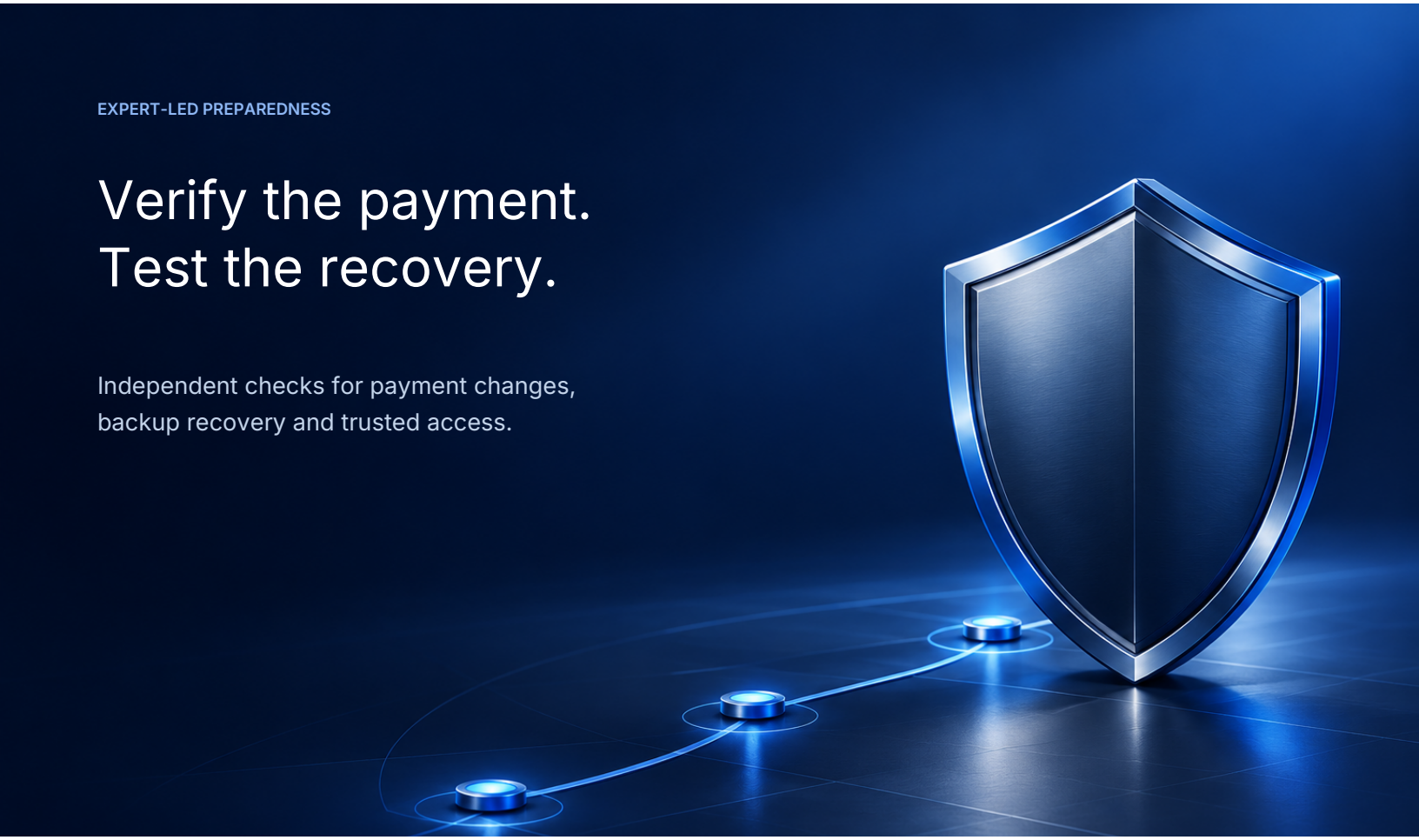
CYBER INCIDENT READINESS

Security threat report

Verify payments. Check who has access.

