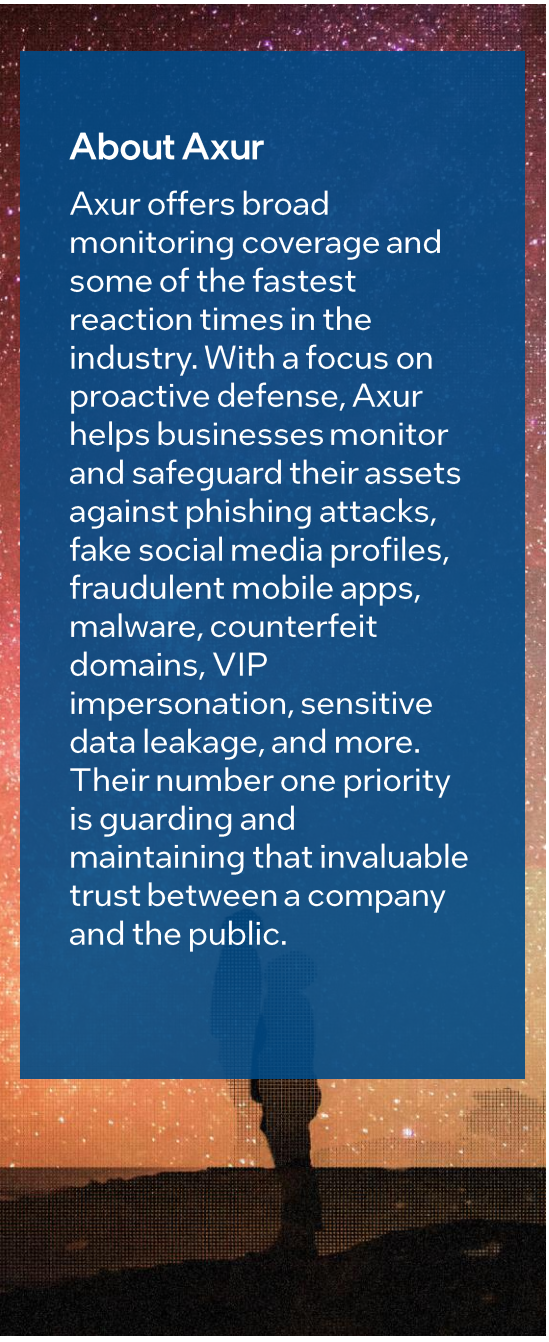
Solution Brief

Forensic Threat Intelligence
Situational Monitoring

Fortifying Businesses With External Cyber Threat Intelligence To Stop Fraud And Reduce The Costs Of Cybercrime

Axur's Digital Risk Protection solution leverages Intel® technology to address external cybersecurity risks and allow businesses to proactively protect their brand and assets.

accelerated by intel



About Axur

Axur offers broad monitoring coverage and some of the fastest reaction times in the industry. With a focus on proactive defense, Axur helps businesses monitor and safeguard their assets against phishing attacks, fake social media profiles, fraudulent mobile apps, malware, counterfeit domains, VIP impersonation, sensitive data leakage, and more. Their number one priority is guarding and maintaining that invaluable trust between a company and the public.

The Unfortunate Reality of Cyber Fraud

As technology advances so do cybercriminal methods and capabilities. It is no longer feasible to expect that a company can protect itself and its customers just through firewalls and company mandated security trainings. During the pandemic, companies worldwide were compelled to digitize their assets to maintain market share. This shift has enabled cybercriminals to expand digital schemes involving companies' and consumers' information, like selling leaked credit or debit card information, corporate credentials with privileged access, database samples, and more.

