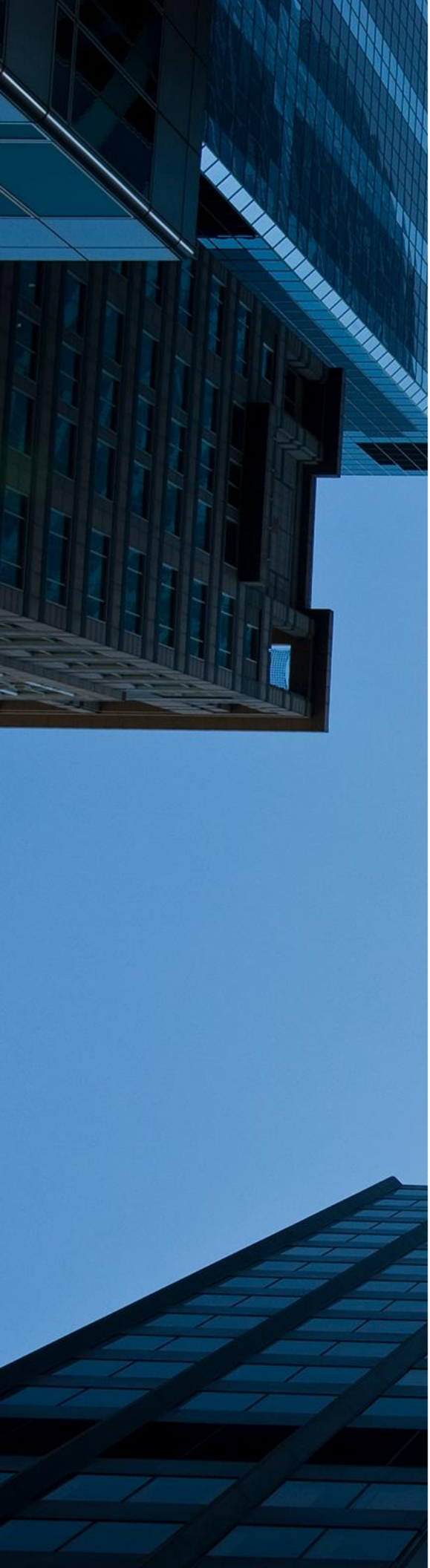


Aite Novarica

AUGUST 2021

FIGHTING CRIME WITH OPEN-SOURCE SOLUTIONS

PREPARED FOR:

pwc

AUGUST 2021

FIGHTING CRIME WITH OPEN-SOURCE SOLUTIONS

TABLE OF CONTENTS

EXECUTIVE SUMMARY 2
INTRODUCTION 3
METHODOLOGY 3
CHALLENGES 4
OPEN-SOURCE DIGITAL CRIME FIGHTING 6
BENEFITS OF AN OPEN-SOURCE MARKET APPROACH TO SOLUTIONS 9
IMPLEMENTATION CONSIDERATIONS 10
CALL TO ACTION 12
ABOUT PWC 13
ABOUT AITE-NOVARICA GROUP 14
CONTACT 14
AUTHOR INFORMATION 14

LIST OF FIGURES

FIGURE 1: CORE CHALLENGES 5
FIGURE 2: DIGITAL CRIME-FIGHTING FRAMEWORK 6
FIGURE 3: DIGITAL CAPABILITIES 8

LIST OF TABLES

TABLE A: BENEFITS OF DIGITAL CRIME FIGHTING 9

EXECUTIVE SUMMARY

Fighting Crime With Open-Source Solutions, commissioned by PwC and produced by Aite Group, considers how open-source, digitally enabled solutions can enable financial institutions (FIs) to significantly improve their anti-money laundering (AML) controls and move from a position of "following the pack" to one of leading in the fight against financial crime.