A working briefing for business leaders and their IT teams



IN THIS EDITION

Business email compromise / ConnectWise / Product advisories

Prepared by DFI Forensics | Sources checked 15 November 2026

01 / BUSINESS EMAIL COMPROMISE

Verify the payment before it moves

A payment-change request can look authentic because it comes from an impersonated sender or a real mailbox someone has taken over. In its 5 November review, Microsoft described invoice and payroll-change lures. Earlier this year Cranbrook RCMP reported payment fraud involving compromised Microsoft 365 accounts. [9, 10]

Make the first check independent

Pause an emailed change, call an established number unrelated to the message, and ask a second approver to review the recorded verification before funds are released. The Canadian Anti-Fraud Centre recommends independent verification of changes to payment instructions. [11]

Situation	First action / owner	What to keep
Change is pending	Finance: pause it; confirm with an authorized contact through a known number and get an independent second approval.	Name of authorized contact, time and source of callback number; second approval.
Funds may have moved	Finance: contact the bank immediately through its established fraud contact. Notify the incident lead.	Payment references, transaction dates, related invoices, approvals and original messages.
Mailbox may be compromised	IT and response: coordinate containment through a trusted channel. Review sessions, authentication, permissions and mailbox changes. [12]	Relevant sign-in and audit records, suspicious messages and rules, and the documented scope of the review.

RECORD THE DECISION

Finance owner / independent callback evidence:

Bank notified if funds moved / incident owner or next action:

A suspect payment instruction alone does not establish whose account was compromised. Do not send incident evidence to an address you suspect is affected.

02 / CONNECTWISE CLOUD BACKUP

Verify restoration tenant by tenant

ConnectWise reported unauthorized access to application credentials associated with Cloud Backup, formerly SkyKick. The vendor's 4 November update says backups and restores are available for re-authorized Microsoft 365 tenants while phased restoration continues. This is different from the ScreenConnect activity described on the next page. [13, 14]

Keep two records

Your provider can show whether backups are running and prove that a controlled restore works. Your tenant administrator and incident lead separately assess what the retained evidence says about earlier access. Neither result determines the other.

Check	Evidence to ask your provider for
Backup coverage	Last known-good backup before the interruption; first verified backup after supported reconnection; dates or workloads with no coverage.
Restore readiness	Result of an agreed test restore, what was restored, where the test ran and any exception that affects recovery.
Historic review	Which Microsoft 365 tenants and legacy connections were considered; scope of application sign-in, permissions and role review; log gaps and follow-up. [13, 14]

USE ONE RECORD PER AFFECTED TENANT

Tenant reference / backup and security owners:

Backup dates and test result / unresolved recovery or investigation question:

A vendor status update does not establish that any specific customer was compromised. Suspicious authentication alone does not show which data, if any, was accessed.

03 / REMOTE SUPPORT ASSESSMENT

Remote support deserves two checks

ConnectWise reported unauthorized access to some partner cloud-hosted ScreenConnect environments on 11 November. Microsoft independently confirmed the activity on 13 November and observed unauthorized remote-access tools on managed computers. ConnectWise's 13 November update reported additional activity targeting self-hosted environments. [1, 2]

> **The decision for leaders**
>
> Ask your IT team or managed service provider for two distinct answers: what was changed and verified, and what the available records show about earlier unauthorized activity. One answer cannot substitute for the other.

What the current advisory does and does not establish

ConnectWise had not found evidence that its infrastructure was compromised or that a flaw in the core ScreenConnect product was used for initial access. The cause remained under investigation. A listed extension on a system is not a compromise finding. The workstation update and extension actions address separate risks. [1]

Scope	What to verify
Hosted	Ask the hosting and service owners which vendor-side actions apply. Confirm versions on every technician workstation.
Self-hosted	Apply the current vendor extension directions immediately. Check every relevant instance and separately verify technician-client versions.
Both models	Verify ScreenConnect client 26.6.5 or later on every technician workstation. If access is suspected, review downstream devices and use a trusted response route. [1, 2]

The broader business risk is loss of confidence in the support channel and the devices it reaches. Responders may need to look across organizational boundaries, including provider systems and your managed devices. The public reports do not establish whether your organization was affected.