Cybersecurity challenges

Global cost of cybercrime is expected to rise from $8.44 trillion in 2022 to $23.84 trillion by 2027.[1]

More than 40% of data breaches involved internal actors. It's estimated that half of all data breaches that involve internal actors are intentional, while the other half are accidental.[2]

In 2021 the average lifecycle of a data breach, from identification to containment, was 287 days. Just identifying a cybersecurity breach took around 212 days.[3]

Whether it's an international conglomerate company or a small local business, cybercriminals and fraudsters are continuously looking for ways to exploit businesses and their customers for profit. As a matter of fact, it's been reported that as many as 43% of cyberattacks are targeted towards small businesses.[2] This problem is not isolated to specific industries or sectors. Nearly all businesses are susceptible to cyberattacks, whether they house data online or not. Cybercriminals plan their schemes online, targeting all industries from finance and ecommerce to manufacturing. To stay ahead of cybercrime, businesses need a more proactive approach to cybersecurity and that means identifying fraud before attacks occur – the kind of detection and analysis Axur experts can help provide.

Axur Digital Risk Protection Solution

Axur is a leading digital risk prevention, protection, and fraud intelligence solutions provider. The Axur platform leverages AI models to monitor, analyze, and react to digital cybercrime schemes that mention customers and key terms on different web signals. Their innovative SaaS platform helps companies proactively protect their assets outside their firewalls and provides exceptional visibility into surface, deep, and dark web cyber risks.

Serving as an expert cybersecurity assistant, Axur provides key information and enables businesses to act on cybercriminal schemes and identify leaked information. To garner an accurate threat diagnostic, they monitor more than 9000 internet environments in search of fraudulent and illicit activities pertaining to users.[4] By analyzing data based on pre-established criteria and machine learning capabilities, Axur determines a risk score for each potential threat and enables cybersecurity teams to prioritize the most relevant information.

The Axur system collects hundreds of thousands of messages that fraudsters exchange daily across diverse environments. These messages go through a processing pipeline that streamlines information into digestible and actionable reports:

Identification of topics: Filters irrelevant conversation points so the exchanged messages reflect an accurate depiction of the risk.

Normalization and translation: Converts terminology and slang to a more formal, readable text.

Summarization: Groups messages according to their topics and time windows, then summarizes the information in bullet points via a large language model (LLM). The summarized messages are shown to the users, who can quickly overview what is being discussed about their companies without reading thousands of messages. Users can click on any bullet point and read the original messages to access more details.

Simple and fast to deploy, the system runs in AWS cloud with no hardware or software installation required. Typical deployments consist of creating access credentials and setting up the terms the user needs to monitor (brands, products, assets, etc.).

Axur users can also choose to request the removal of fraudulent or filtered content through takedowns, which can be automated or completed manually with a single click. By automating the takedown of deceptive content and leveraging machine learning, Axur helps ensure real-time mitigation of risks to digital assets.

Key Features

- Multi-environment monitoring and triage
- Optical character and image recognition
- Logo detection
- LLM and generative AI based summary
- National Institute of Standards and Technology framework applied automatically with artificial intelligence 24/7
- Transparency on detection statuses
- Cutting edge speed of detection, analysis, and removal
- AI-automated risk takedown

Intel Partners with Axur to Improve Performance

Through the partnership with Intel, both the embedding model used for topic identification and the LLM for summarization have been optimized to handle large volumes of messages and data. The entire solution runs on the cloud, and Axur chooses instances that use Intel hardware to benefit from the performance improvements. By leveraging Intel® technologies Axur was able to increase process performance without increasing costs.

Intel has played a key role in the optimization of Axur's OCR model that is used to read text from images. The OCR extracted texts are used in the summaries presented to clients.

Comparing the model performance before and after using Intel® Distribution of the OpenVINO™ Toolkit, Axur observed an increase in the model inference performance (BERTopics).

By leveraging Intel technology, Axur has been able to improve platform speed and accuracy at a fraction of the cost. These efficiencies allow users to get insights faster and act quickly in the face of cyber threats.