Key takeaways from the study include the following:

- FIs face many choices when deciding to augment or replace current anti-financial crime systems, with many vendors offering competing solutions.
- Large-scale, off-the-shelf commercial systems often take many months to implement and may not meet the requirements or be the right solution for the firm.
- Artificial intelligence (AI) and machine learning approaches bring the promise of increased efficiencies and effectiveness. FIs need to trial and fully understand them in a safe environment before they fully adopt them.
- Digital crime-fighting solutions bring together several innovative elements to fighting financial crime. These solutions are based on the use of open-source code using a cloud based "activation" model that significantly accelerates benefits realization with no or low system requirements.
- Open-source code provides greater transparency with the ability to understand solutions using "plug-and-play" approaches that reduce complexity and integration costs.
- The use of open-source code with a "plug-and-play" approach allows an easy route to customizing the solutions to ensure they meet specific client needs and allow for future changes in business models.
- An agile development methodology provides fast implementation, driving value and changes during the implementation, and placing the focus on the end user—the compliance officer.
- Digital crime-fighting solutions can quickly improve Know Your Customer (KYC), fraud, AML, and sanctions screening controls for FIs, bringing much-needed automation to support human decision-making, and ensuring consistent and high-quality decision-making across all areas of their AML operations.

INTRODUCTION

FIs are facing many challenges, including evolving regulation and criminal threats, as well as new digitalization that has been accelerated by the COVID-19 pandemic. FIs now have access to massive data sets and a plethora of systems and solutions. The industry recognizes the need to use innovation to make a step change, with regulators across the globe giving the "green light" to the trial and use of advanced data analytics and machine learning. However, given the current fragmented marketplace, with many competing vendors and solutions, FIs are finding it harder to choose between the many options presented and determine which is the best route to take.

The larger the scale and size of a solution, the higher the implementation risk in terms of costs, time scales, and meeting the success criteria. FIs are reluctant to rip and replace current AML systems due to implementation complexity and risks. FIs are seeking easier and less-risky means of trialing and benefiting from new innovative approaches; they are looking to simplify their architecture and systems, thus reducing complexity and integration costs.

This white paper proposes an open-source digital crime-fighting strategy. It also positions solutions as enablers that bring innovation and advanced analytics through open-source code and an agile approach, allowing FIs to trial, review, and deploy "plug-and-play" alternatives that bring automation, consistency, greater efficiencies, and enhanced human decision-making.

METHODOLOGY

This white paper is based on Aite Group's ongoing conversations with AML executives at FIs and vendors in this space. It is also informed by a survey of 22 North American AML executives at FIs conducted in September 2020.

CHALLENGES

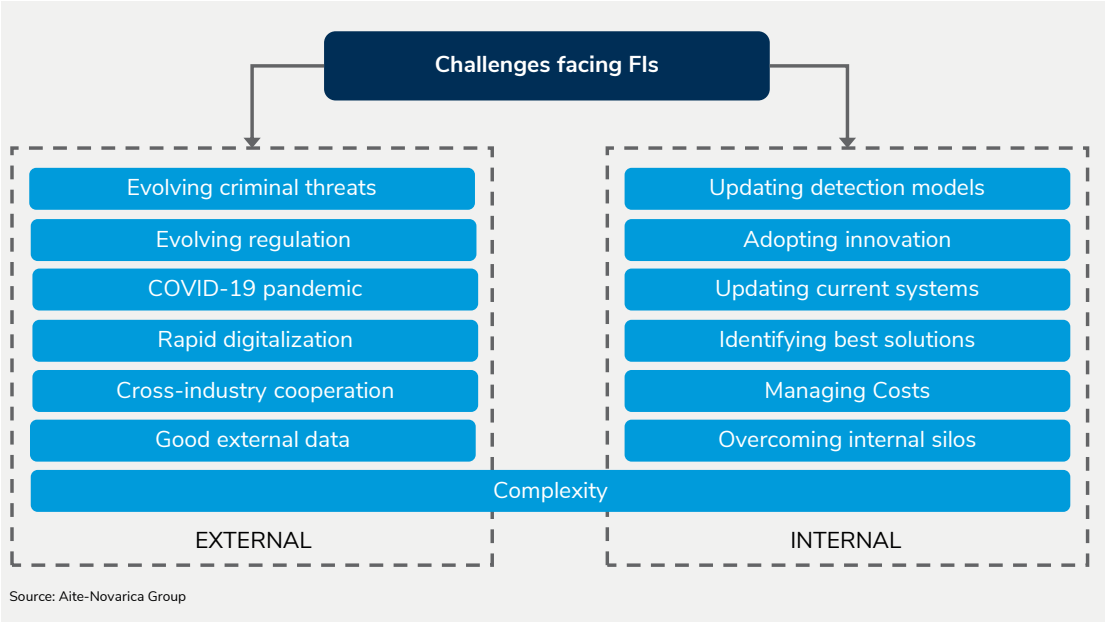
FIs face both external and internal challenges, as shown in Figure 1. While FIs largely focus on external challenges, the internal challenges can become significant impediments to progress if not addressed in a timely manner.

