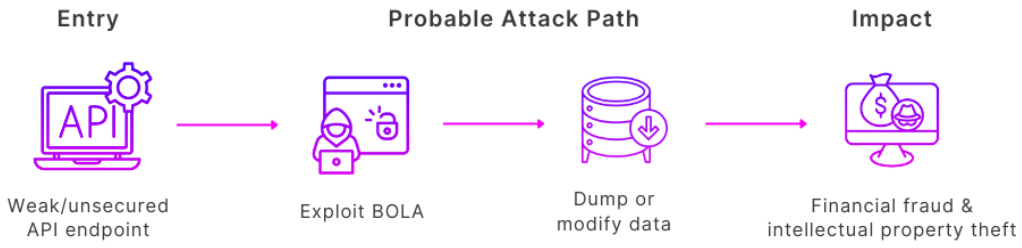
• **Facebook (2021):** Vulnerability let attackers scrape 533M phone numbers via an API feature.
• **LinkedIn (2021):** API abuse enabled scraping of 700M user profiles.
• **Dell (2024):** Partner portal API flaw leaked 49M customer records, including order histories.
• **Optus (2022):** An open, unauthenticated API endpoint exposed 10M Australian customer records.
• **CenturyLink (2019):** Misconfigured notification API left 2.8M customer records exposed.

D. Business Impact

• **Silent Data Breach:** Attackers can siphon millions of records before detection.
• **Data Manipulation:** Potential for financial fraud (changing invoices, payouts).
• **Compliance Exposure:** Failure to secure APIs can violate PCI-DSS, GDPR, and sector regulations.
• **Ecosystem Risk:** When a shared partner API is breached, multiple clients are simultaneously impacted , leading to coordinated disclosure events and loss of trust.

C. Risk Signals to Monitor

• **Anomalous API Use:** Sudden spikes in query volume or record enumeration from a single token.
• **Unexpected Error Patterns:** Surge in 404/403 responses can indicate probing.
• **Third-Party Key Leaks:** Monitor GitHub and public repos for exposed keys.
• **Framework CVEs:** Stay ahead of vulnerabilities in API gateways, backend frameworks, or auth libraries.



5. Malicious Software Components (Supply Chain Attacks)

A. How It Happens

1. **Compromise of the Upstream Source:** Attackers infiltrate a software vendor's build system, CI/CD pipeline, or update servers.
2. **Injection of Malicious Code:** They insert backdoors, remote access trojans, or data exfiltration logic into legitimate code.
3. **Signed & Shipped:** Because the tainted software is signed and distributed by a trusted vendor, it bypasses most security controls (AV, EDR, code-signing verification).
4. **Execution in Target Environment:** As soon as customers apply the update or install the package, the malicious code executes with the privileges of the trusted software, often SYSTEM or root level.

B. Attacker Tactics

• **Build System Breach:** Compromising CI/CD servers (e.g., Jenkins, TeamCity) to insert malware during compilation.
• **Repository Poisoning:** Uploading trojanized open-source packages or hijacking a popular maintainer account.
• **Update Channel Hijack:** Gaining access to vendor update servers or signing keys, distributing malicious updates to thousands of clients.
• **Firmware/Driver Backdoors:** Inserting malicious code in device firmware that loads early in the boot process.

C. Real-World Examples

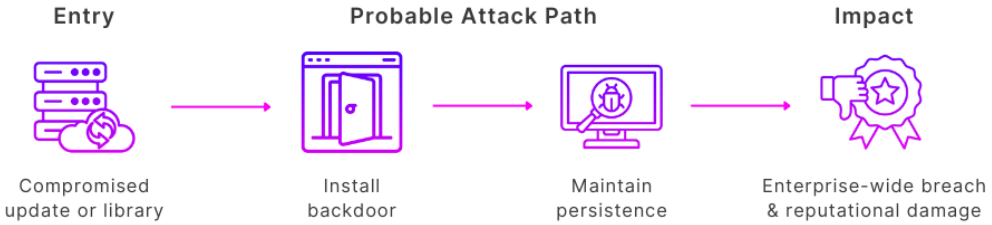
- **SolarWinds Orion (2020):** Attackers inserted a backdoor ("SUNBURST") into Orion updates, which were downloaded by ~18,000 customers. This granted nation-state actors access to Fortune 500 and U.S. government networks.
- **MOVEit Transfer Exploits (2023):** The Clop ransomware group used SQL injection zero-days to compromise hundreds of organizations simultaneously by exploiting a widely used file-transfer tool.
- **Cleo File Transfer (2024):** Zero-day vulnerabilities allowed breaches at 60+ enterprises including Adidas and Kellogg's.