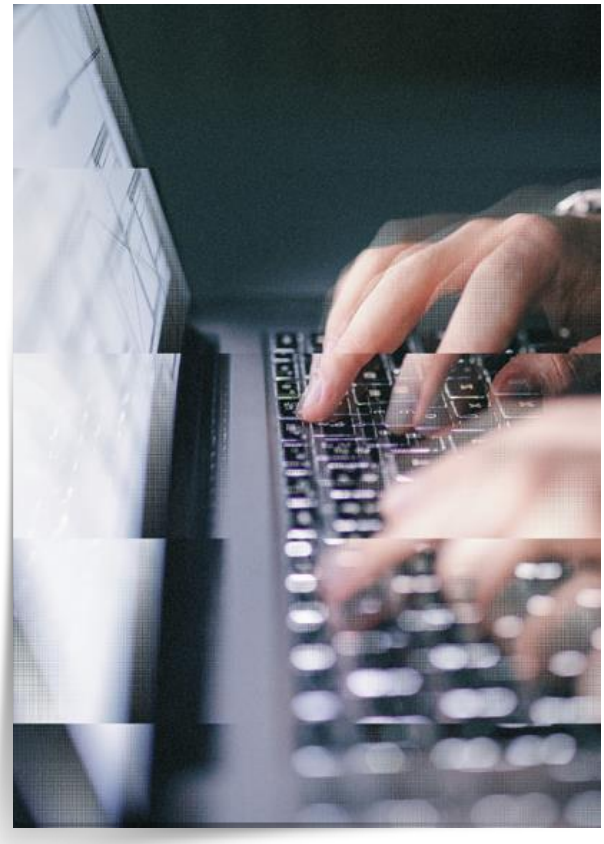
Intel® Distribution of OpenVINO™ toolkit: Intel® Distribution of OpenVINO™ toolkit is used by Axur to improve performance by expediting inference engine processing and optimizing AI for Intel platforms, so machine learning models can keep up with and process heavier loads of data. OpenVINO™ enables scaling up and down across compute power and is flexible across Intel hardware including Intel® Xeon® Scalable Processors.

Intel® Xeon® Scalable Processors: These processors are built specifically for the flexibility to run complex AI workloads on the same hardware as existing workloads. With AI acceleration and optimization that goes silicon deep and ecosystem wide, Intel® Xeon Scalable processors take embedded AI performance to the next level.

Privacy is Paramount

Users do not provide Axur with sensitive data. However, collected data may be sensitive in nature as the information being exchanged by fraudsters often consists of leaked data. Axur values the privacy of users' and customers' data, so the platform works within the Personal Data Privacy Policy framework. This framework demonstrates Axur's commitment to data protection by Law no. 13,709/2018, the "General Law on Personal Data Protection" (LGPD). Axur aims to deliver the highest levels of privacy possible and to ensure that private data is automatically protected in any information technology system or business practice. The collected messages are stored in databases in AWS with access restricted to verified users only. Users are able to search and read messages but cannot write or edit in the database.

Axur guarantees that the data used in its Digital Risk Protection platform will be captured on the internet with analysis being run only with the consent of the owner of the information. That is to say, only customers who have signed a contract with the respective consent, will have their data analyzed and processed.



Axur Digital Risk Protection in Action

MadeiraMadeira is the largest furniture and decoration online store in Latin America and operates more than 100 physical stores in Brazil. They found themselves suffering large losses in credit card chargebacks as fraudsters were purchasing furniture with stolen credit cards. To complicate things, these cybercriminals would rent a temporary location (such as an AirBnb) to receive the illegally purchased furniture. Later, MadeiraMadeira would have to return the stolen amount to the credit card owner, but without being able to recover the furniture.

At first, MadeiraMadeira was unaware of how the scheme worked and how to detect and prevent it. To understand the problem, Axur collected close to 1 million mentions of the MadeiraMadeira brand and products in online messages. Out of those, about 22 thousand were real threats, in the sense that they mentioned ongoing frauds and detailing how the scheme worked.

Thanks to Axur, MadeiraMadeira was able to extract useful information from a sea of data, understand the fraud strategy, and start mapping the scenario. Their next step was to implement additional security measures for payment and product delivery.

