Reach

Ten Hidden Cybersecurity Misconfigurations

How to Find and Fix Them in 2026

In 2025, organizations spent billions on security, deploying EDR/XDR, SASE, firewalls, identity platforms, email security, web security, and more. And yet, breaches persist. The reason often isn't a zero-day, an advanced persistent threat, or a cutting-edge exploit; it's far more mundane. Misconfigurations across identity, endpoint, network, and email/web security tools remain among the top root causes of incidents.

According to one recent analysis, "Misconfigurations drive 80% of security exposures,[1]" many of them involving identity and credential issues.

Meanwhile, another 2025 industry report from a major security vendor found that misconfiguration-related issues already fueled more than 9.5 million cyberattacks in just the first half of the year [2].

Do you know what misconfigurations are hiding across your security stack? Are you able to identify them quickly and remediate?

Here are 10 critical cybersecurity misconfigurations we expect to see in 2026, and how you can identify and fix them before attackers can exploit them.

[1] Misconfigurations drive 80% of security exposures, Security Magazine
[2] Sonicwall Report Finds Misconfigurations Driving Surging Cyberattacks in 2025

1. EDR Tamper Protection Not Enabled

The issue:

On many endpoints, EDR/XDR agents are installed, but "tamper protection" is left off. A local admin (or malware with elevated rights) can simply stop, uninstall, or reconfigure the agent, often without detection.

Why it matters:

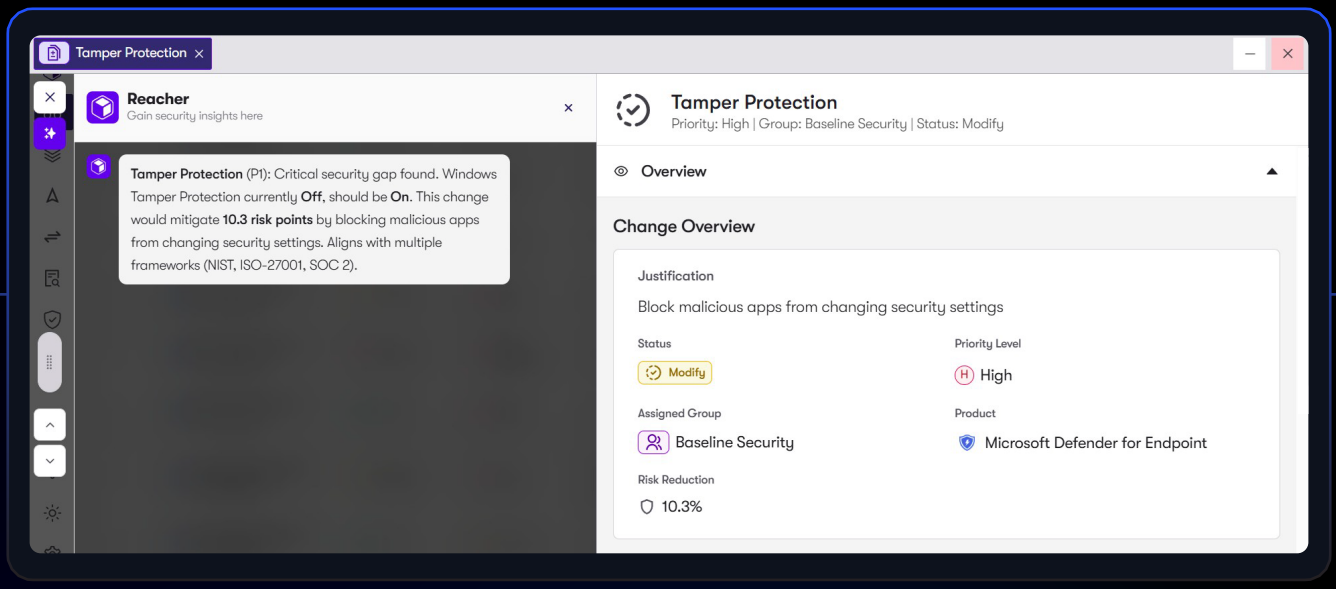
Once the agent is disabled or removed, endpoint visibility vanishes. Attackers roam free; detection and response stop before they've begun.

The control:

Modern EDR/XDR tools include a tamper-protection option (sometimes called "agent hardening," "anti-tamper," or "end-user protection"). When enabled, it prevents unauthorized uninstallation, modification, or disabling of the agent, unless via a signed policy push or authorized console.

How Reach Security helps:

- Reach scans all endpoints to confirm tamper protection is enabled and enforced.
- If tamper protection is turned off across any endpoints, they are flagged and remediated, and the control is turned on.
- With tamper protection turned on, this blocks malicious apps from changing security settings. This drastically reduces risk. This control maps to 10 major security frameworks (NIST 800-53, ISO-27001, HITRUST, etc), making it a critical component of your security baseline.



Reach identifies a disabled tamper protection on Microsoft Defender for Endpoint and recommends a remediation.

2. Allowing Anonymizers, Proxies, VPNs, or TOR Exit Nodes

The issue:

Many networks allow outbound traffic without blocking anonymizers, proxies, VPNs, or known TOR exit nodes.