D. Business Impact

- **Mass Data Theft:** SolarWinds victims had email, IP, and secrets stolen.
- **Operational Disruption:** NotPetya forced global shipping giant Maersk to reinstall 45,000 PCs and 4,000 servers from scratch.
- **Financial & Regulatory Fallout:** Equifax's breach (caused by an unpatched open-source web component) cost $1.4B in settlements.
- **Loss of Trust:** Customers lose confidence in both you and your vendors; IT teams may hesitate to apply critical updates, ironically making future breaches more likely.

E. Risk Signals to Monitor

- **Post-Update Anomalies:** Systems contacting unknown IPs/domains after a software update, sudden creation of scheduled tasks, or new admin accounts appearing.
- **Integrity Failures:** Hash or digital signature mismatches on downloaded software.
- **Threat Intel Alerts:** Public advisories that a library, package, or vendor tool has been backdoored.
- **Community Chatter:** Multiple organizations reporting identical weird behaviour (e.g., errors, C2 callbacks) after installing the same update, often the first clue of a supply chain event.



6. Email & Phishing Vectors via Third Parties

A. How It Happens

1. **Impersonation (Spoofing):** Attackers register lookalike domains (vendor-support.co vs. vendor-support.com) or use display-name spoofing to impersonate a supplier. The message may request a password reset, payment approval, or file download, and recipients are more likely to trust it because it references a real partner or vendor relationship.
2. **Vendor Email Compromise (VEC):** attackers break into a vendor's mailbox (stolen creds, malware, brute force) and send legitimate-looking emails that bypass email auth and filters. After access, they are typically:
    - Install info-stealers or ransomware.
    - Run BEC scams (e.g., change invoice bank details).
    - Steal VPN/SSO creds for deeper access.

B. Attacker Tactics

• **Lookalike Domains:** Using typosquatted domains (detected with tools like DNSTwist).
• **Credential Phishing Pages:** Fake login portals (O365, DocuSign) to harvest credentials.
• **Thread Hijacking:** Replying to existing email threads from a compromised vendor account to add legitimacy.
• **Malware Delivery:** Sending malicious macros, PDFs, or links disguised as vendor contracts or shipping documents.

C. Real-World Examples

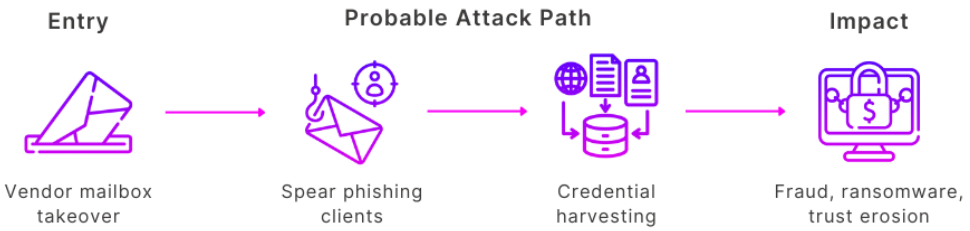
• **Marks & Spencer / Co-op Breach (2025):** Started with phishing at their shared delivery provider. Attackers stole vendor credentials, accessed order data for millions of customers, and later deployed ransomware , forcing M&S to take systems offline.
• **Toyota Boshoku (2019):** Lost $37 million after attackers spoofed a partner's email and tricked finance staff into wiring funds.
• **Ubiquiti Networks (2015):** Lost ~$46 million to a vendor impersonation BEC scam that exploited trusted supplier relationships.

D. Business Impact

• **Direct Financial Loss:** Fraudulent invoice payments can cost hundreds of thousands or millions , recovery is often difficult.
• **Data Breaches & Ransomware:** Phishing can be the first step to credential theft, VPN compromise, or ransomware deployment.
• **Customer Trust Erosion:** If your vendor's hacked email account sends malware to your clients, your brand takes the hit.
• **Operational Disruption:** Email compromise may require global password resets, DMARC policy tightening, and mass incident response efforts , which can paralyze business temporarily.

