opentext™

POINT OF VIEW

AI-powered threat detection and response in the financial services industry

Find threats that matter, faster

Industry backdrop

Financial services organizations are under attack and the consequences are severe:

- **Loss of sensitive data:** Financial data, personally identifiable information (PII), and trade secrets are prime targets.
- **Compliance costs:** Breaches trigger investigations and reporting under regulations like GDPR and PCI DSS.
- **Fraud and identity theft:** Stolen data often leads to fraudulent transactions and identity theft, costing financial institutions millions.
- **Customer attrition:** Customers are likely to switch to competitors if they lose trust in a bank's ability to secure their data.
- **Reputational damage:** Breaches erode trust and tarnish a brand's credibility, impacting customer retention and future business opportunities.

The financial industry experienced an average data breach cost of $6.08 million in 2024, up from $5.90 million in 2023, indicating a rising financial impact within the sector.[1]

A significant source of exposure is employees with access to sensitive files. As of 2021, a financial services employee had access to an average of 11 million files, with more than 64 percent of financial services companies having more than 1,000 sensitive files accessible to every employee.[2]

Negligent employees can be manipulated into exploiting this access leading to significant losses. The human element is involved in three out of every four breaches[3] and these insider threats have become a top cyber defense priority. To further complicate matters, malicious insiders are carrying out planned data exfiltration.

Meanwhile, there's a notable shortage of skilled cybersecurity professionals, influencing the effectiveness of cybersecurity defense. The global cybersecurity workforce gap reached a new high in 2024, with an estimated 4.8 million professionals needed to effectively secure organizations, a 19-percent year-on-year increase.[4]

Limited resources can also hinder the cybersecurity team's ability to implement comprehensive security measures and maintain round-the-clock vigilance. Eighty percent of CISOs report that they do not have sufficient funding to implement robust cybersecurity measures.[5]

Addressing these challenges requires a multifaceted approach that includes advanced threat detection technologies, continuous staff training, and robust incident response strategies.

1 Statista, *Cost of data breaches in financial industry worldwide*, 2024

2 Varonis, *82 Must-Know Data Breach Statistics*, 2024

3 Verizon, *2023 Data Breach Investigations Report: Frequency and cost of social engineering costs skyrocket*, 2023

4 ISC2, *Growth of Cybersecurity Workforce Slows in 2024 as Economic Uncertainty Persists*, 2024

5 Forbes, *Want To Win The Cybersecurity Battle? Start By Supporting Your CISO*, 2024

The rise of generative AI (GenAI) presents both opportunities and significant threats to the financial services industry. While GenAI offers innovative solutions for fraud detection, customer support, and risk assessment, its misuse by malicious actors can create new vulnerabilities. Here's an overview of the threats posed by GenAI:

- Advanced phishing and social engineering : GenAI can generate highly convincing phishing emails, voice calls, or deepfake videos that mimic trusted individuals or institutions.

The impact: increased success rates of phishing attacks, leading to credential theft, unauthorized transactions, or data breaches.

- Code generation for cyberattacks : GenAI can assist cybercriminals in writing malware, automating ransomware attacks, or finding vulnerabilities in financial systems.

The impact: Increased frequency and sophistication of cyberattacks targeting financial institutions.

- Insider threat amplification: Insiders with malicious intent could misuse GenAI to automate data exfiltration or generate convincing cover stories.

The impact: Increased risk of insider threats and data breaches.

Open Text vision

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 prevalent in other tools. Cybersecurity Aviator capabilities 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 identifying some of the most difficult to find threats in the world. The experience we have gained through working with our global customers is invaluable in finding the threats that matter, faster. Our threat hunting experts provide a service that complements your existing operations and helps you maximize your technology investment.

Business outcome

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 your transition without disruption to your 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.

OpenText Core Theat 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 adapt to your changing business environment, helping detect insider threats and rogue actor activities without additional configuration.
Seamless ontegration with Microsoft Defender for Endpoint and Entra ID	Integrate directly with Microsoft security tools, such as 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. OpenText Core Threat Detection and Response prioritizes high-risk threats, such as malicious insiders, with behavior-based risk scoring, reducing alert fatigue and helping teams address most critical incidents in days rather than months.

OpenText Threat Detection and Response enables financial institutions to enhance their ability to protect client data, maintain regulatory compliance, and prevent unauthorized access to sensitive information. With advanced round-the-clock behavior monitoring that adapts to a changing environment, financial services organizations can detect irregular user patterns to uncover hard-to-detect attacks or emerging threats from within, reducing the likelihood of costly damage to their bottom lines and reputations.

Next steps

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

opentext™