Why it matters:

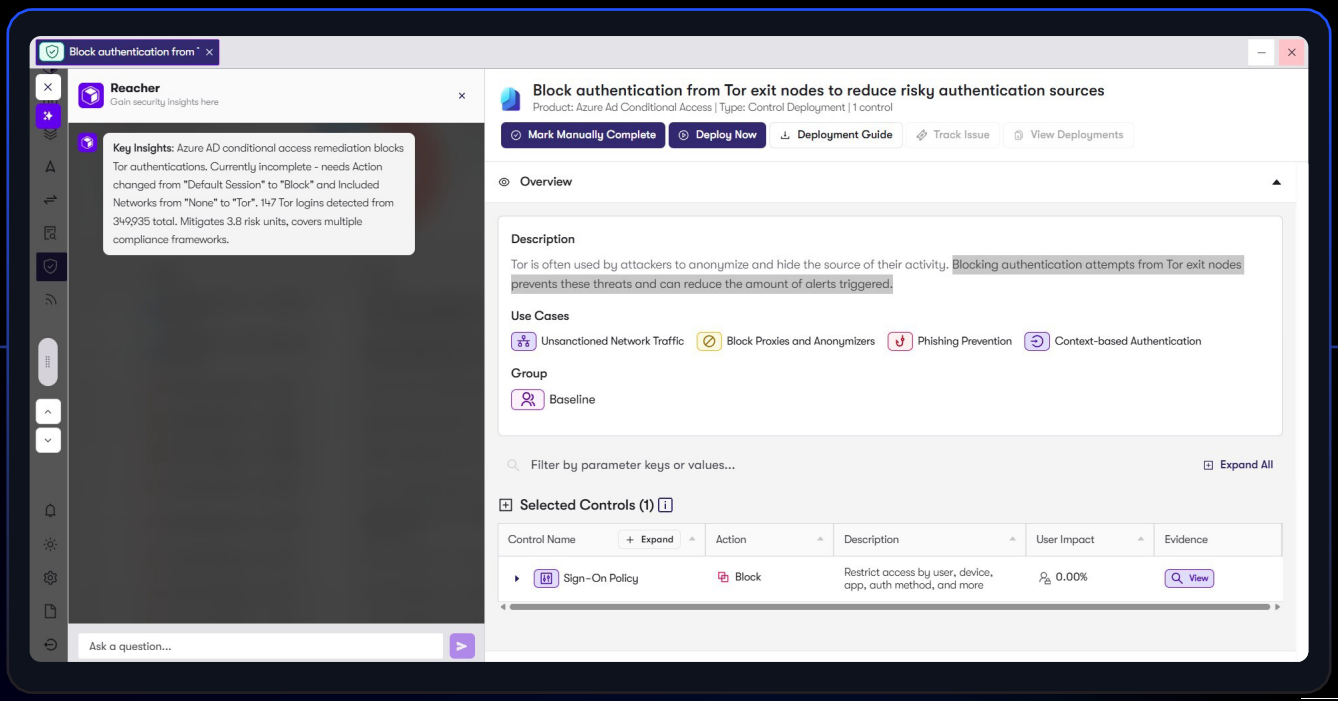
Attackers – or malicious insiders – use those tools to anonymize and hide the source of their activity. Attackers can hide their origin, bypass geolocation or IP-based controls, bypass network restrictions, or exfiltrate data under the radar. Once anonymized, it becomes much harder to detect, attribute, or block malicious traffic.

The control:

Firewalls, web gateways, SASE systems, and some identity and access management (IAM) tools often support blocking of known anonymizer IPs, proxy lists, VPN endpoints, or TOR exit nodes. Tools like Microsoft Entra ID Conditional Access can block authentication attempts from Tor exit nodes. Some tools integrate threat-intel feeds or allow custom block-lists.

How Reach Security helps:

- Reach reviews your firewall/SASE/web gateway policies and determines if anonymizers or proxy traffic is currently allowed.
- If allowed, Reach integrates threat-intel block-lists or custom rules to block or monitor such traffic.
- The payoff: attackers lose their ability to hide behind anonymizers. De-anonymized traffic improves attribution, detection, and overall network hygiene.



Reach identifies that Tor exit nodes are not being blocked and recommends a remediation using an available control from Microsoft Entra ID Conditional Access.

3. Email “Safe Links” or URL-Protection Controls

The issue:

Many organizations rely on basic anti-spam or anti-malware filtering, but leave URL rewriting / click-time protections disabled in their email stack.

The control:

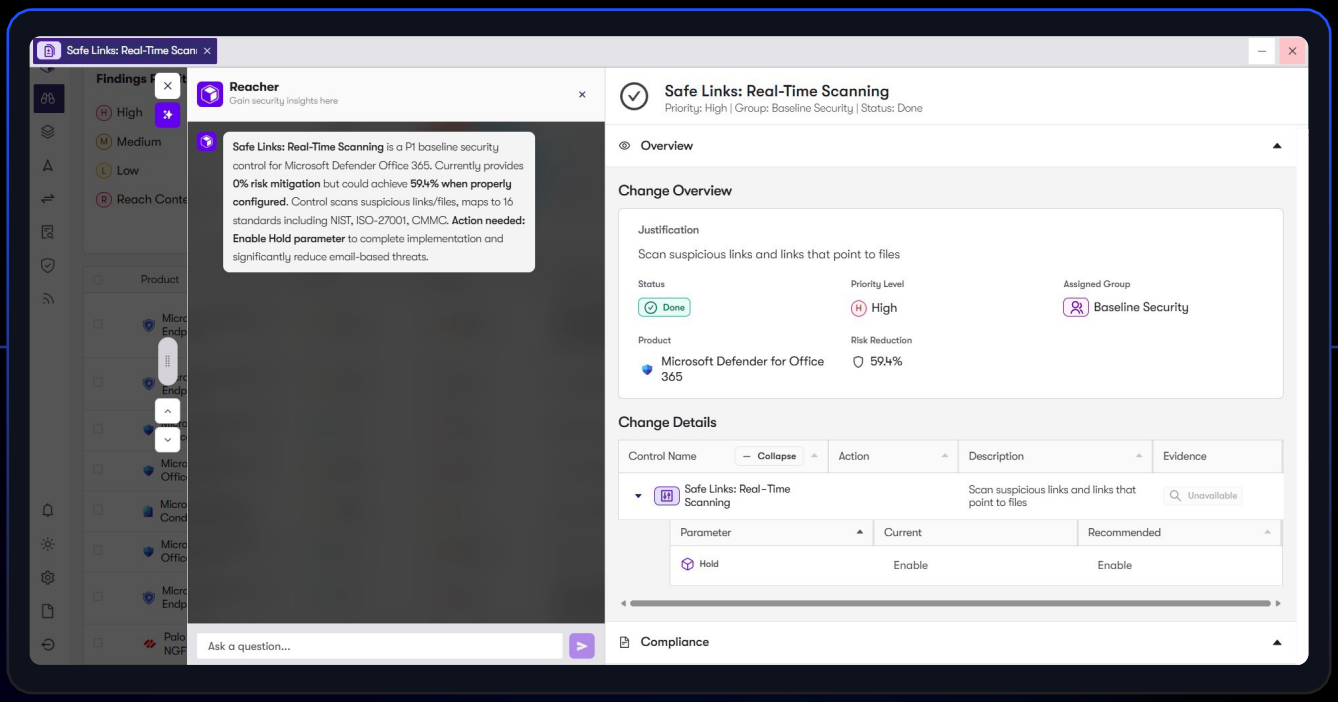
Email security gateways or suites (for example, Microsoft Defender for Office 365) provide “Safe Links,” URL rewriting, sandboxing, or click-time scanning which rewrites each link when the user clicks, then checks the destination against threat intelligence or sandbox verdicts.

