WHITEPAPER

# THE BIG GAP

## IN CYBERSECURITY

What security teams miss about insider risk.

www.netclean.com

NetClean.

# WHY YOU MUST READ THIS GUIDE

**Organizations today invest millions in EDR solutions, SIEM platforms, and IAM frameworks. Yet while security teams perfect their external defenses, the most dangerous vulnerabilities often exist within the organization itself.**

Insider risk is frequently misunderstood. It rarely takes the form of corporate sabotage or espionage. More often, it originates with trusted employees whose personal behaviors – online or offline – create critical security liabilities.

These behaviors can go far beyond poor password hygiene or clicking suspicious links. In some cases, individuals engage in high-risk activities that not only violate company policy but also make them uniquely susceptible to external manipulation. This creates an ideal scenario for coercion and blackmail, turning insiders into active vulnerabilities.

When individuals use corporate devices or networks to engage in inappropriate, high-stakes behavior, they open a gateway for threat actors. These actors don't need to breach technical defenses when they can exploit personal shame, secrecy, or legal exposure to compel access from within.

Such activities are rarely flagged by conventional security tools. They are often discovered only after a breach or by accident, leaving organizations exposed and unprepared.

This is not an edge case. It is a pervasive and growing concern. With increasing digital access, blurred work-home boundaries, and more distributed workforces, this form of insider risk continues to expand.

Security leaders must recognize this behavioral vulnerability for what it is: **a potent and under-addressed blind spot.**

In this guide, you will learn how leading organizations mitigate this gap before adversaries exploit it. →