E. Risk Signals to Monitor

• **Vendor Email Anomalies:** Unexpected requests for payments, credential resets, or urgent actions.
• **Lookalike Domains:** External emails from domains similar to your vendors but with slight variations.
• **Multiple Employees Targeted:** Several staff receive the same suspicious vendor email , may indicate a phishing campaign.
• **Complaints or Bounce backs:** Vendors or clients report "your company sent phishing emails," which could indicate account compromise.
• **O365 / Email Logs:** Logins from unusual geographies, multiple failed login attempts, or token refresh activity for vendor-linked accounts.



7. Compromised Endpoints

A. How It Happens

1. Initial Compromise of the Device: The vendor employee clicks a phishing link, downloads malware, or gets infected by a drive-by download or USB-borne worm.
2. Credential Harvesting: Info-stealer malware collects VPN credentials, SSH keys, or session cookies from the device and sends them to the attacker.
3. Network Access: When the vendor reconnects (or the attacker reuses the stolen credentials), the malicious traffic is seen as coming from a legitimate, trusted device or user.
4. Pivoting & Lateral Movement: Malware on the device can directly scan internal subnets, install additional payloads, or propagate into your network.

B. Attacker Tactics

• **Infostealers:** Malware families like Redline or Raccoon grab browser-stored passwords and VPN creds.
• **RATs (Remote Access Trojans):** Tools like Remcos or Quasar RAT allow attackers to operate the vendor's device as if sitting in front of it.
• **Malicious USB Payloads:** Dropped payloads (Rubber Ducky scripts, autorun malware) on devices that contractors later connect to internal machines.
• **Living-off-the-Land:** Using the vendor's legitimate admin tools (PowerShell, PsExec) to spread silently once inside.

C. Real-World Examples

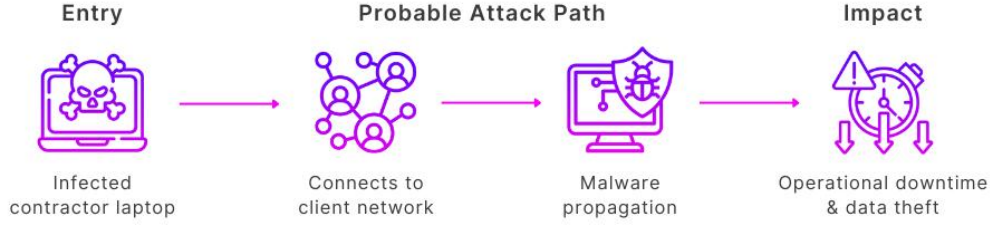
• **Hy-Vee Breach (2025):** Stormes Group used infostealer malware to capture credentials from a vendor endpoint, then accessed Hy-Vee's internal Confluence and Jira, exfiltrating 53 GB of sensitive documentation.
• **Target (2013):** HVAC vendor's PC was likely infected first, leaking VPN credentials that let attackers reach Target's POS network.
• **DoorDash (2022):** Attackers exploited a compromised third-party support provider's device, stealing DoorDash internal tool credentials and customer data.

D. Business Impact

• **Silent Intrusion:** Because vendor devices often aren't covered by your SOC, malware activity may go unnoticed for weeks, allowing long dwell times.
• **Cascade Breaches:** If a vendor works with multiple clients (e.g. MSPs), the same compromised device may be used to breach many organizations at once.
• **Regulatory & Legal Risk:** Explaining to regulators that "our contractor's laptop was infected" may not satisfy compliance obligations , you're still accountable for resulting data exposure.
• **Business Disruption:** If the compromised device operates critical infrastructure or manages part of your IT, its compromise can lead to outages, ransomware events, or halted operations.

E. Risk Signals to Monitor

• **Device Posture Failures:** Endpoint detection showing missing patches, AV disabled, or suspicious processes on vendor laptops.
• **Abnormal Network Behaviour:** Contractor machines that normally connect to a single server suddenly scanning multiple subnets.
• **Correlated Alerts:** Multiple EDR or SIEM alerts tied to the same vendor account or IP within a short period.
• **Lost/Stolen Device Reports:** Treat vendor notifications of stolen laptops or compromised machines as high-risk until access is revoked and credentials are rotated.



8. Insider Threats via Third Parties

A. How It Happens

When outsourcing or integrating partners, you expand your insider threat surface. A "third-party insider" is anyone off-payroll with system access, contractors, consultants, MSPs, call centre staff, or vendor engineers.