Why it matters:

Phishing campaigns often deliver malicious links. Without runtime URL scanning, users can click seemingly harmless links that lead to credential phishing, malware downloads, or C2 infrastructure.

How Reach Security helps:

- Reach audits your email security configuration, verifying whether Safe Links / URL protection is enabled for inbound (and internal) mail.
- If disabled or misconfigured, Reach enables and properly scopes the policy (e.g., include forwarded mail flows).
- The result: phishing links are significantly less effective. Users who click are redirected through the scanning infrastructure, giving security teams time to block, alert, or quarantine before damage occurs.



Reach identifies that the Safe Links feature on Microsoft Defender for O365 is misconfigured and recommends a remediation.

4. No Maximum Session Duration / Overly Long Sessions for High-Risk Logins

The issue:

Many identity and access management (IAM) platforms default to long-lived sessions whereby login tokens or cookies may remain valid for days or even weeks. Organizations rarely shorten or limit session durations, even for high-privilege accounts.

The control:

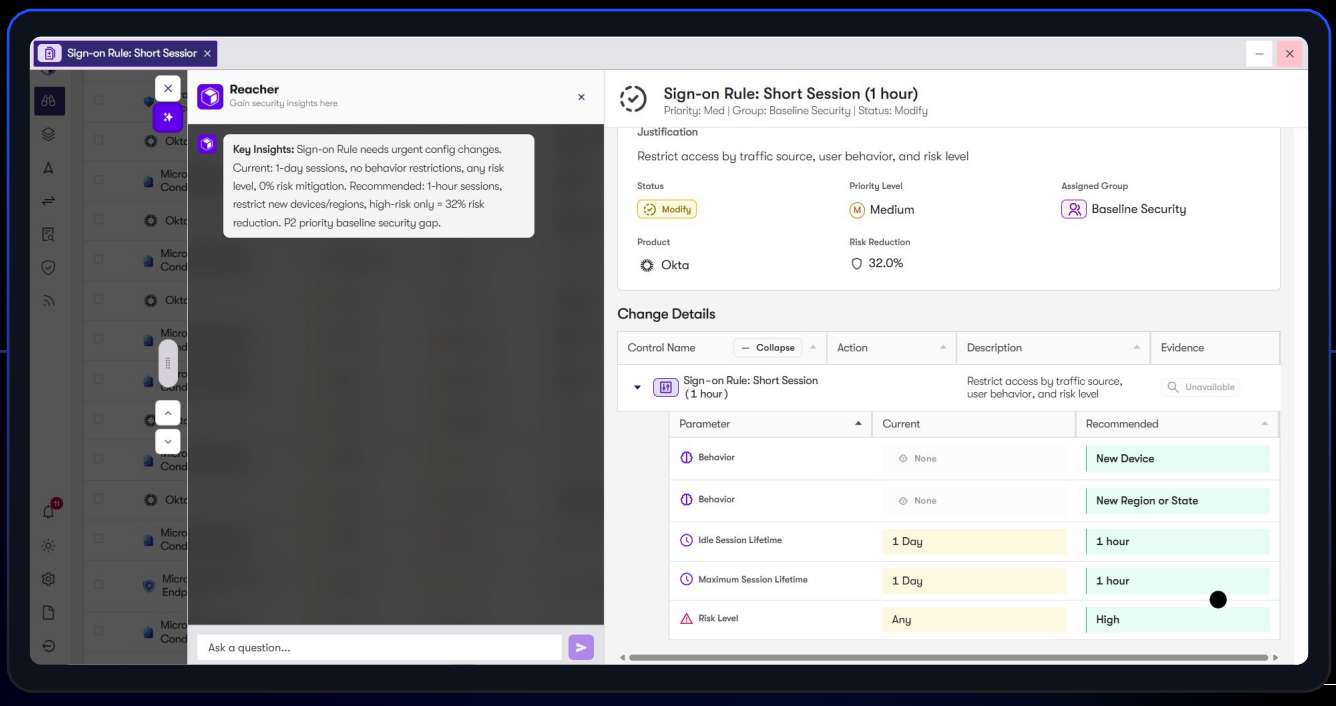
IAM platforms (e.g., Okta, Microsoft Entra ID, other identity providers) allow configuring session lifetimes, maximum session durations, and re-authentication requirements, especially around high-risk operations (privileged access, configuration changes, sensitive apps).