External challenges include the sophistication and evolution of the criminal, through to informed regulators setting ever-higher standards of compliance. The COVID-19 pandemic has impacted FIs' ability to respond, and the consequential rapid adoption of digital customer interaction models has increased new multichannel customer interactions. Cooperation across the industry is seen as vital to preventing criminals, though it is difficult to achieve for reasons such as data sharing. Accessing high-quality external data is still harder than it should be, but it provides an ability to unlock intelligence from the data.

Internally, challenges include keeping detection models effective against new threats and using innovation. Current systems need continual refinement, and FIs struggle with the many choices of vendor solutions. Costs are an ever-present concern, with organizational silos increasing costs and preventing the adoption of consistent solutions across all areas.

Complexity is a significant challenge, both externally and internally. Externally, there is a complexity of criminal threats and emerging risks as well as a complexity of vast arrays of data. Internally, the many different systems and fragmented data and processes create complexity and friction in processes that seek to detect and prevent financial crime.

FIGURE 1: CORE CHALLENGES



Source: Aite-Novarica Group

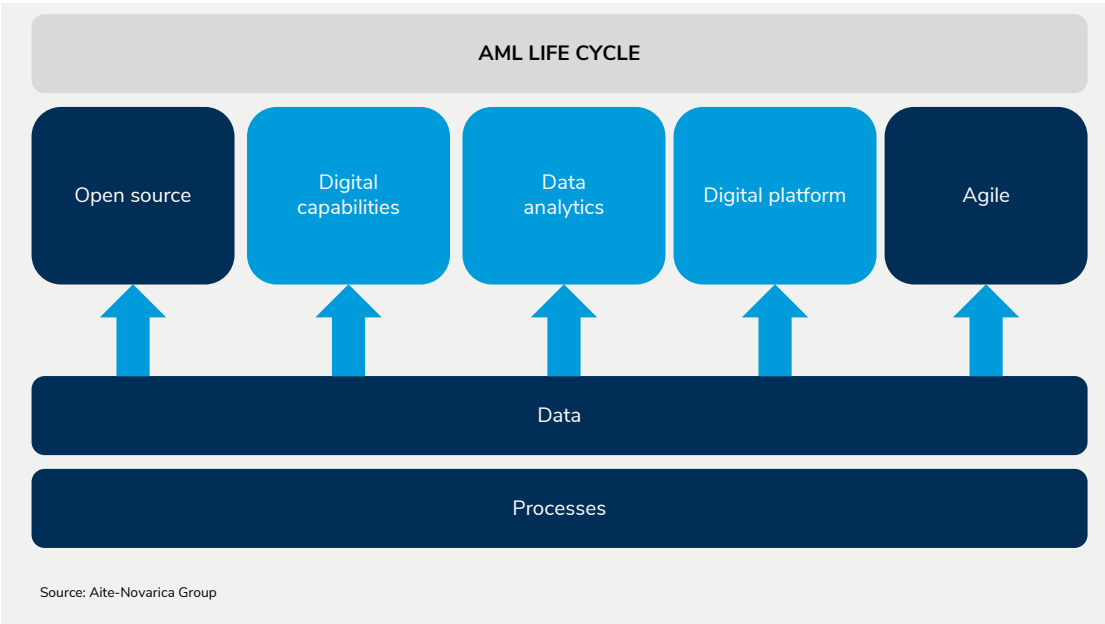
Faced with a choice of keeping existing systems or undertaking a complete replacement, FIs are often left in an undesirable position, with costs from both options. Existing systems will need refinement and upgrading and may have gaps. A new replacement is expensive, takes time, and comes with implementation risk. FIs need an effective way of trialing, reviewing, and quickly implementing solutions that can either directly replace current functionality or, in many cases, augment it, reducing noise from current systems and improving efficiencies.