Threat types:

- **Malicious**: Deliberately steals, sabotages, or leaks.
- **Compromised**: Bribed, blackmailed, or recruited to plant malware or steal data.
- **Careless**: Accidentally leaks, misconfigures, or loses sensitive assets.
  These users often bypass corporate controls due to weaker checks, less oversight, and remote access.

B. Attacker Tactics

• **Credential Abuse:** Using legitimate vendor logins to copy data, create backdoor accounts, or disable security controls.
• **Privilege Escalation:** Attempting to gain higher access rights or abuse shared admin accounts that aren't tightly monitored.
• **Social Engineering:** Recruiting or bribing vendor staff to hand over credentials or install malicious software.
• **Data Smuggling:** Copying sensitive data to USB drives, personal cloud accounts, or emailing it externally.
• **Negligence:** Misconfiguring permissions (e.g., setting a cloud bucket public) or sharing screenshots/files that contain secrets.

C. Real-World Examples

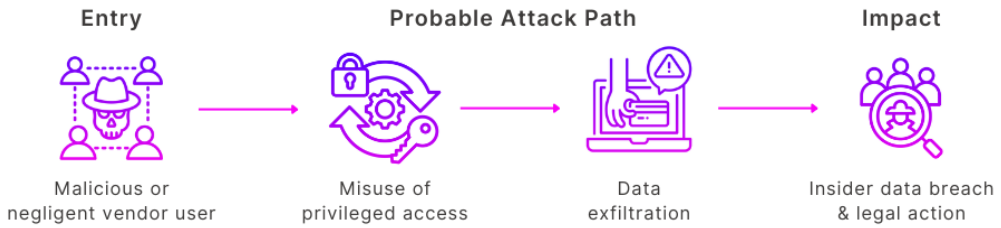
• **Marks & Spencer (2025):** Attackers compromised a TCS contractor's email account, then used that insider access to infiltrate M&S systems and steal 9.4M customer records , costing ~£300M and forcing a six-week cleanup.
• **Edward Snowden (2013):** As a contractor at the NSA, Snowden used his insider position to exfiltrate classified intelligence , demonstrating the scale of damage a single contractor can cause.
• **Tesla (2020):** Foiled plot where a Russian group attempted to recruit a Tesla insider with $1M to plant malware on Tesla's network.

D. Business Impact

• **Large-Scale Breaches:** Third-party insiders often have privileged access , a single rogue contractor can cause a breach affecting millions of records (e.g., M&S incident).
• **Sabotage & Downtime:** A malicious insider could plant a logic bomb or delete critical configs, causing outages.
• **Regulatory Exposure:** Breaches caused by vendor insiders still fall under your compliance responsibility (GDPR, HIPAA, PCI-DSS), triggering fines and breach notifications.
• **Reputation & Trust Damage:** Partners and customers may question your vendor vetting practices, forcing a review of third-party risk processes.

E. Risk Signals to Monitor

• **Unusual Data Access:** Contractors pulling large volumes of data unrelated to their work, or accessing systems outside of their project scope.
• **Orphaned Accounts:** Third-party accounts that remain active after a contract ends.
• Privilege Escalation Attempts: Vendor users running admin commands or probing systems they normally don't.
• **Behavioural Red Flags:** DLP alerts (large file zips, USB writes, mass email forwards), or abnormal working hours for external accounts.
• **Human Signals:** Reports of disgruntled contractors, suspicious financial behaviour, or insider chatter suggesting data theft intent.



9. Shadow IT and Unvetted Tools

A. How It Happens

"Shadow IT" refers to technology used outside of official IT control, from free SaaS apps and personal Google Drives to rogue Wi-Fi routers and unapproved laptops. These tools create a blind spot in your security program because they bypass risk assessment, governance, and monitoring.

Attackers exploit this blind spot in several ways:
• **Data Exposure:** Sensitive documents stored in unapproved cloud apps can leak if misconfigured or breached.
• **Credential Reuse:** Employees often use corporate passwords on unsanctioned tools; a breach of that app can give attackers credentials to your enterprise accounts.
• **Unpatched Systems:** Shadow IT servers or devices may never receive updates, leaving exploitable vulnerabilities.
• **Unmonitored Entry Points:** Rogue access points, personal laptops, or test servers become easy targets since SOC teams aren't watching them.