Why it matters:

If a session token is stolen – via cookie theft, session hijacking, or other means – an attacker can maintain access indefinitely, bypassing periodic re-authentication. Long-lived sessions extend dwell time and amplify risk.

How Reach Security helps:

- Reach reviews session-management settings across identity providers.
- Reach recommends and implements shorter session durations (e.g., minutes/hours) for high-risk or privileged logins, with re-authentication for critical operations.
- As a result, stolen credentials or hijacked sessions become far less useful to attackers, with their window of opportunity shrinking drastically.



Reach identifies a misconfigured sign-on rule on Okta and recommends a remediation to change to a 1-hour short session and restrict access by traffic source, user behavior, and risk level.

5. Failure to Block Abused or Unused Networks, IP Blocks, or Suspicious ASNs

The issue:

Networks, IP ranges, or Autonomous System Numbers (ASNs) that once had business purpose – or never had any – often remain open or unmonitored.

The control:

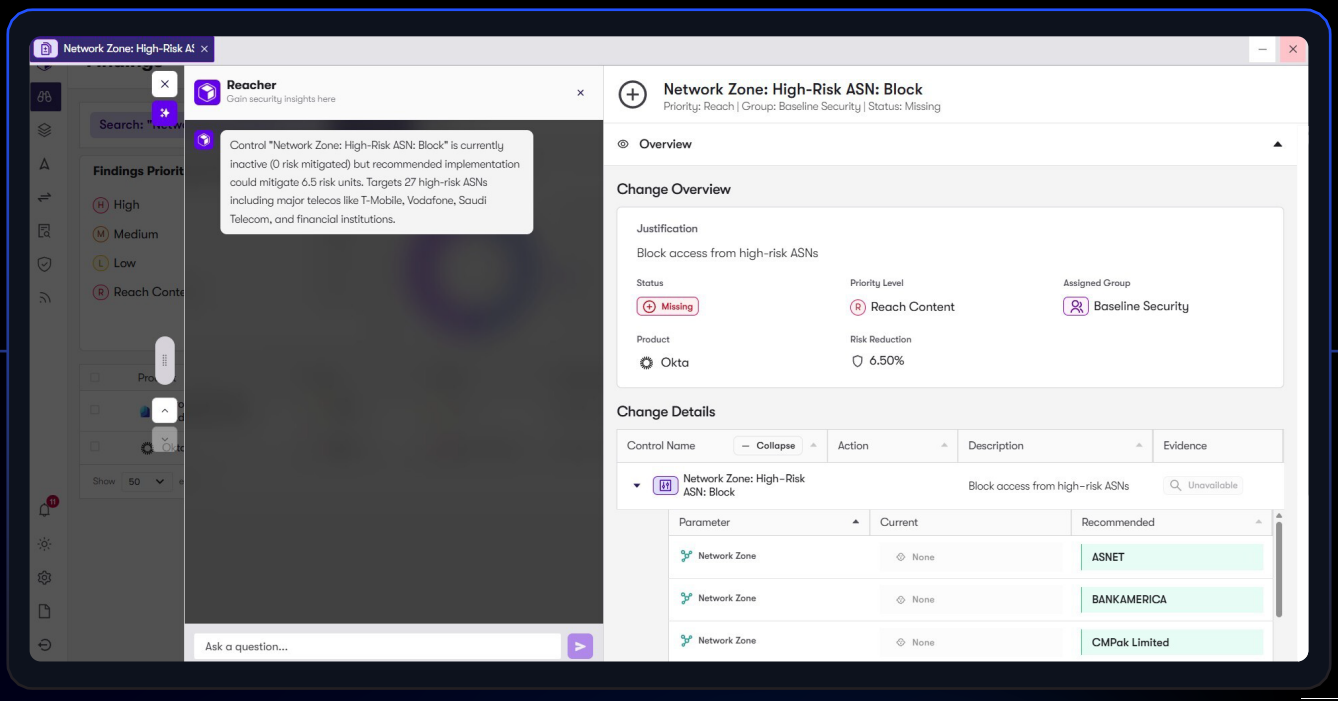
Network security tools (firewalls, SASE, web proxies) can block external IP ranges or ASNs, import blacklists, or flag suspicious communication.

Why it matters:

Attackers scan for unused paths. Unblocked or unmonitored IP blocks, ASNs, or network ranges are low-hanging fruit for exfiltration, phishing landing zones, command-and-control, or other illicit traffic.

How Reach Security helps:

- Reach analyzes external communication patterns, historic logs, and network flows to identify unused, legacy, or suspicious networks.
- Reach will recommend blocking or strictly monitoring those networks, especially those with no legitimate business use or high-risk history.
- As a result, you can shrink your attack surface, eliminate blind spots, and make lateral movement or exfiltration more difficult for attackers.



Reach identifies an inactive high-risk ASN block capability on Okta and recommends a remediation to implement it (which targets 27 high-risk ASNs).

6. No SSL/TLS Inspection & Weak Web-Security / URL-Filtering Controls

The issue:

Many organizations treat HTTPS as a black-box: encrypted traffic passes through firewalls/SASE without inspection, and web access policies are minimal or absent.