04 / PRIORITIZE THE APPLICABLE PRODUCTS

Outlook and exposed appliances

A shared decision applies to each item below: verify the change on the affected asset, then ask whether the asset was exposed in the relevant period and whether the available evidence warrants investigation. Priorities depend on deployment, business impact and actual findings.

Microsoft Outlook for Windows desktop | CVE-2026-124194

Microsoft addressed an exploited vulnerability on 10 November. It involves opening a malicious file in an affected Outlook desktop app; the Preview Pane alone is not a trigger. Possible consequences include account impersonation. Verify Microsoft's affected-product and update-channel tables; spot-check device-level deployment, including overdue and offline computers. If suspicious activity is reported, preserve the original file and review relevant identity and mailbox records with the incident lead. [3, 4]

Check Point security products | CVE-2026-123039

The Cyber Centre reports exploitation. Check Point identified internet-accessible Security Gateways using Mobile Access as primary targets and reported limited destructive cases. Have the network owner verify applicable gateway and management product remediation in the current vendor guidance and review historic exposure when relevant. [5, 6]

Barracuda Email Security Gateway | CVE-2026-111560 and CVE-2026-116606

CISA added the two ESG issues on 10 November. The appliance owner should check whether the affected administrative interface was exposed, verify the vendor's rollout and instructions for that appliance, and assess earlier exposure separately. This does not apply to all Barracuda email services. [7, 8]

> **Record the exception, not just the successful update**
>
> For an offline endpoint or deferred appliance change, document the owner, reason, temporary safeguards and next review time. If you cannot verify a product version or past reachability, keep the status open or unknown.

05 / WORKING TOOL

Exposure and remediation worksheet

Fill this out with the provider or team that can show evidence. Make a copy for each instance, endpoint group or appliance. Store records securely with your incident or change record; do not submit this worksheet to download or access the report.

Check	Record to request
Ownership and scope	Service owner; MSP contact; hosted/self-hosted model; assets or device groups in scope.
ScreenConnect	Relevant extensions and action; verification across instances; technician-client version evidence. [1]
Outlook	Actual Windows desktop products/channels; device update evidence; off-network exceptions. [3, 4]
Appliances	Relevant product and version; historic external reachability; vendor remediation evidence. [5-8]
Coverage gaps	Missing assets, unavailable logs, last time records were available; who will follow up.

RECORD ONE RESULT

Service or asset group / owner:

Evidence reviewed / date and time zone:

Remediation status / remaining exceptions:

Historical review status / records unavailable:

Next step / accountable owner / due date:

Use a precise status: verified, not applicable with evidence, pending, or unknown. A closed change ticket is not a historical investigation finding.

06 / INCIDENT COORDINATION

Preserve records and coordinate safely

Escalate credible signs of unauthorized access through your incident plan and notify the IT provider through a trusted contact route. If you suspect ScreenConnect was used, do not use that same service to investigate or clean suspected endpoints. Use a separate trusted tool or route agreed with responders. [1, 2]

Who leads	Preserve or document	Decision it informs
IT provider / tool owner	Relevant platform activity, session history, administrative and extension records, affected instance list.	Which systems and accounts might have been reached?
Endpoint security	Relevant endpoint security alerts, process or software inventory and unapproved remote-access tools, where available.	Which technician and managed devices should be prioritized?
Identity and messaging	Relevant sign-in, session and mailbox audit records; record any suspicious file report without reopening the file.	Are accounts, sessions or mailbox changes in scope?
Incident lead	Decision and action log: who approved isolation or restoration, why, and what was unavailable.	What was decided, and what is still uncertain?