# NAVIGATION

001

## HUMAN RISK:

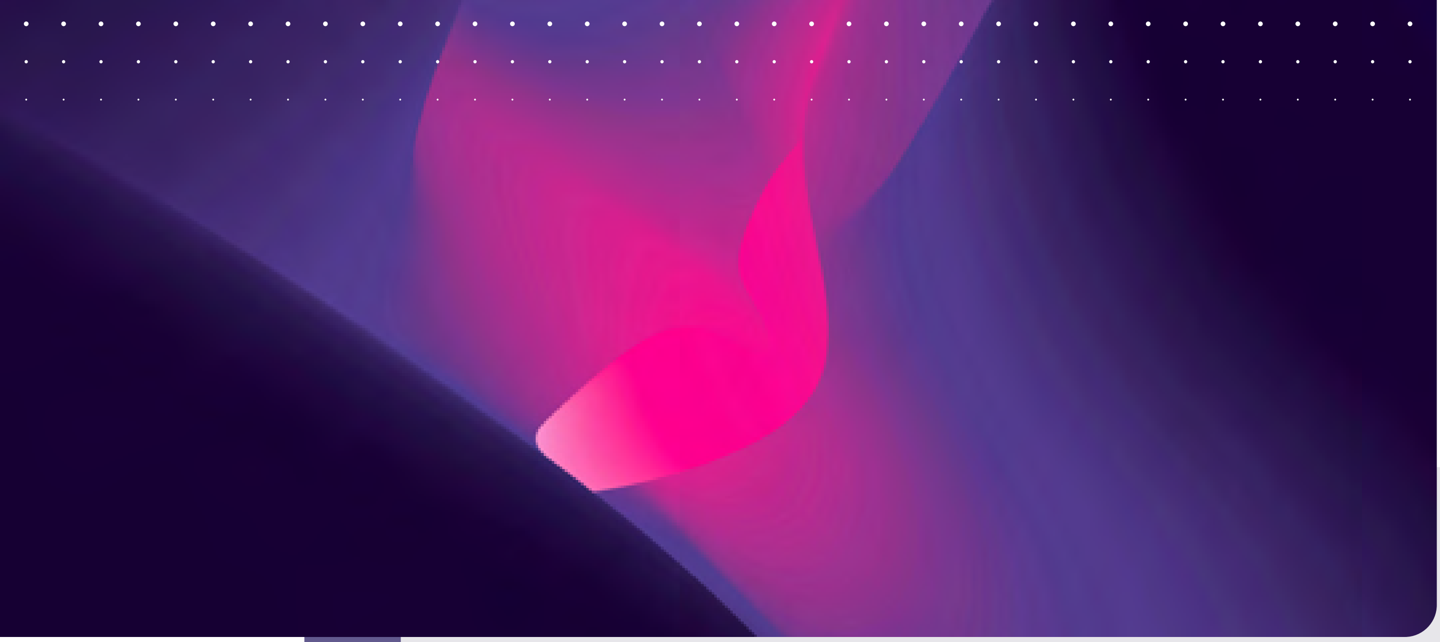
# THE BIGGEST THREAT TO YOUR SECURITY

Imagine your organization as a digital fortress. You've built high walls through firewalls, stationed guards via access controls, and deployed sophisticated detection systems through your SIEM platforms. From the outside, it appears impenetrable.

But what if the greatest danger isn't trying to scale your walls – it's already prowling within them? State-sponsored threat actors in countries like Russia and China have increasingly recognized this vulnerability as a highly effective attack vector. Intelligence reports indicate they actively target employees with compromising behavior as recruitment opportunities.

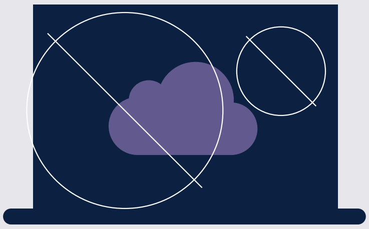
Meanwhile, technology trends have amplified this risk. Remote work, personal device integration, and cloud services have created unprecedented opportunities for employees to access illegal content using corporate resources without detection.

While traditional security tools focus outward, these sophisticated adversaries focus inward, exploiting the one threat your expensive security stack cannot see.



## Why your security tools can't see the biggest risk

Traditional security technologies excel at blocking unauthorized access, but often remain blind to high-risk activities happening within your perimeter. These security gaps exist because:



1. Multiple tools create analytical islands that can't be shared between systems
2. Security tools generate far too many false positives
3. Local storage on endpoints remains difficult to monitor
4. High-risk content hidden in personal folders evades detection
5. Behaviors that create coercion vulnerabilities aren't tracked by conventional tools

This blind spot is where sophisticated attackers focus. Rather than breaching your fortified perimeter, they identify and exploit humans who already have legitimate access.

## What makes insider risk so dangerous

Insider threat is not limited to either disgruntled or poorly security trained employees. The more insidious risk comes from the subset of users whose personal behavior creates security vulnerabilities - which cannot be addressed through traditional safeguards.

When individuals engage in high-risk activities or access inappropriate content on corporate systems, they create perfect leverage for blackmail. Under coercion, a compromised insider can:

- Hand over their trusted credentials
- Disable security systems or share their knowledge of security controls
- Create backdoor access
- Escalate privilege
- Exfiltrate sensitive data without triggering alerts

These actions often bypass security controls because they originate from authorized users performing technically legitimate functions.

## The escalating cost of doing nothing

The consequences extend far beyond immediate data loss. Regulatory penalties, reputational damage, and operational disruption compound the impact. Yet many organizations hesitate to implement detection, concerned about privacy implications.

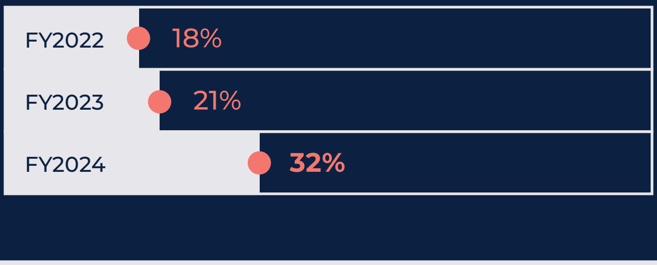
Solutions like NetClean directly address this concern by using precise detection that targets only confirmed illegal content. Unlike broad monitoring systems, this technology identifies exactly what matters most while respecting privacy boundaries.

The vulnerability is now proactively addressed - with zero false positives, and without broad infringement on employee privacy.

### This risk has doubled

32% of insider incidents last year involved insiders collaborating with a malicious outsider.

Source: DTEX and Ponemon Global Report 2025



002

## THE INSIDER THREAT IN PRACTICE:

# HOW IT HAPPENS AND WHY IT'S SO DANGEROUS

Insider threats don't appear out of nowhere. They evolve through specific patterns, following three distinct pathways to compromise.