The control:

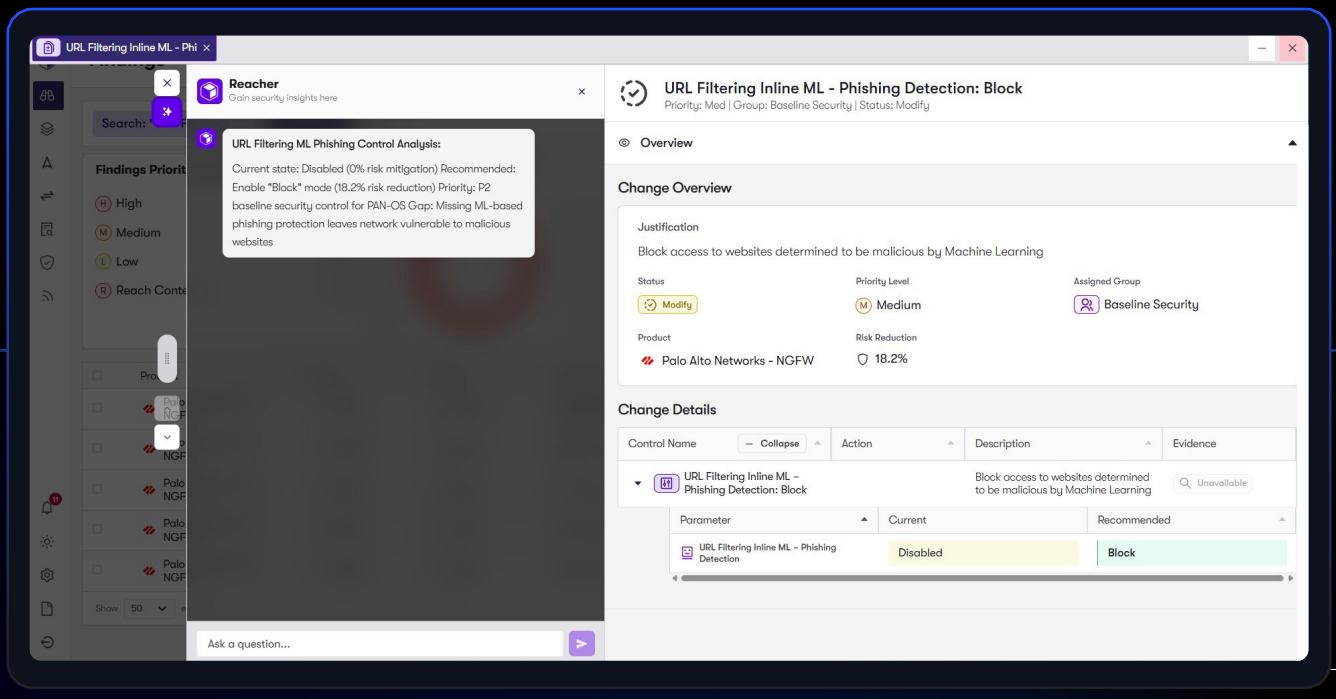
Network security solutions – such as SASE gateways, secure web gateways, firewalls, or web proxies – support TLS/SSL inspection (decryption), URL filtering, domain- or category-based blocking, sandboxing, and logging / alerting.

Why it matters:

Encrypted traffic often carries malware, phishing pages, C2 traffic, or opportunities for data exfiltration. Without TLS/SSL inspection and URL filtering, everything looks like harmless HTTPS – even malicious content.

How Reach Security helps:

- Reach audits network gateways to check if TLS/SSL inspection is enabled and whether URL filtering policies exist.
- If these controls are missing or weak, Reach advises on deploying or reconfiguring security tools with inspection, URL filtering, and logging capabilities. Security teams can block access to websites determined to be malicious. Some tools, like Palo Alto Networks NGFW, use machine learning functionality to make this determination.
- This gives you visibility into encrypted traffic, making it far harder for attackers to hide malicious downloads, phishing, or C2 channels behind HTTPS.



Reach identifies a disabled URL filtering control on PAN NGFW and recommends that "block mode" be enabled to block access to websites determined to be malicious.

7. Missing Credential Phishing Detection Controls

The issue:

Even with Safe-Linking and basic email/web filtering, many organizations do not enable specialized credential-phishing detection controls or they ignore domain-impersonation, login-form protections, or credential harvesting.

The control:

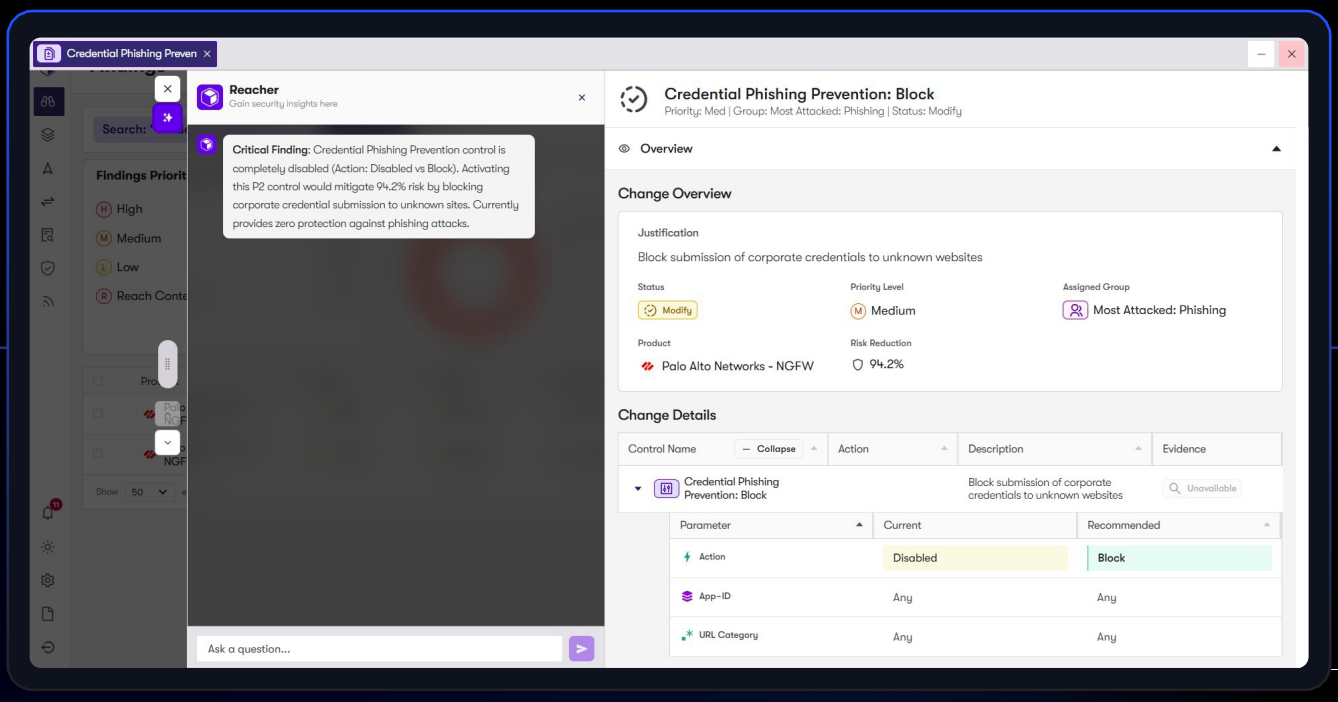
Modern email gateways, web gateways, firewalls, or SASE systems may offer anti-phishing modules that can detect suspicious login forms, block login forms on unknown domains, sandboxing, or offer real-time analysis of credential-harvesting attempts.