OPEN-SOURCE DIGITAL CRIME FIGHTING

It is evident from these challenges that FIs must dynamically review and address many areas of their financial crime compliance (FCC) control framework, including current and future system solutions, the use of innovation, and the integration of data, people, and processes. These challenges need to be addressed in ever-shorter time scales and cannot be met through elongated systems implementations.

PwC's digital crime-fighting approach provides a marketplace for downloading assets, models, integrations, and rule sets made available through transparent open-source code. It brings together several key approaches that enable FIs to trial and quickly implement new and innovative techniques. Figure 2 shows the key elements of a digital crime-fighting framework. These elements in isolation provide substantial benefits, which are significantly enhanced when they are bought together into a consistent integrated framework. Open-source code and agile approaches provide the transparency, ease, and speed of adoption. Digital capabilities, data analytics, and a digital platform provide the core technologies and approaches that support all aspects of the AML life cycle, from KYC/customer due diligence (CDD), screening, and monitoring to reporting and control.

FIGURE 2: DIGITAL CRIME-FIGHTING FRAMEWORK



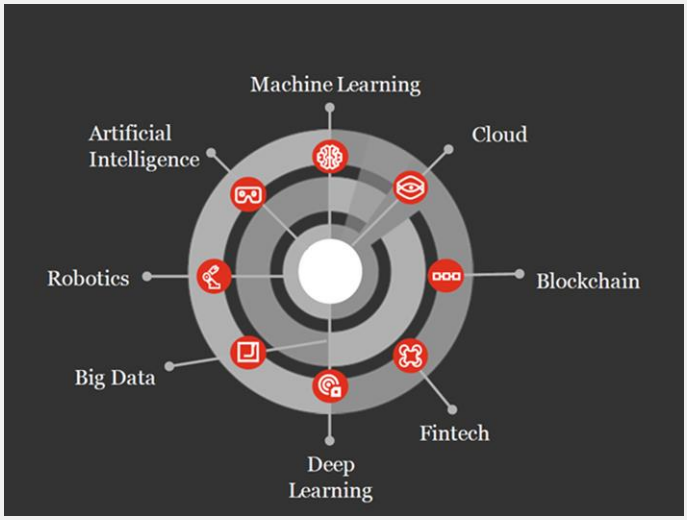
Source: Aite-Novarica Group

The individual elements of the framework are defined below:

- **AML life cycle:** Having good individual controls is important; however, it is ultimately the sum of all the controls that determines how effective and efficient the FI will be at protecting, detecting, and preventing financial crime. Solutions need to be consistently applied across all areas of AML—from supporting KYC/CDD and accessing risk to screening, monitoring, investigating, reporting, and controlling AML.
- **Open-source code:** This provides flexibility and transparency; it removes the dependency on any one vendor's proprietary code. Using open-source code, FIs can "plug and play" different elements to meet their needs.
- **Digital capabilities:** These bring together several approaches and solutions to enable greater efficiencies and improvements to core financial crime-fighting capabilities. The approaches are interconnected, as shown in Figure 3. They range from those that are established and well-understood, such as cloud and robotics, to emerging areas such as blockchain and deep learning. Using digital capabilities, FIs can apply the elements they are most comfortable with in the first instance and then expand into new areas as their knowledge and understanding increases.
- **Data analytics:** The availability of large data sets has enabled the adoption of "data-hungry" analytical and machine learning approaches. These have brought greater transparency and effectiveness to model management, tuning, and reporting. Models underlie risk rating and monitoring approaches; they should move beyond the use of a narrow set of rules and take in a wider data set that is based on many features and patterns discovered from the data. Data analytics includes:
    - AML analytical methodologies and model selection
    - Data quality frameworks, including data lineage frameworks
    - Model simulation and diagnostics
    - Alert and case analytics
    - Dashboarding and reporting, both of the business-as-usual state and results of tuning and changes
- **Digital platforms:** These provide a wider framework that delivers many benefits and the next level of integration needed by the FI. The platform should build upon the data analytics capabilities, providing a means to test ideas and solutions in a sandbox and allowing for assessment, benchmarking, and automation.