## The anatomy of an insider threat

Every insider risk falls somewhere along a critical spectrum:

- **Unintentional:** Risk without intent, mishandling data, falling for phishing, or breaking rules to save time.
- **Compromised:** Trustworthy individuals forced into becoming threats due to personal vulnerabilities.
- **Malicious:** Intentional insiders seeking to harm, evade detection, and cause maximum damage.

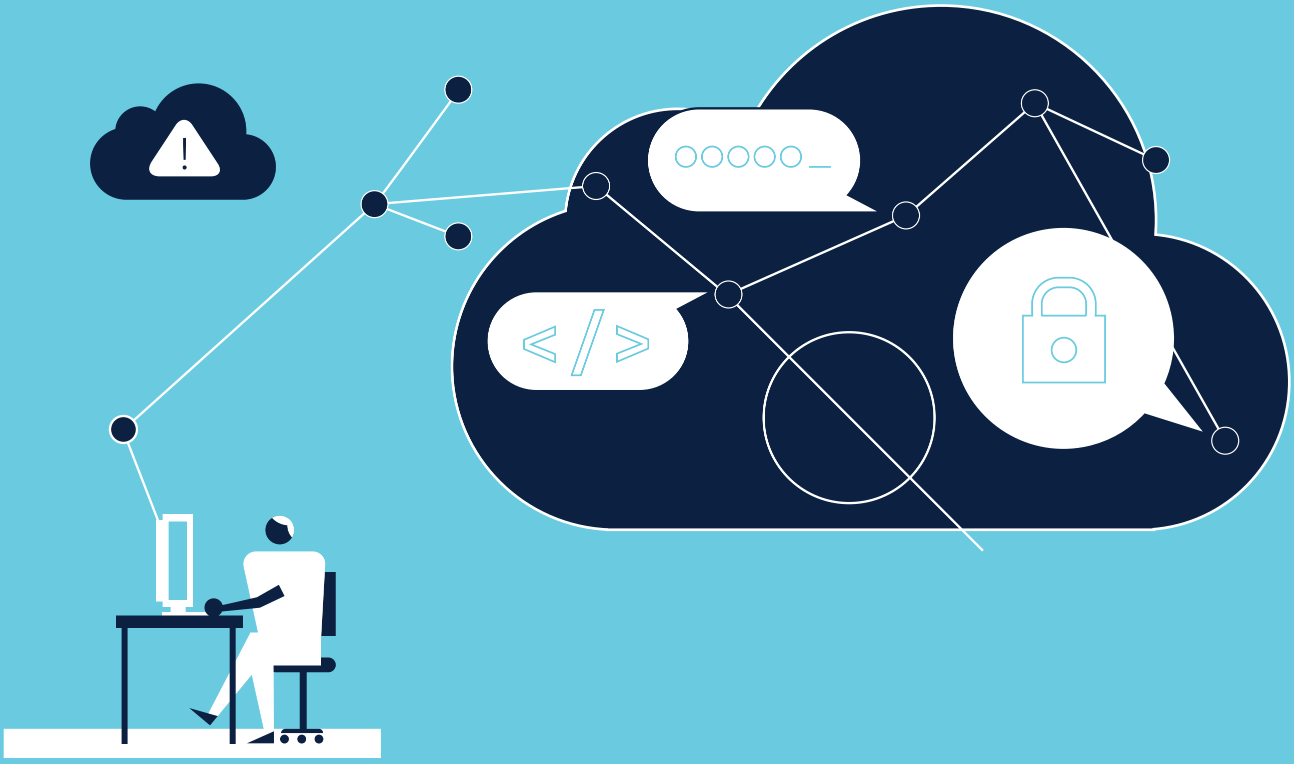
The most dangerous insider isn't always the unintentional, accidental, or malicious staff member.

It's the compromised trusted employee who, through coercion, blackmail, or other threat, is pressured into actions that are targeted and conceived by a malicious third party.

## How personal risk becomes organizational exposure

What begins as a personal behavior, such as accessing illegal content, creates the perfect recruitment opportunity.