Why it matters:

Attackers increasingly deploy sophisticated phishing kits that mimic login portals, credential-harvesting pages, or malicious OAuth consent screens. Without phishing protections, these attacks can bypass URL scanning, because the link might look benign on delivery, but becomes malicious at runtime.

How Reach Security helps:

- Reach evaluates whether your email, firewall, and web stack provides capabilities around phishing-centered detection, including credential-phishing blocking.
- Reach integrates across your email, firewall, and web security tools to proactively activate phishing modules, integrate threat-intel feeds, and can deploy identity-aware proxies that detect credential-harvesting attempts.
- The outcome: credential phishing becomes much harder. Even when elements like links bypass basic filtering, credential harvesting pages can be blocked or flagged before users submit credentials.



Reach identifies that credential phishing prevention is disabled on PAN NGFW and recommends activating this control to block corporate credential submission to unknown sites thereby mitigating risk by 94.2%.

8. MFA Not Enforced for Sensitive Actions

The issue:

Many organizations enforce multifactor authentication (MFA) only at login, not necessarily at critical identity or device workflow events such as password changes, device enrollments, device joins, or privilege elevation. Even with robust MFA policies in place, configuration drift can occur under the radar. For instance, IT teams could disable MFA for high-risk users (like the C-suite), without consulting the security team.

Why it matters:

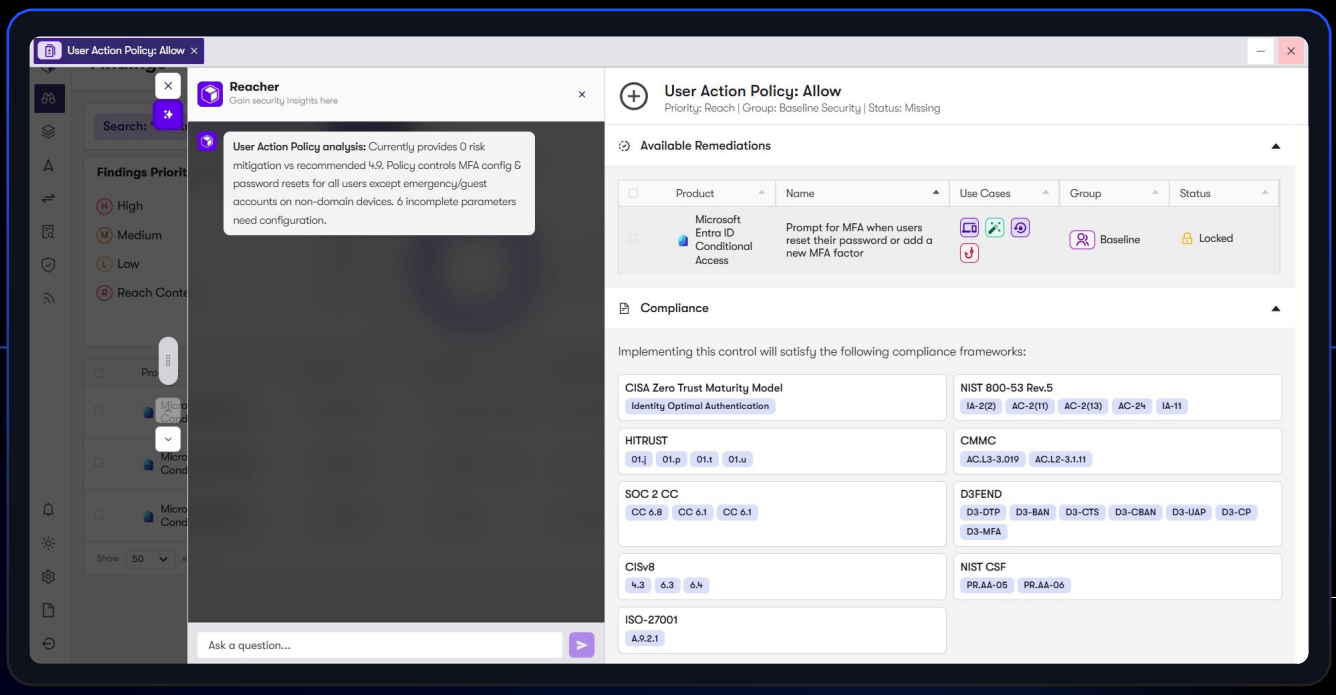
If an attacker hijacks a session or obtains credentials, they can perform sensitive operations like resetting a password or registering a new device – without a second factor. This undermines your MFA protection, exposes the organization, and increases ease of access to sensitive data (to which executives are privy) by attackers.

The control:

IAM platforms, device-enrollment workflows, and device-management tools can enforce conditional MFA, not only at login, but also for sensitive operations such as password resets, device joins, enrollment, or privileged actions.

