3 KEY TRENDS

DRIVING THE NEED FOR SECURITY ANALYTICS

Cognyte

Formerly a Verint company

TABLE OF CONTENTS

INTRODUCTION

In theory, achieving rapid resolution to criminal, terror, and cyber investigations should be relatively straightforward in our technology-driven world.

After all, nowadays government and enterprise security organizations have more data available and more sophisticated tools to assist them than ever before.

Yet when it comes down to it, effectively detecting and preventing threats is a much more elusive goal than would seem.

Security organizations, whether government agencies or within enterprises, face similar challenges in this respect. Investigative, operational and SOC teams at these organizations are charged with keeping people, property and processes safe, and preventing operational disruption and reputational damage.

Although these security teams have advanced technology and highly trained personnel, all too often investigations take too long to resolve, or go unresolved altogether. Data is siloed in disparate databases, preventing critical pieces of information from being fused, correlated and leveraged. And as a result, security teams frequently lack high-quality, real-time information and key indicators are missed, which prevents damaging incidents from being averted before they occur.

In recent years, virtually all industries have begun using analytical solutions to generate insights in order to gain a competitive edge - whether to improve manufacturing processes or to optimize pricing and advertising. While some security organizations have followed this trend and have deployed analytics platforms, in many cases, these platforms are proprietary home-grown solutions that do not adequately support the evolving needs of security teams and cannot provide the deep level of insight required.

With the old approach of homegrown development no longer viable, security organizations are increasingly turning to open **security analytics platforms**.

In this white paper, we'll examine what's driving security organizations, both government and enterprise, to make this shift.

MULTIPLE USERS AT SECURITY ORGANIZATIONS

Investigative teams: Responsible for the resolution of investigations, which may take several days or even a number of years. These cases involve detecting and preventing future terror, criminal and cyber threats, or investigating after the fact to catch the perpetrators.

Operational teams: Responsible for carrying out security missions in the field. For these professionals, it's of vital importance to get real-time or near real-time insights to ensure successful completion of missions.

SOC operators: Cyber Security Operations Centers (SOC) are responsible for detecting and mitigating cyber threats, while physical security SOCs are responsible for employee safety and business continuity.

SECURITY ANALYTICS PLATFORMS

These platforms fuse, visualize, and analyze disparate data sets at scale to help security organizations conduct investigations, detect threats, and extract actionable insights. The types of organizations which stand to benefit from security analytics platforms covers a wide range - from law enforcement and intelligence agencies to security organizations within enterprises.

TREND 1:

SECURITY THREATS ARE BECOMING MORE DIFFICULT TO DETECT AND MITIGATE

As digital transformation has driven innovative services and created new industries and markets seemingly overnight, an unintended consequence of this shift is that crime and terror groups have received a significant technology-fueled boost. Backed by well-organized and well-funded groups and organizations, malicious actors now have access to better, faster, and more advanced tools than ever, enabling them to operate covertly and avoid detection more effectively.

> Europol, the European Union agency for law enforcement cooperation, underscored the severity of the challenge, stating, **"For almost all types of organized crime, criminals are deploying and adapting technology with ever greater skill and to ever greater effect. This is now, perhaps, the greatest challenge facing law enforcement authorities around the world, including in the EU."**[1]
>
> EUROPOL

TODAY'S PLAYING FIELD HAS SHIFTED; SECURITY ORGANIZATIONS ARE FIGHTING INCREASINGLY SOPHISTICATED BATTLES, AGAINST ADVERSARIES WHO ARE MUCH MORE ADVANCED THAN THOSE OF THE PAST.

ADVANCED TOOLS HELP PERPETRATORS EVADE DETECTION

Perpetrators use numerous tools and platforms to evade detection, which makes fighting security threats much harder. Here are a few examples:

CRYPTOCURRENCIES:

Traditional payment methods are monitored and traceable. To bypass this, terrorist groups and criminals are increasingly using cryptocurrencies such as Bitcoin and Monero to pay for illicit goods and services and to launder money.

SOCIAL MEDIA:

Criminals often leverage fake social media accounts across platforms such as Twitter, Instagram, TikTok, and Facebook, to communicate with other criminals covertly and to threaten and lure in new customers and victims, while extremists leverage social media for the purposes of recruitment and incitement.

