AI-powered threat detection and response combats IP theft in the high-tech industry

Find threats that matter, faster

By 2027, the global cost of cybercrime, such as IP theft, is estimated to reach more than $23 trillion (up from roughly $8 trillion in 2022)[1] according to intellectual property law firm Mandelbaum Barret PC. highlighting the critical need for strong IP protection. It's a problem that is exacerbated within the high-tech industry.

In 2023, two former Tesla employees leaked the personally identifiable information (PII) of more than 75,000 current and former Tesla employees to a German newspaper. It wasn't the first insider threat incident for Tesla, which had previously been the victim of extensive data exfiltration of its intellectual property (IP) and sabotage and another incident in which an employee was bribed to facilitate a ransomware attack. Tesla isn't alone. The high-tech industry is particularly vulnerable to insider attacks due to its unique characteristics, including the high value of intellectual property (IP), extensive reliance on data, and complex internal networks. There are several reasons for this vulnerability:

1. High value of intellectual property (IP)

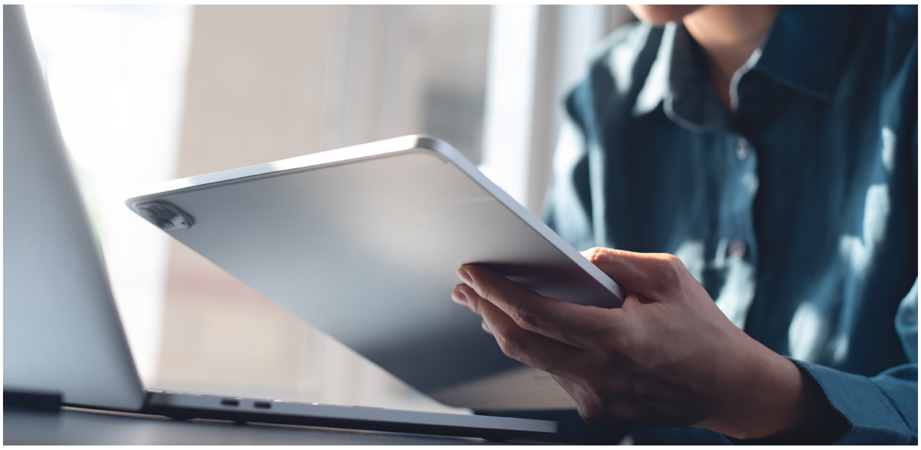
Significance of IP: High-tech companies often develop cutting-edge technologies and products, making their IP highly valuable and a prime target for theft or sabotage.

Motivations for theft: Insiders may steal IP for personal gain, to benefit competitors, or to aid foreign entities engaging in corporate espionage.

2. Extensive access to sensitive information

Broad access: Employees, contractors, and partners often have significant access to sensitive systems, proprietary data, and trade secrets.

Challenges in monitoring: It can be difficult to distinguish between legitimate work-related access and malicious activity, especially in dynamic environments.



[1] Mandelbaum, Barret PC, *Protecting Intellectual Property in the Digital Age*, 2024

One in three CEOs cited cyber espionage and loss of sensitive information or intellectual property as their top concerns for 2025[2]—for good reason. According to a recent Forbes article, intellectual property theft alone accounts for billions of dollars in annual losses.[3]

3. Collaboration-driven culture

Shared resources: The industry thrives on collaboration and open communication, often requiring shared access to proprietary tools and datasets.

Potential exploitation: This culture can be exploited by malicious insiders who take advantage of trust and open access.

4. Workforce dynamics

High turnover rates: The competitive nature of the high-tech industry results in frequent employee movement between organizations, increasing the risk of IP theft when employees leave.

Disgruntled employees: High-pressure work environments can lead to job dissatisfaction, increasing the likelihood of sabotage or data theft by disgruntled employees.

5. Rapid innovation and short product cycles

Competitive pressure: High-tech companies are under constant pressure to innovate, making them targets for competitors looking to gain an edge.

Targeted theft: Insiders may steal early-stage research or designs to sell to competitors or start their own ventures.

6. Insider motivations

Financial incentives: Malicious insiders may be motivated by financial gain, selling stolen IP or sensitive information to competitors or foreign entities.

Espionage: State-sponsored actors often recruit insiders to steal proprietary technologies critical to national interests.

Ideological or personal reasons: Insiders may act out of a desire for revenge, to expose perceived wrongdoing, or due to ideological motivations.

7. Complex supply chains

Third-party risks: The high-tech industry relies on extensive supply chains and contractors, creating additional touchpoints for potential insider threats.

Weak links: Third-party vendors with less stringent security protocols can become entry points for insider attacks.

8. Difficulty in detection

Sophisticated actors: Insiders often understand the organization’s systems and security measures, enabling them to bypass detection.

Subtle behaviors: Insider threats are often harder to identify than external attacks, as they can blend in with legitimate activity.