How Reach Security helps:

- Reach audits your identity and device management policies to verify where MFA is enforced.
- If MFA is missing for sensitive actions, Reach can enable conditional MFA for password changes, new device enrollments, and privileged ops. Furthermore, if changes are made to MFA controls unbeknownst to the security team, Reach configuration drift detection will identify the change, create a drift alert, and automatically remediate before risk is introduced.
- This ensures that sensitive data is protected, MFA policies are enforced, and even in the case of configuration drift, that security posture is continuously validated over time. Also, even if credentials are compromised, attackers cannot easily escalate their control or persist via new device enrollments.



Reach identifies a missing user action policy in Microsoft Entra ID Conditional Access and recommends it be set to "allow" to control access to MFA configurations, self-service password resets, and device management.

9. Relying on Default Configurations and Under-Utilizing Custom Detections on Endpoint Security Tools

The issue:

Many security teams deploy EDR/XDR with vendor-supplied, default detection rules. They may not customize them to match their environment, threat model, or asset profile. Or if they do customize, they're unable to strike a proper balance as too many additional rules can overwhelm security teams with more work and more alerts to track and resolve.

Why it matters:

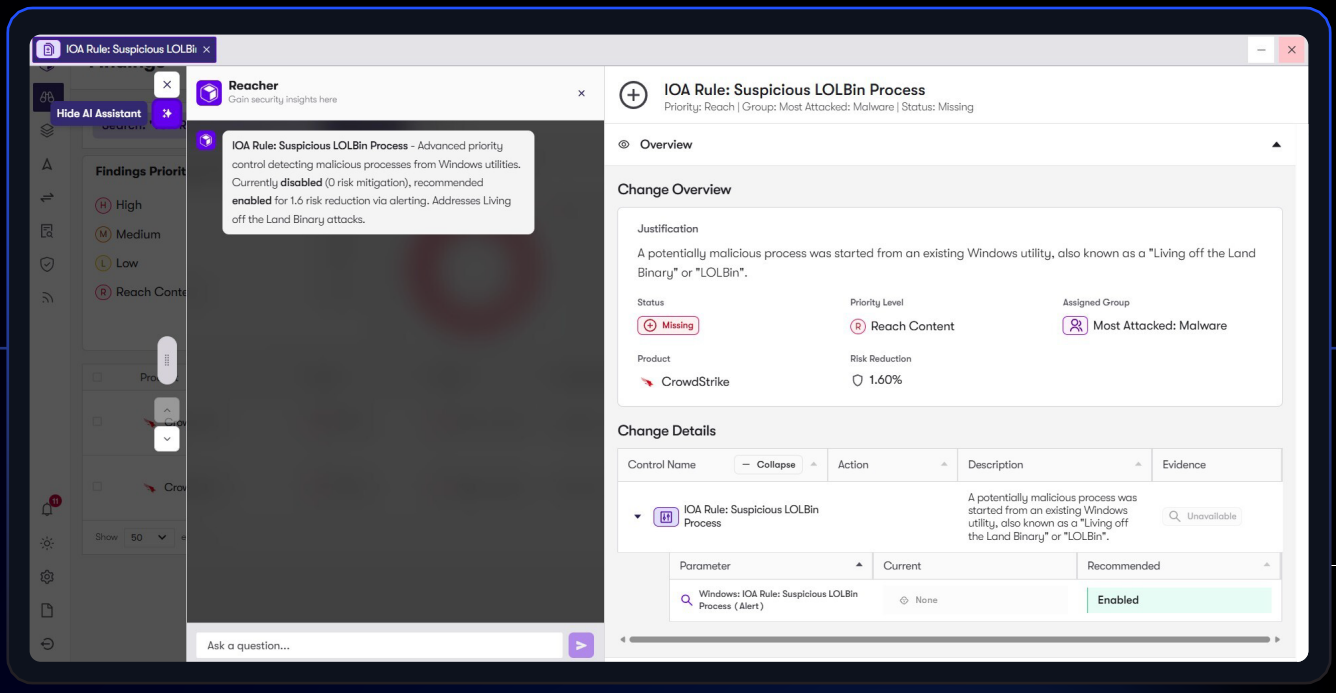
Attackers understand default detection rules. They often develop tactics specifically designed to avoid them. Without custom detection rules, you may miss stealthy or targeted attacks. Configuring custom rules on your endpoint security provides better visibility into an attacker's intent and behavior and gives insight into threat patterns that provide added context outside of regular IOC's.

The control:

Modern EDR/XDR platforms allow custom rule creation: behavioral detections, indicator-of-attack (IOA) rules (in Crowdstrike), storyline active response (STAR) rules (in SentinelOne), custom YARA signatures, environment-specific alerting, and tailored policies.

How Reach Security helps:

- Reach ingests attack data and recommends optimal configurations for endpoint tools. Reach can tune and deploy custom IOA, STAR, and other rules to identify and contain malicious behavior. Reach can help you define a custom detection strategy based on your assets, typical behavior, risk profile, and likely attacker TTPs (tactics, techniques, procedures).
- Reach refines how these rules are applied, helps correlate data across tools, and enacts defensive measures to address threats company-wide.
- Result: detection becomes more sensitive to targeted attacks that standard rules might miss, giving you higher visibility and faster detection.



Reach identifies a disabled IOA rule on CrowdStrike and recommends it be enabled to address "living off the land binary attacks".

10. No / Unsafe File-Type Blocking on Email Gateways

The issue:

Misconfigured email gateways can allow delivery of attachments with potentially malicious file types like executables, script files, or macro-enabled Office documents that contain VBA (visual basic for apps), without blocking, sandboxing, or scanning them. There has been a rise in spear-phishing attacks using RDP files, underscoring the need for consideration of policies blocking based on attachment types.