DARK WEB MARKETPLACES:

Only accessible via a specialized Tor browser, dark web marketplaces facilitate the anonymous purchasing and selling of cyber security exploits, leaked data, illicit drugs, illegal weapons, and more. **Dark web marketplace sales grew by 70% in 2019, demonstrating their pivotal role in illegal activities.**[2]

CHATBOTS:

AI-based chatbots can automate the entire process of tricking people into infecting their own computers, or disclosing sensitive information. For example, **in 2016, thousands of Facebook users were tricked into downloading malware by human-like chatbots,** displaying the potency of this new technology.[3]

Using these and other tools, attackers can avoid detection and carry out activities on an unparalleled scale. And the ease with which anyone with malicious intent can act means that there is a wider range of threat actors than ever before - from cross-national criminal organizations and nation-state backed hacking groups, to lone-wolf terrorists and individual hackers. This potent combination of better tools and more potential perpetrators makes the job of detecting and preventing criminal and terror activity exceedingly difficult.

THREATS ARE MORE COMPLEX AND MORE DAMAGING

Not only have the tools become more advanced, the threats themselves have become more complex and cause more harm than those of the past. Therefore, any delay in detecting and mitigating threats can cost lives and cause significant damage and disruption to the public.

For example, while security organizations once had to combat illegal activities on a local scale, today they face sophisticated cross-border crime networks, running complex drug smuggling, weapons trafficking, and poaching operations. And consider the crime-as-a-service model spreading via dark web marketplaces, in which experienced cyber criminals sell prepackaged tool kits that put the power of advanced tools and methodologies in the hands of anyone willing to pay for them. These can include ransomware, distributed denial-of-service (DDoS), phishing, and malware kits.

> Christopher Wray, Director of the U.S. Federal Bureau of Investigation, recently stated, **“We are battling the increasing sophistication of criminal groups that place many hackers on a level we used to see only among hackers working for governments.”**[4]

Then there are the growing threats targeting critical infrastructure providers such as public transport, airports, and even hospitals, as well as key industries such as energy and banking. Attacks have increased in recent years, with a noticeable uptick even since the COVID-19 pandemic began. An October 2020 global survey of security professionals in the critical infrastructure sector, reported that **56% of respondents have experienced more threats and 70% have seen cybercriminals using new tactics to target their organization since the pandemic began**.[5]

> In the words of Prof. Audrey Kurth Cronin from the Center for Security, Innovation and New Technology, **“Never have so many possessed the means to be so lethal. The diffusion of modern technology (robotics, cyber weapons, 3-D printing, autonomous systems, and artificial intelligence) to ordinary people has given them access to weapons of mass violence previously monopolized by the state.”**[6]

When it comes to cyber attacks - not just against critical infrastructure but all sectors - digitization has led to a major expansion of the attack surface, one that cyber attackers are of course well aware of, and use to their advantage. With more and more connected devices and a larger than ever connected supply chain, there is a continuously growing number of entry points - in the organization or via third parties and vendors. As such, malicious actors have many windows of opportunity to infiltrate the organization or even an entire sector they are targeting.

THE CONFLUENCE OF ALL THESE ELEMENTS MEANS IT’S NEVER BEEN SO EASY TO BE SO BAD. AND AS A RESULT, ORGANIZATIONS NEED BETTER AND HIGHER QUALITY ANALYTICS FOR MUCH FASTER DETECTION AND THREAT MITIGATION.

TREND 2:

DATA IS GROWING RAPIDLY AND IS HIGHLY FRAGMENTED, MAKING IT HARDER TO CONNECT THE DOTS

The next trend driving the adoption of open security analytics platforms is the fast-growing volume and richness of data in the digital era and, consequently, the increasing potential of mining that data for actionable insights.

> **“We are drowning in information but starved for knowledge.”**
>
> John Naisbitt, noted author and thought leader[7]

THE VARIETY, VOLUME AND FRAGMENTATION OF DATA POSE TOUGH CHALLENGES

The world is overflowing with digital experiences, and the byproduct of this is our growing digital footprint. As research firm IDC reports, **"Today, more than 5 billion consumers interact with data every day – by 2025, that number will be 6 billion, or 75% of the world's population. In 2025, each connected person in the world on average will have a digital data engagement over 4,900 times per day – that's about 1 digital interaction every 18 seconds."**[8]

This phenomenon is just as true and relevant with perpetrators as it is with ordinary citizens. Using analytics, the potential exists for security organizations to sift through the massive amounts of data to gain a deeper view into a perpetrator's intentions and actions, uncover hidden patterns and connections, and reach insights that would be impossible to find manually.