The customer saw a strong and quick reduction in losses from this type of fraud. Many fraudulent furniture deliveries were able to be identified and canceled. After the fact, Axur's platform found many messages from the fraudsters complaining about these cancellations.

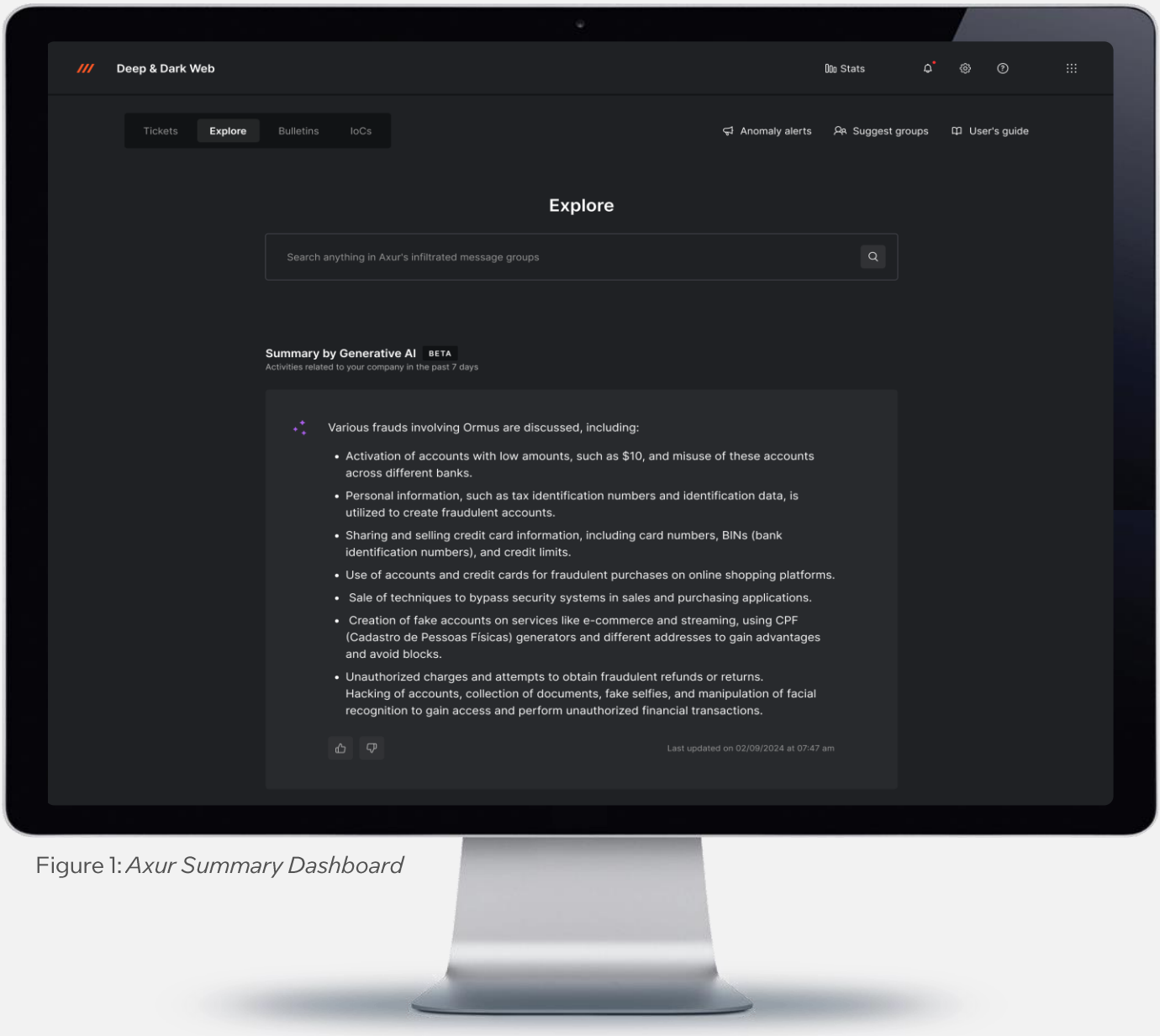
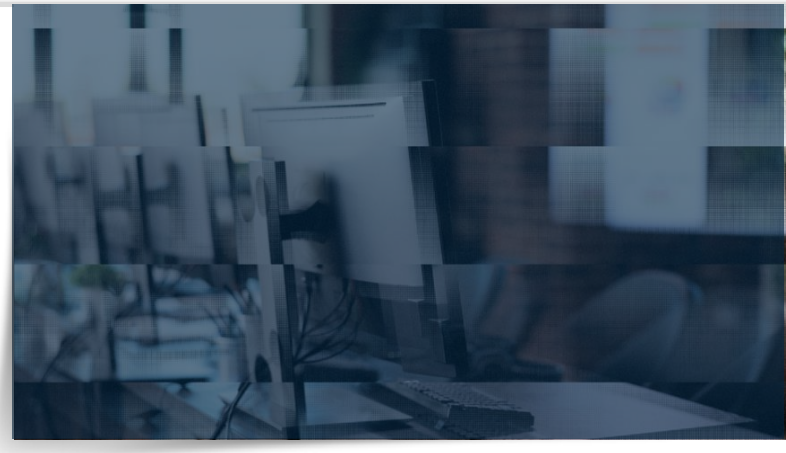