Why it matters:

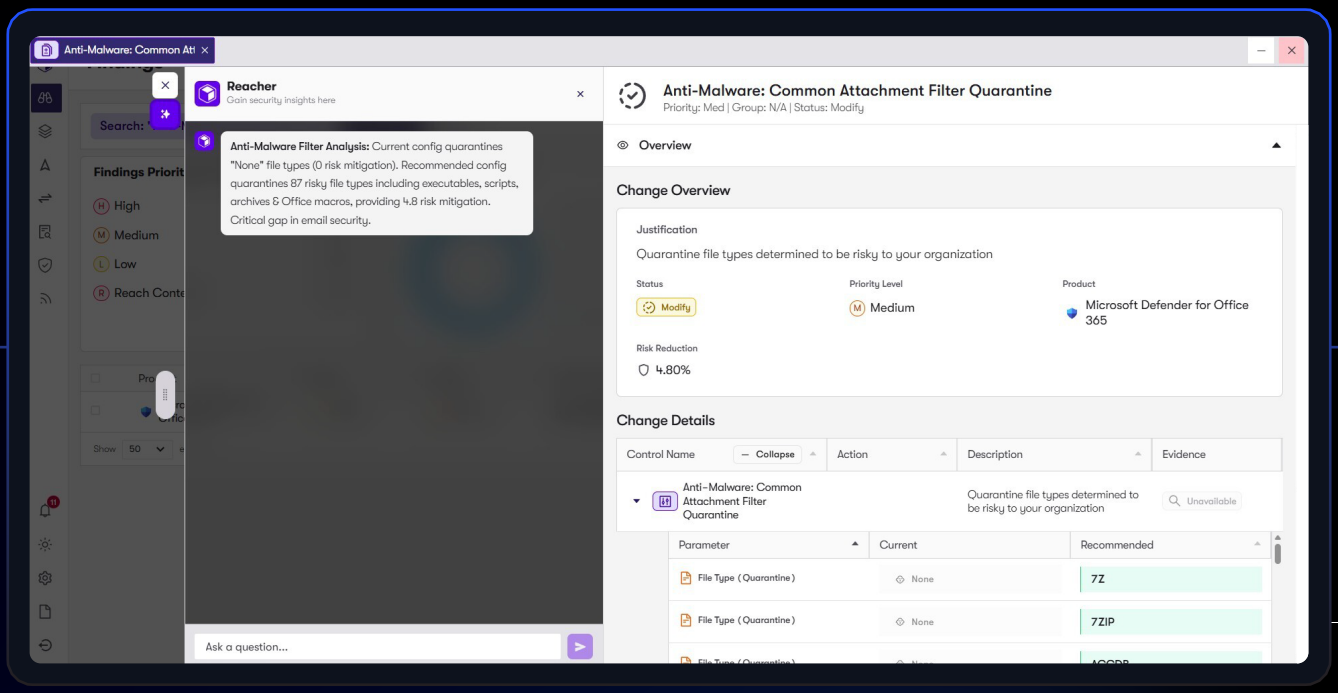
Malicious attachments remain one of the most common vectors for malware, ransomware, credential stealers, or initial compromise. Without blocking or sandboxing, simply receiving an email can lead to breach.

The control:

Email security gateways typically support blocking of dangerous file types, sandboxing of attachments, pre-delivery scanning, quarantining of suspicious files, or policy-based restrictions on executables / script-enabled files.

How Reach Security helps:

- Reach audits your email gateway configuration to verify whether dangerous file types are blocked or sandboxed. Reach analyzes data from email security gateways to better understand the types of malicious emails being delivered to users and the associated malicious file types.
- Reach can prioritize attachment blocking decisions that best protect users and align with real-world threats, and can implement stricter file-type restrictions or sandbox attachments before delivery.
- Result: you reduce the risk of malware or ransomware entering via email, which is one of the most common initial compromise vectors.



Reach identifies a misconfigured attachment filter quarantine control for file types determined to be risky and recommends a configuration modification on Microsoft Defender for Office 365 that would quarantine 87 risky file types, including executables, scripts, archives, and Office macros.

Identify Misconfigurations, Prioritize Action, Remediate, and Continuously Validate

Security tools are only as strong as their configurations allow them to be. Every default left unchallenged, every policy left generous, every gateway that quietly permits anonymized traffic, and every endpoint with soft protections adds up to systemic exposure.

Configuration hygiene is not a "set-and-forget" exercise. As tools evolve, staff change, workloads shift, and business priorities evolve, security settings must evolve too.

Exposure assessment and configuration management is an ongoing discipline that requires continuous audits, baseline reviews, custom hardening, and policy tuning for your actual risk profile.

The reality is that deploying more tools doesn't necessarily make you safer. Configuring them correctly – and maintaining and continuously validating that configuration – does.

A Configuration Hygiene Checklist for 2026

Here's your quick remediation checklist for 2026, aligned to the 10 misconfigurations above:

- [ ] Enable tamper protection for all EDR/XDR agents on endpoints.
- [ ] Block anonymizers, proxies, TOR exit nodes, and suspicious external networks at network gateways.
- [ ] Enable "Safe Links" / URL rewriting / click-time scanning in email security.
- [ ] Set maximum session durations / require re-authentication for high-risk logins in IAM tools.
- [ ] Audit external IP ranges / ASNs communicating with your environment; block or monitor unused or suspicious networks.
- [ ] Enable SSL/TLS inspection (decryption) and apply web-security / URL-filtering policies.
- [ ] Deploy credential-phishing detection capabilities on email and web gateways.
- [ ] Require MFA not only at login, but also for password changes, device enrollments, admin operations, and device joins.
- [ ] Build and deploy custom detection / on your EDR/XDR platforms.
- [ ] Block or sandbox unsafe file types and attachments in email gateways.