- **Agile deployment:** Solutions adopt the best from the world of agile development and implementation. This allows not only a shorter time to deployment and benefits but also tuning and amendment based on results through the process.
- **Integrated data and processes:** Solutions need to work with data and support both automated and human processes. The digital crime-fighting framework should have data and processes as key embedded considerations.

FIGURE 3: DIGITAL CAPABILITIES



Source: PwC

BENEFITS OF AN OPEN-SOURCE MARKET APPROACH TO SOLUTIONS

The use of a broad array of digital capabilities, analytics, and a digital platform brings core capabilities to the table. These elements improve controls and processes across the AML life cycle and—through the use of open-source code and an agile deployment—provide benefits in a timelier and more cost-effective manner than large-scale system replacements and upgrades. Table A shows the key benefits.

TABLE A: BENEFITS OF DIGITAL CRIME FIGHTING

BENEFIT	
Comprehensive coverage	Digital crime fighting is not limited to a single area. The open-source code approach and framework can be applied to the entire end-to-end AML life cycle, hence uplifting all AML controls.
Data and process integrated across all solutions	This means removing the siloed approach, integrating data and process tightly into controls to ensure the processes and systems have quality data as and when needed, and ensuring that end users are working with the latest set of data, be that customer, alert, transaction, or other data.
Reduced complexity	Complexity is costly; it requires additional steps and produces unwanted noise and friction in business processes. An open-source approach provides tools and solutions that are integrated, share data easily, and seek to reduce complexity across the breadth of AML solutions and processes.
Adaptable	FIs use machine learning, both supervised and unsupervised, to keep detection models up to date and one step ahead of criminal threats. Models can be amended in real time or near real time as opposed to weeks or months after a threat is identified.
Harness innovation	FIs are able to take advantage of the many innovative techniques and approaches quickly, without the risk of being an early adopter, especially for advanced data analytics, AI, and machine learning.

BENEFIT	
Transparency	Through open-source code, FIs have greater transparency, and their own teams can explain and expand solutions without having to be trained in proprietary code and tools. This goes up the entire audit and accountability chain, enabling clear explanations behind decisions and solutions to be presented to senior management, internal audit, and external regulators.
Iterative and speedier deployments	This is the ability to test and improve solutions during development and implementation, learning from results and harnessing functionality and benefits iteratively as opposed to having to wait to the end of a long implementation cycle.
Reduced implementation risk	The agile approach, based on the use of open-source code, reduces implementation risk, as each stage is clearly defined and understood, and functionality is delivered in a manageable and controlled manner.
Greater efficiencies	Through automation of routine processes, including basic information and case creation, FIs can gain significant efficiencies, ensuring scarce human resources can be focused on key decision-making.

Source: Aite-Novarica Group

IMPLEMENTATION CONSIDERATIONS

The agile approach is used across many areas of product and project management. It not only speeds up solution development and implementation times but also allows functionality to be trialed, with the results used to inform future iterations and functionality. Agile methods focus on the end users, putting their needs and requirements at the heart of the development. Open-source code is known within the development industry, using languages such as Python for data analytics and machine learning. It means that solutions can be understood and tested without having to learn proprietary code or tools.

FIs should ensure they have sufficient skills and expertise available, both from a data science and development perspective and from a project implementation team. Where these skills are not available or there is insufficient knowledge and expertise, FIs should consider working with a partner, such as PwC, that can bring these skills. Technical

teams should work closely with compliance officers and stakeholders to ensure that changes are prioritized and that solutions meet AML requirements.