B. Attacker Tactics

• **OSINT Discovery:** Searching for exposed Trello boards, Google Docs, Slack workspaces, or public Git repos containing sensitive info.
• **Credential Stuffing:** Using leaked shadow IT creds to log in to enterprise portals.
• **Lateral Movement:** Pivoting from a shadow IT system (e.g., an unmanaged dev server) into the main network.

C. Real-World Examples

• **Trello Data Leaks:** Researchers found hundreds of public Trello boards containing login credentials, project roadmaps, and internal documents from major companies.
• **CenturyLink (2019):** A misconfigured third-party notification database left 2.8M customer records exposed , effectively shadow IT from a vendor perspective.
• **IBM (2017):** Sensitive internal documents were found on an unsecured third-party staging server set up without proper approval.

D. Business Impact

• **Compliance Breaches:** Data stored in unvetted systems may violate GDPR, HIPAA, or data residency requirements.
• **Data Loss:** Misconfigured apps can leak sensitive data with no logging to support forensics.
• **Reputation Damage:** Being named in "public exposure" reports (e.g., Trello leaks) erodes trust.
• **Operational Risk:** Business processes relying on unofficial tools can fail if the service is shut down or breached.

E. Risk Signals to Monitor

• **Cloud Access Visibility:** CASB solutions or firewall logs showing traffic to unapproved SaaS domains.
• **Employee Adoption Patterns:** Multiple users registering company emails on a non-approved SaaS tool.
• **External Search Results:** Company documents appearing in public search indexes or on paste sites.
• **Expense Reports:** Recurring purchases of SaaS subscriptions outside of procurement processes.

10. Exposed Web Portals & Partner Interfaces

A. How It Happens

Partner- and vendor-facing portals, supplier dashboards, dispute resolution sites, API gateways, are prime targets because they are internet-facing and often handle sensitive data.

Risks arise from:
• **Unpatched Software:** Outdated frameworks (Apache Struts, PHP versions) with known exploits.
• **Weak Authentication:** Default passwords, no MFA, or shared logins for partner users.
• **Authorization Flaws:** One partner viewing another's data due to broken access control.
• **Injection & Logic Bugs:** SQLi, XSS, and insecure API endpoints allowing code execution or data exfiltration.
• **Third-Party Components:** Chatbots, analytics widgets, or storage buckets integrated into portals that can be hijacked.

Attackers continuously scan the internet for such portals, testing for weaknesses with automated tools.

B. Attacker Tactics

• **Recon & Dorking:** Finding exposed portals with search engines or Shodan.
• **Exploit Kits:** Running SQL injection, XSS, RCE payloads against known-vulnerable components.
• **Credential Spraying:** Attempting weak passwords on partner login pages.
• **Web Shell Deployment:** Using a vulnerable upload form to plant persistent access.

C. Real-World Examples

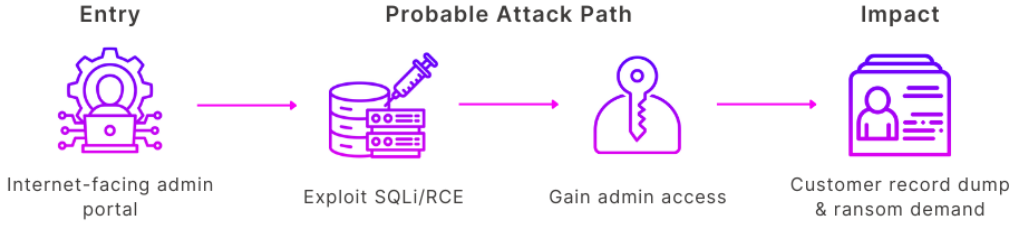
• **Equifax (2017):** Exploited an unpatched Apache Struts vulnerability in a consumer dispute portal, leading to theft of 147M records.
• **Harrods Supplier Portal (2025):** Attackers leveraged a flaw in a third-party hosted portal to access internal documents and supplier data.
• **Dell Partner Portal (2024):** API flaw exposed 49M customer records, including order histories.

D. Business Impact

• **Mass Data Breaches:** Equifax-type incidents lead to regulatory fines, lawsuits, and leadership fallout.
• **Operational Disruption:** Temporary shutdown of portals may halt supplier/customer processes.
• **Legal Liability:** Partners may pursue breach-of-contract claims if their data is exposed.
• **Foothold for Deeper Attacks:** Compromised portals can be used to deploy web shells or pivot into internal systems , escalating to ransomware events.