Coordinate containment and evidence preservation

If suspicious activity is ongoing, do not put off containment for a complete evidence collection. Work with responsible responders to secure systems while documenting what was changed. Preserve originals, record time zones and retention limits, and keep access to sensitive records restricted.

Confirm the basis for restoration

Have the system owner and response lead confirm trusted administrative access, removal of any identified unauthorized access, the scope of device verification, and what monitoring or follow-up is still needed. If identity compromise is suspected, confirm session actions as well as credential changes. [1, 2]

07 / LEADERSHIP DISCUSSION

Agree who can act, and on what evidence

Use this page in a short meeting with leadership, IT and the provider. These prompts support internal decisions; they are not regulatory deadlines or a determination that an incident occurred.

Decision	Owner and confirmation
Accountability	Name the person who consolidates provider and internal findings and can answer which services and assets are in scope.
Escalation	Name the person who can invoke the incident plan and approve disruption if containment is needed. Verify a callback number or another independent route.
Operational impact	Identify critical services that depend on remote support or the affected device. Agree which teams require an alternate support arrangement.
Unresolved evidence	Document log gaps, affected devices not yet seen and whether a provider review excludes any part of your environment. Assign a next review time.
Closure	Record remediation status separately from what the investigation can show. Decide who accepts remaining uncertainty and who will update the record.

SIGN-OFF RECORD

Accountable decision owner / date:

Next review time / open question:

Readiness your team can put to work

BreachReady starts with retained incident-response specialists and priority 24/7 support from day one of an active annual agreement. Alongside your IT team, DFI helps practise decisions and guide practical ransomware and business email compromise safeguards. Existing clients should use their agreed response contacts for a suspected incident.

Planning ahead? Discuss your current response arrangements with DFI.

08 / SOURCES AND EDITORIAL BOUNDARIES

Sources

Primary sources checked 15 November 2026. The dated developments below are the foundation for this briefing. Check the current vendor advisory before implementing production changes.

1. ConnectWise Trust Center: ScreenConnect advisory
   11 November; latest update used: 13 November 2026
2. Microsoft Security Research: ScreenConnect abuse
   13 November 2026; independent observations and response guidance
3. Microsoft: CVE-2026-124194
   10 November 2026; use product and update information for your deployment
4. Canadian Cyber Centre: November Microsoft monthly rollup
   10 November; updated 12 November 2026 with exploitation/KEV details
5. Canadian Cyber Centre: Check Point advisory
   12 November; updated 13 November 2026
6. Check Point: vendor security advisory
   12 November 2026; mitigation and reported impact
7. Canadian Cyber Centre: Barracuda advisory
   2 November; 10 November update; page modified 12 November 2026
8. Barracuda Trust Center: Email Security Gateway advisory
   Product and remediation scope; see vendor for current directions
9. Microsoft: Email threat landscape, Q3 2026
   5 November 2026; invoice and payroll-change impersonation
10. Cranbrook RCMP: Email payment fraud
   7 May 2026; Canadian context for payment diversion
11. Canadian Anti-Fraud Centre: Fraud trends
   First half of 2026; verify changes and contact bank
12. Microsoft Learn: Respond to a compromised mailbox
   Defensive account-recovery guidance
13. ConnectWise: Cloud Backup restoration
   4 November 2026 status; affected tenant review and recovery
14. Microsoft Security Research: October Cloud Backup incident
   21 October 2026; downstream app and identity observations

What remains outside this report

This is general threat intelligence and defensive guidance. It does not establish any reader's exposure, compromise status or remediation outcome. No client systems were accessed or assessed for this publication. DFI's business interpretation and prioritization are editorial guidance rather than vendor or government deadlines.

Edition 2026-11-15 | Version 1.0 | Initial edition | DFI Forensics