FIs should create an FCC strategy and roadmap that clearly shows how solutions meet current and future AML requirements, and how they will enhance capabilities over the next 12 to 24 months and beyond. A key decision is whether to augment or replace existing solutions. In some cases, augmenting current solutions can provide benefits—for example, better segmentation for transaction monitoring or accurate extraction of entities from documents for name screening. In other cases, systems may no longer meet current or future business requirements and should be considered for replacement.

Considerations should include the following:

- How costs can be taken out of the AML operation without impacting effectiveness
- The use of open-source code to reduce dependency on propriety code
- The use of innovation to drive value into the compliance operations, thus simplifying processes and enabling better human decision-making
- The different approaches available and how they can be applied—for example, the use of Python libraries and analytics for alert scoring and triaging, or natural language generation and natural language processing for case creation
- How robotics can be used to automate and embed quality into routine processes, bringing quality, consistency, and efficiencies
- What skills are needed, especially scarce resources such as data scientists, and how teams can take advantage of open frameworks, open programming platforms, and open-source languages
- What data the FI has—e.g., whether it has sufficient data to support the data model and improve quality and consistency, and if not, whether it needs to obtain further data
- How data and processes can be integrated into solutions, and what steps are required to improve the quality and consistency of data and processes
- How information be can securely shared across the industry for the benefit of fighting financial crime

CALL TO ACTION

The digital crime-fighting framework provides an open-source code marketplace for downloading assets, models, integrations, and rule sets, enabling FIs to quickly take advantage of the latest innovation in data analytics and machine learning.

FIs:

- Review your FCC strategy and roadmap, and prioritize areas of highest need over the next 12 to 24 months and beyond.
- Identify how the FCC strategy and roadmap can be delivered. Will current systems be replaced or augmented?
- Review what data is available, both internally and externally. What is the quality and completeness of that data, and how can it be integrated into FCC solutions and processes, and support the data model?
- Work with a partner, such as PwC, that can advise and support you on the journey, providing an open-source code framework along with advice, skills, and necessary know-how.
- Look to reduce complexity using open-source approaches to avoid having to invest in proprietary code and tools that bind you to any single vendor.
- Seek to trial, review, and deploy changes using an agile framework. This will not only bring immediate improvements but will also provide longer-term strategic alignment.

ABOUT PWC

Across our global network of more than 284,000 people in 155 countries, PwC committed to advancing quality in everything we do, with a purpose to build trust in society and solve important problems at the core of everything we do. It guides how PwC serves clients and our teams around the world. To help clients build trust and deliver sustained outcomes, PwC provides professional services across two segments: Trust Solutions and Consulting Solutions. Within these segments we bring a range of capabilities to help organizations solve faster, solve more and realize more value. These capabilities include cloud and digital, deals, ESG, cybersecurity and privacy, governance/boards, risk, transformation, tax services and more.

PwC's Financial Crimes Unit brings together the full breadth of PwC's technology, regulatory, and investigative experience with the work of over 2,000 global financial crimes professionals in cybersecurity, anti-money laundering, sanctions, fraud, and anti-bribery/anti-corruption to create an adaptive, comprehensive approach that reflects that of major financial institutions and government agencies.

ABOUT AITE-NOVARICA GROUP

Aite-Novarica Group is an advisory firm providing mission-critical insights on technology, regulations, markets, and operations to hundreds of banks, payments providers, insurers, and securities firms as well as the technology and service providers supporting them. Our core values are independence, objectivity, curiosity, and a desire to help all participants in financial services create better, more effective strategies based on data, well-researched opinions, and proven best practices. Our experts provide actionable advice and prescriptive business guidance to our global client base.

CONTACT

Research and consulting services:
Aite-Novarica Group Sales
+1.617.338.6050
sales@aite-novarica.com

Press and conference inquiries:
Aite-Novarica Group PR
+1.617.398.5048
pr@aite-novarica.com

For all other inquiries, contact:
info@aite-novarica.com

Global headquarters:
280 Summer Street, 6th Floor
Boston, MA 02210
www.aite-novarica.com

AUTHOR INFORMATION

Colin Whitmore
cwhitmore@aite-novarica.com