These individuals become targets not because of who they are – but because of what they've done. State-sponsored attackers from Russia and China, as well as sophisticated criminal groups, excel at identifying these vulnerabilities. With evidence of illegal or compromising behavior, they apply quiet pressure. The target complies because the alternative, exposure, appears worse than cooperation. The result isn't an external threat. It's an embedded, persistent vulnerability hiding in plain sight.



# WHY THE RISK HAS INCREASED

## Several factors have amplified this threat in recent years:

**Remote work:**

Corporate devices now operate on home networks, adjacent to personal devices, with blurred boundaries between professional and personal use. This makes it easier for high-risk behaviors to occur on corporate assets.

**Enhanced surveillance capabilities:**

Foreign intelligence services have dramatically improved their ability to identify and exploit personal vulnerabilities.

**Increasing digital footprints:**

Employees leave more traces of their activities than ever before, creating more potential leverage points.

## The perfect recruitment scenario

When the leverage involves deeply personal behavior and the risk of exposure is devastating, compromised insiders rarely report what's happening. They comply.

> They're not spies. They're trapped.
> They have access. They stay silent.

And they become what counterintelligence agencies call: the perfect recruitment scenario.

## The cascade of consequences

Once compromised, these insiders can:

- Introduce **malware** by visiting high-risk websites
- Share **credentials** with attackers
- Disable **security controls** to cover their tracks
- Use **encryption or VPNs** to smuggle data out undetected

These actions bypass conventional security precisely because they involve legitimate users performing technically authorized functions, ultimately making them the most difficult threats to detect and mitigate.

## THE MARKET SHIFT:

# INSIDER RISK AS A STRATEGIC PRIORITY

## Forward-looking organizations are already acting

While most security teams still focus on perimeter defense, forward-looking security leaders have shifted their attention inward. They recognize that the most dangerous threats aren't attempting to break in. They already have legitimate access.

Since 2023, global spending on insider risk technologies has more than doubled. This acceleration isn't driven by fear, but by strategic recognition: insider risk represents the last major blind spot in modern cybersecurity frameworks.

## Why 2025 marks a turning point

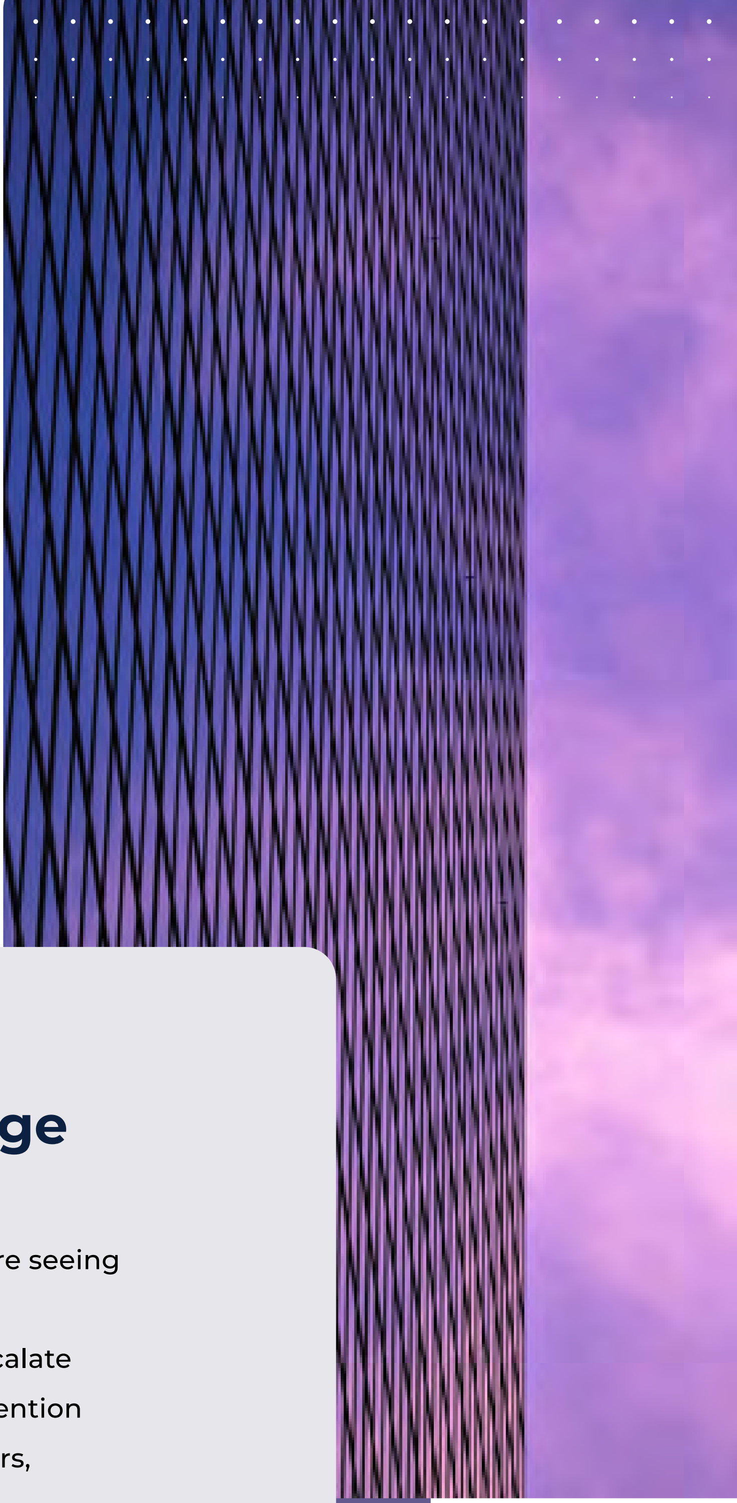
Security analysts point to 2025 as a pivotal year for insider risk management as multiple trends converge:

- Detection technologies have reached new levels of precision and scale, with solutions like NetClean ProActive leading innovation in targeted illegal content detection
- Human risk indicators are being integrated into core security operations
- Regulatory expectations are expanding across regions and industries
- Boards are demanding visibility into people's vulnerabilities inside the firewall
- Threat actors are increasingly targeting people, rather than systems

This convergence is already reshaping security priorities and boardroom conversations. Organizations waiting for clearer signals will soon find themselves reacting rather than leading.

> Organizations can no longer afford to ignore what's happening inside the firewall.

Anna Borgström
CEO, NetClean



## From technical issue to strategic imperative

Insider risk has evolved from an isolated IT concern to a cross-functional business challenge. It now features prominently in discussions about compliance, governance, and organizational resilience.

Executive teams increasingly recognize that insider threats affect data protection, legal and regulatory exposure, operational stability, and stakeholder trust. In leading organizations, insider risk is reported alongside other business-critical risks, appearing in leadership briefings rather than being ignored or buried in technical dashboards.

## The competitive advantage of early adoption

Organizations addressing insider risk proactively are seeing measurable benefits:

- Earlier threat identification before incidents escalate
- Reduced incident response costs through prevention
- Enhanced stakeholder confidence from investors, clients, and regulators
- Streamlined compliance with evolving regulatory frameworks
- Improved resilience against sophisticated threat actors

While reactive organizations scramble to implement solutions under pressure, early adopters build systematic approaches aligned with their broader security strategy.

# SETTING THE NEW BASELINE FOR MATURE SECURITY

Every year widens the gap between organizations treating insider risk as a strategic priority versus those viewing it as tomorrow's problem.

Early adopters aren't merely implementing technology. They're developing institutional knowledge, establishing processes, and defining best practices before these become industry standards. In the years ahead, organizations won't just be evaluated on whether they addressed insider risk, but how early they recognized its importance.

In a security landscape where threats constantly evolve, addressing insider risk isn't just about prevention. It's about organizational maturity, leadership foresight, and strategic positioning.

## NetClean

With NetClean, users are able to identify, investigate and remediate cyber risk triggered by CSAM material. The solution bridges an existing security gap by identifying deliberate actions that can compromise company assets. It acts as a red flag for known threats.

004

## THE MODERN APPROACH:

# RETHINKING DETECTION WITHOUT OVERREACH

**The biggest barrier to addressing insider risk isn't technical complexity. It's an organizational perception.**

Too many organisations hesitate to implement insider risk detection because of misconceptions around cybersecurity education being sufficient, or due to concerns about employee privacy. Executive, HR and Legal teams may worry that effective detection will necessitate invasive monitoring. This false dichotomy between security and privacy leaves organisations stuck and vulnerable.