But extracting these insights is no simple feat. The incredible variety of sources, the vast amount of data,, and the fragmentation of this data all create significant roadblocks. This is all the more frustrating since this data should be used as a strategic asset, yet much of the data that security organizations have access to is overlooked, unmined, and untapped for analytics.

VARIETY

Data variety refers to the tremendous diversity of data types that must be collected and analyzed for investigations, especially by government security organizations.

In order to gain a deep understanding of a perpetrator's activities and intentions, investigative teams must fuse together data from varied sources, including government databases, such as criminal records and vehicle records, as well as the web, financial transactions, flight records, ship movements, and many other sources. And this diversity continues to grow as new sources pop up, from digital wallets to chatbots.

Not only does the data from each source come in a multitude of different types and formats, an estimated **80% of the data generated today is unstructured data**. The inherent nature of unstructured data makes it much more challenging to process and mine for insights than structured data.

> According to John Edwards, CIO of the U.S. Central Intelligence Agency, **the variety of data that security organizations analyze is vast and much broader than most companies**. He adds that **"the data sets are probably among the most complex in the world."**[12]

UNSTRUCTURED DATA

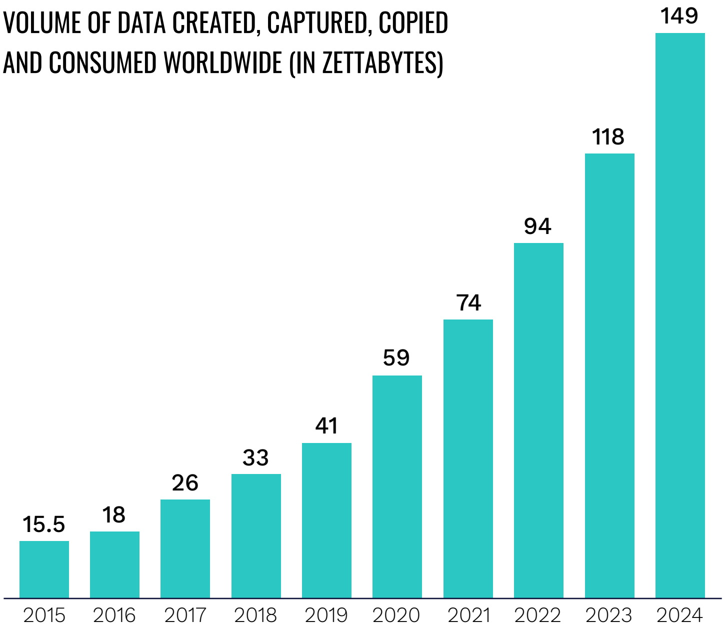
Unstructured data is not structured according to established data models and cannot be easily captured in relational databases. This category is vast and includes just about everything not included in structured data (i.e., photos, videos, emails, reports, log files, social media posts, satellite imagery, and sensor data, among others).

VOLUME

Today, there is more data available to be captured, analyzed, and leveraged than ever before. **At the start of 2021, IDC estimates that the digital universe is made up of an estimated 74 zettabytes of data. That number is expected to grow by roughly 26% annually to reach 149 zettabytes by 2025**. While no one knows the exact numbers, what is clear is that the amount of data produced by humans and machines is staggering and growing exponentially each year.[9]

This massive amount of data is created by sensors in IoT devices, Web traffic, social media, security cameras, mobile payments, and so much more. If it could all be properly harnessed, it could - and does - hold key information that can be used to mitigate threats in less time and with better results.

VOLUME OF DATA CREATED, CAPTURED, COPIED AND CONSUMED WORLDWIDE (IN ZETTABYTES)



source: Statista.com

THE INFORMATION OVERLOAD CHALLENGE

In the past, security organizations invested enormous efforts to obtain even small bits of information. Today, they have the opposite challenge - sifting through the information overload to extract meaning and insight from enormous volumes of data.

Two data points to give a sense of the magnitude of the challenge:

127 TERABYTES

The amount of information collected by U.S. special forces from enemy material alone in one year (Oct. 2017 - Sept. 2018).[10]

11,000 DRONES

The number of drones reportedly operated by the U.S. military, with each one recording 'more than three NFL seasons worth' of high-definition footage each day. However, according to a U.S. Department of Defense source, the military does not have sufficient analysts or an adequate system to comb through the data in order to derive actionable intelligence analysis."[11]

FRAGMENTATION

Compounding the previous issues, when data is siloed (i.e., stored across disconnected systems, within and outside of the organization), it becomes almost impossible to apply analytics on a large scale due to the work required to integrate, fuse, and analyze data manually.