E. Risk Signals to Monitor

• **Portal Log Anomalies:** Repeated failed logins, enumeration attempts, or suspicious parameter fuzzing.
• **Security Scan Results:** High-severity CVEs detected by web vulnerability scanners.
• **Public Data Leaks:** Snippets of internal data appearing on forums/paste sites without internal indicators.
• **Partner Complaints:** Reports of cross-tenant data exposure or odd portal behaviour.



Conclusion

The ten attack vectors we examined show how identity sprawl, SaaS proliferation, fragile APIs, and software supply chain complexity create new breach pathways that attackers exploit faster than organizations can adapt.

What the Data Shows

- **Prevalence:** Nearly 60% of breaches involve a third-party component (Ponemon Institute, 2023).
- **Cost:** Third-party breaches cost 20–25% more than enterprise-only breaches, averaging USD 4.88M (IBM Cost of a Data Breach 2024).
- **Accountability:** Regulations such as NIS2, DORA, and GDPR now hold organizations responsible for their vendors' failures.

Strategic Imperatives for CISOs

- **Shift the Lens:** Treat third-party risk as enterprise risk, not a procurement issue. Elevate it to the board level.
- **Control the Interfaces:** Vendor identities, SaaS tokens, APIs, and supply chain components are the new perimeter. Protect and monitor them as first-class assets.
- **Design for Containment:** Assume a vendor will be breached. Use isolation, segmentation, and just-in-time access to limit blast radius.
- **Move to Continuous Oversight:** Replace point-in-time questionnaires with continuous monitoring, outside-in scanning, and real-time vendor telemetry.
- **Test and Prepare:** Develop playbooks for vendor-origin incidents and rehearse them with critical partners.

Closing Note

"Inevitable" does not mean "unmanageable." Third-party risk can be reduced, contained, and made transparent with the right mix of governance, technical control, and vigilance.

How genesis platform helps in third party risk management

Genesis Platform redefines Third-Party Risk Management (TPRM) by combining continuous monitoring, AI, and automation into one ecosystem.

AI-Powered Questionnaires

Eliminate onboarding delays

➤ Vendors complete intelligent questionnaires auto filled with prior evidence, drastically cutting assessment time.

Continuous Attack Surface Scanning

Detect risks outside-in.

➤ Identify exposed credentials, misconfigurations, and shadow IT in real time across the vendor ecosystem.

Automated Risk Remediation

Go beyond findings for third parties

➤ Vendors receive step-by-step fixes for immediate issues, plus a maturity roadmap that tracks progress from basic compliance to advanced security readiness.

Real-Time Risk Visibility

Board-ready dashboards.

➤ Continuous monitoring and reporting give CISOs instant clarity on vendor posture, compliance, and ecosystem health.

With Genesis, organizations move faster, onboard smarter, and defend stronger**,** transforming third-party risk from a drag on operations into a strategic advantage for resilience and trust.

Get a free Vendor Security Report

genesisplatform.co

About the Author

Syed Amoz

Syed Amoz is the Co-Founder of Genesis TPRM, specializing in third-party risk management, attack surface discovery, and threat intelligence research. His expertise spans designing frameworks for outside-in security scanning, developing methodologies to identify third-party attack paths, and aligning technical findings with enterprise risk priorities.

In addition to his work on Genesis, Amoz is actively exploring decentralized cybersecurity technologies, including peer-to-peer intelligence sharing, distributed reconnaissance, and resilient detection models, aimed at making cybersecurity more collaborative and less reliant on single points of failure.

Khalifa Al Shehhi

Khalifa Al Shehhi is the Co-Founder of Genesis TPRM, with expertise in enterprise risk management, governance, and cybersecurity for high-risk industries. His experience spans oil & gas, energy, and critical infrastructure, giving him a deep understanding of regulated environments, risk frameworks, and operational resilience.

Khalifa's focus includes advancing modern approaches to TPRM, such as exploring decentralized management delegation to distribute risk accountability across business units and integrated continuous monitoring models that combine outside-in attack surface visibility with inside-out assessment data. This perspective shapes his vision for enabling CISOs and boards to maintain a unified, real-time view of vendor and supply chain risk.