Modern insider risk detection works differently. Rather than broad surveillance, it uses precise detection of specific high-risk indicators. Solutions like NetClean's ProActive technology trigger only on confirmed illegal content, not general behavior patterns or communications.

This targeted approach preserves privacy while addressing critical security gaps. Enabling organizations to identify serious vulnerabilities without undermining trust or compromising operational efficiency.

Leading organizations are implementing these solutions today, not just because the technology exists, but because they recognize there's no longer a legitimate reason to leave this significant vulnerability unaddressed.

### The risk is human

**60%** of cybersecurity incidents involve the human element.

Source: Verizon DBIR Report 2025

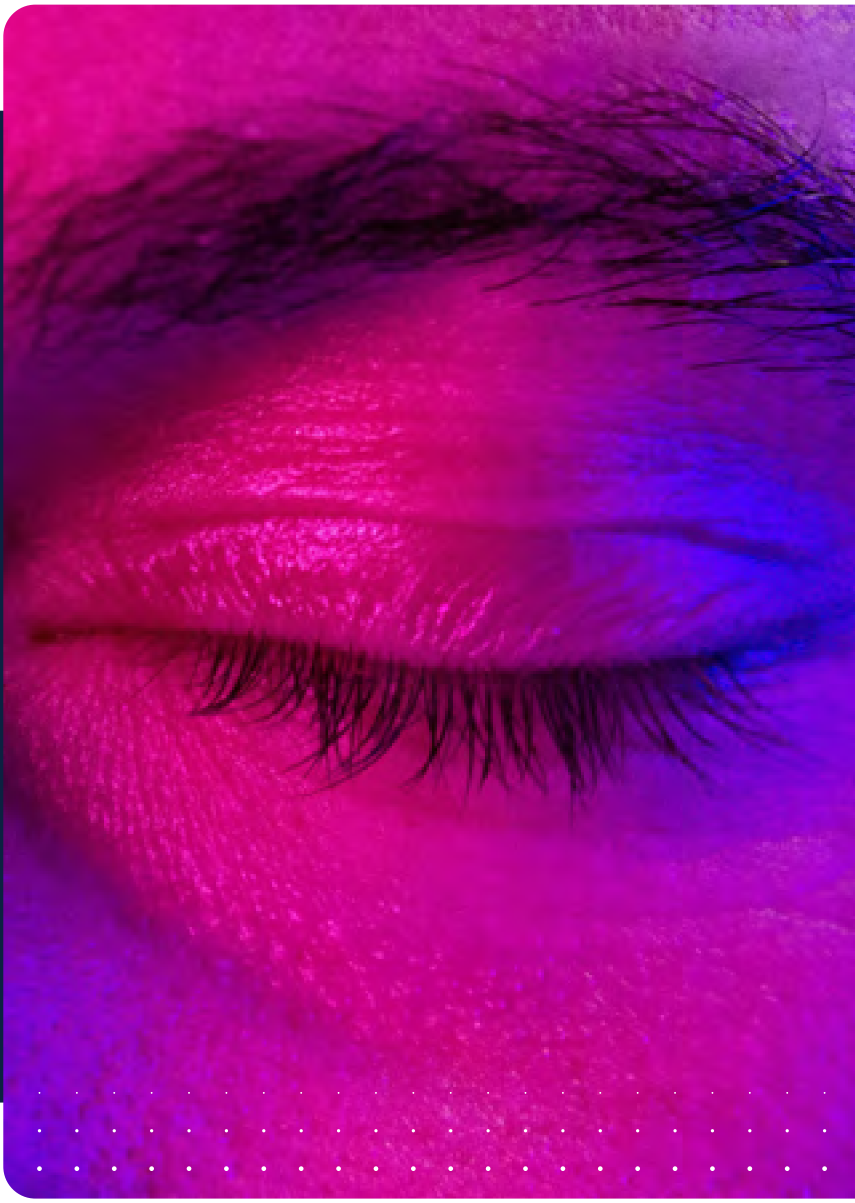
005

# WHERE DOES INSIDER RISK FIT IN YOUR COMPLIANCE FRAMEWORK?

## The compliance blind spot

Insider threats have evolved from purely security concerns to critical compliance issues. While existing frameworks primarily focus on external threats, they increasingly encompass risks from within.