Figure 1: *Axur Summary Dashboard*

Conclusion

Axur provides an easy-to-use platform that discovers frauds, leaks, and schemes from thousands of sources from across the web. By combining cyber threat intelligence with machine learning, Axur's platform helps gain critical insights into the threat landscape and protects your business and customers. Understand and stop cybercriminal schemes before they affect your business by reaching out to Axur at https://start.axur.com/en-us/



Learn More

- Axur Website
- About Us Axur Website
- Axur institutional presentation
- Axur Deep & Dark Web module datasheet
- Madeira Madeira case study
- Intel CitC Episode On AI Digital Fraud Protection
- Intel® Distribution of OpenVINO™ Toolkit Product Page
- Intel® Xeon® Scalable Processors Product Page
- Intel® oneAPI Analytics Toolkit Product Page
- Intel® Optimization for PyTorch Product Page

accelerated by intel®

Accelerated by Intel® offerings take advantage of at least one Intel® technology, such as built-in accelerators, specialized software libraries, optimization tools, and others, to give you the best experience possible on Intel hardware.

By taking advantage of acceleration technologies, such as Intel® Advanced Vector Extensions 512 (Intel® AVX-512), Intel® Advanced Matrix Extensions (Intel® AMX), and others, our optimized solution helps accelerate time to innovation and insight.

With Intel technologies and capabilities, a vendor's optimized offering can go beyond the traditional compute and extend to accelerated networking, storage, edge, and cloud. It's all part of helping customers build an optimized infrastructure across the company.

Sources

1. Chart: Cybercrime Expected To Skyrocket in Coming Years, Statista, 2022
2. 30 Crucial Cybersecurity Statistics: Data, Trends And More, Zippia, 2023
3. Cost of Data Breach Hits Record High, Ponemon Institute, 2021
4. Data from internal tests results of Axur. Intel does not control or audit third-party data. Please review the content, consult other sources, and independently confirm if the data provided is accurate.

Notices & Disclaimers

Intel is committed to respecting human rights and avoiding complicity in human rights abuses. See Intel's Global Human Rights Principles. Intel® products and software are intended only to be used in applications that do not cause or contribute to a violation of an internationally recognized human right.

Intel technologies may require enabled hardware, software or service activation. No product or component can be absolutely secure. Your costs and results may vary. Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy. Code names are used by Intel to identify products, technologies, or services that are in development and not publicly available. These are not "commercial" names and not intended to function as trademarks.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.