[2] World Economic Forum, *Global Cybersecurity Outlook* 2025, 2025

[3] Forbes, *Protecting Intellectual Property in a Borderless World*, 2024

The rapid rise of GenAI poses increased cybersecurity headaches for tech companies, which often operate within intricate digital ecosystems, including interconnected applications and services. This complexity can be exploited by attackers to launch coordinated GenAI-driven cyberattacks. Moreover, the prevalence of insider threats in the tech industry can be exacerbated by GenAI tools. Employees with access to sensitive information may inadvertently or maliciously use GenAI to exfiltrate data or develop exploits, increasing the risk of data breaches.

OpenText believes we must partner with security operations teams to elevate their cybersecurity maturity level in a cost-effective and non-disruptive manner. Our approach is anchored by four key principles:

1. Enable threat detection that matters:

- Without robust detection, effective response is impossible. OpenText™ Core Threat Detection and Response is built to uncover elusive threats, such as insider attacks, novel attacks, and advanced persistent threats while reducing false positives.

2. Enhance existing security posture:

- OpenText Core Threat Detection and Response is designed to complement and enhance existing security frameworks, particularly for organizations already using Microsoft Defender for Endpoint and Entra ID (and more in the future).

3. Deliver tangible value:

- Find threats others miss: Our advanced and patented (10+) behavioral analytics built on 100-percent online machine learning reveal hidden threats that evade traditional (rule-based) tools, giving organizations early and actionable detection capabilities.
- Reduce alert fatigue: OpenText Core Threat Detection and Response uses behavioral risk scoring to prioritize threats, reducing alert overload and ensuring the team focuses on high-risk activities first.
- Ease of use and lower overhead: Dynamic detection automatically evolves with a changing environment and eliminates manual adjustments that are prevalent in other tools. Cybersecurity Aviator capabilities that interpret and translate high volumes of complex security telemetry into plain language, context rich leads. Our solution helps automate threat hunting to boost operational efficiency.

4. Maximize success with expertise on tap:

- The optimal combination of technology and users often leads to success. Not only are our battle-tested threat hunters skilled in our technology, but they are also experts in finding some of the most difficult to find threats in the world. The experience gained through working with our global customers is invaluable in finding the threats that matter, faster. They provide a service that complements your existing operations and helps you maximize your technology investment.

OpenText Core Threat Detection and Response paves the path to achieve advanced cybersecurity maturity with Blue Team's success (80%+ Red Team's attack detection rate) to boot. From the current state to the future state, OpenText provides the optimal* combination of technology and expert services to accelerate the transition without disruption to your current infrastructure.

Current state	Future state
Baseline protection for known threats and simple risks.	Contextual insights into your organization's unique normal and changing risk profile.
Fear of missing high impact unknown threats in the face of rapidly changing threat landscape.	Confidence in proven AI detecting unknown threats for which there are no rules.
Insider threats often go unnoticed for 86 days, almost three months.	Reduce or eliminate remediation costs by detecting insider threats in days.
Out-of-the-box detection requiring time-consuming customization.	Threat detection optimally customized and automatically adapted to your threat environment.
Wasted human capital on low-quality and inaccurate threat leads.	Maximize your human and technological investments.

new UncaughtException(t,e,
return"function"==typeof u&&u.apply(th
(this.message=t||"Uncaught error with no additional inform
var n=e?null:c.now();i("err",[t,n])}var i=t("handle"),a=t(22),s=t("e
window.onerror=r;t
"addEventListener"in wi

According to internal OpenText customer engagements that leveraged the experience and domain expertise of our threat hunting team and the behavioral analytics capabilities in OpenText Core Threat Detection and Response.

OpenText Core Threat Detection and Response provides:

Core feature	Benefit
AI-driven advanced behavioral analytics	Understands unique organizational behavior to spot deviations that signal threats, helping you prevent data breaches, IP theft, and malicious activity.
Machine learning-based anomaly detection	Unlike most other security tools, OpenText Core Threat Detection and Response is built from the ground up using unsupervised machine learning allowing it to automatically adapts to your changing business environment, helping detect insider threats and rogue actor activities without additional configuration.
Seamless integration with Microsoft Defender for Endpoint and Entra ID	Integrate directly with Microsoft security tools like Defender for Endpoint and Entra ID, leveling up advanced threat detection by providing unique behavioral insights, enhanced risk context, and streamlined security operations.
Risk scoring for threat prioritization	It takes almost 90 days to detect an insider threat, that's almost three months. Prioritizes high-risk threats like malicious insiders, with behavior-based risk scoring, reducing alert fatigue and helping teams focus on the most critical incidents in days, not months.

How OpenText Threat Detection and Response addresses industry-specific challenges

OpenText Threat Detection and Response enables technology companies to significantly enhance the protection of sensitive IP and R&D data by detecting anomalous behavior and insider threats before intellectual property can be compromised. It enables high-tech firms to safeguard proprietary information and maintain competitive advantage.

Next steps

Learn more about what OpenText Core Threat Detection and Response can do for your cyber defence.