Traditional compliance frameworks already contain the foundation for insider risk management – what's often missing is specific attention to this particular vulnerability and implementation of targeted controls to address it.



## NIST AND ISO/IEC 27001:

# INSIDER RISK IS ALREADY THERE

Though frameworks such as NIST Cybersecurity Framework and ISO/IEC 27001 may not explicitly highlight “insider threat,” their controls already address these risks.

Core requirements around monitoring personnel activity, identifying internal threats, and protecting against unauthorized access directly apply to insider risk management.

Implementing insider risk detection strengthens these controls through targeted, high-precision monitoring focused on specific risk indicators. This approach delivers auditable, proportionate responses that align with existing compliance requirements.

## Privacy-aligned by design

Modern detection tools for illegal content, like NetClean ProActive, operate with privacy at their core. Unlike broad-based monitoring, these solutions:

- Operate passively in the background
- Trigger only on corroborated high-risk indicators
- Don't track user behavior or communications
- Process minimal personal data - typically only identifying information when a confirmed risk is detected.

This privacy-centric design makes them compatible with GDPR and similar regulations, especially when supported by documented legal assessments like Legitimate Interest Assessments (LIA).

## Sector-specific compliance requirements

**In highly regulated industries, insider risk management is becoming an explicit expectation:**

**Financial services** regulations increasingly require monitoring for insider risks.

**Healthcare** compliance frameworks mandate the protection of sensitive patient data.

**Critical infrastructure** regulations emphasize insider threat controls.

**Government and defense** contractors face stringent insider risk requirements.

Whether addressing PCI DSS, HIPAA, or national security directives, insider risk detection strengthens controls that traditional perimeter security alone cannot satisfy.

## Demonstrating Due Diligence

Beyond technical compliance, implementing insider risk detection demonstrates organizational diligence to key stakeholders. It shows regulators, business partners, and customers that your security program addresses the full spectrum of threats.

As regulatory expectations continue to evolve, organizations that proactively incorporate insider risk into their compliance frameworks will be better positioned to meet new requirements while avoiding remediation costs and potential penalties.

006

# THE NETCLEAN SOLUTION:

# PRECISION DETECTION FOR A CRITICAL INSIDER RISK

## The vulnerability all others miss

High-risk personal behaviors on corporate devices create the perfect insider threat – devastating if exploited, invisible to standard security tools, and often difficult to address.

This gap leaves organizations exposed to one of the most powerful coercion vectors available to adversaries.

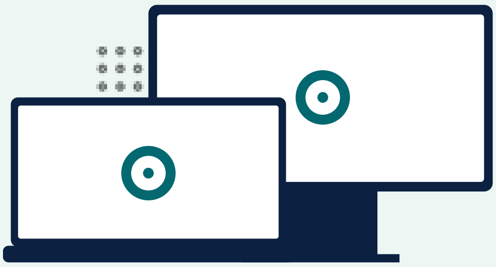
## How NetClean ProActive Works

**NetClean ProActive addresses this vulnerability with unmatched precision:**

→

- Specifically designed to detect Child Sexual Abuse Material (CSAM) using verified signatures
- Operates with zero false positives – when it alerts, the risk is already confirmed
- Runs covertly, requiring minimal resources
- Preserves privacy while eliminating critical security gaps

The solution strengthens compliance across NIST, ISO 27001, GDPR, and industry-specific frameworks by detecting what no other security tool can see. It deploys quickly across any environment, scaling from hundreds to thousands of endpoints without disruption.



# CLOSE THE GAP

The threat is real and active.

## Your current security defenses can’t detect it.

## But NetClean can.

Protect your organization from this hidden vulnerability before it’s exploited.

With NetClean ProActive, you address one of the most dangerous insider risks with certainty, in full compliance, and without compromising privacy values.

Contact us

NetClean.

netclean.com
info@netclean.com