And even if all data has been gathered into one data lake, and is no longer siloed, the organization's security teams often lack the right tools and knowledge to connect the diverse types of data into one unified data layer and to extract meaningful insights. As a result, they are often dependent on small teams of data scientists - who end up being the bottleneck in the process.

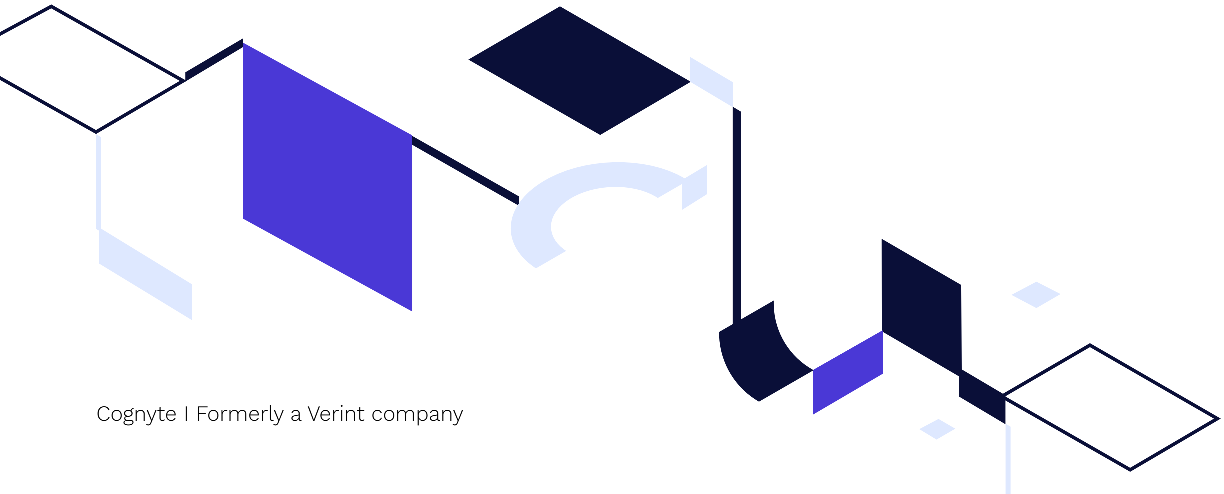
Without the proper solutions, organizations cannot fuse and analyze siloed and diverse data. This prevents them from generating high-value and actionable insights, effectively detecting threats ahead of time, and making optimal decisions.

ILLUSTRATING WHAT HAPPENS WHEN THE DOTS ARE NOT CONNECTED IN TIME

SITUATIONAL INTELLIGENCE

Physical security SOC teams typically have a siloed and incomplete situational awareness view. While they may have hundreds or thousands of security cameras, typically the cameras are feeding into separate, siloed systems. And none of these cameras are necessarily connected to door keypads, fire alarms, etc. Imagine someone carrying a suspicious package into a shopping mall - today, the onsite security team is left to guess whether that person is where they should be, whether the package poses a threat, whether the person is a known criminal, and what they intend to do.

A security analytics platform should connect data from all cameras, door alarms, keypads, license plate readers, facial recognition tools, and various databases to help quickly identify the person as a serious threat and get the right responder to the location, thereby preventing an attack or other serious incident.



TREND 3:

SECURITY ORGANIZATIONS ARE INCREASINGLY ADOPTING OPEN ANALYTICS PLATFORMS

Driven by the need for high-quality, real-time analytical insights, security organizations are moving away from proprietary solutions to open analytics platforms.

> **“Data should not be treated as an IT problem; instead, IT systems should be framed by the operational problems they solve. This requires moving from closed, proprietary architectures... to open architectures and fast transient adoption of new technologies and applications.”**
>
> Lieutenant General John N.T. Shanahan
> U.S. Department of Defense and Cortney Weinbaum[14]

PROPRIETARY SOLUTIONS HAVE SIGNIFICANT LIMITATIONS

In the past, organizations often built their own proprietary solutions with the help of system integrators and internal resources. However, these approaches are no longer sustainable because proprietary homegrown solutions have significant limitations in terms of keeping pace with the rapid evolution of technology, and moreover, they are:

RISKY AND TIME CONSUMING:

They are typically built with complex integrations and patches, and as a result, often fail to deliver a working solution. Moreover, each project takes a great deal of time to build - and by the time the system is deployed, critical opportunities may have been missed.

DIFFICULT TO UPGRADE:

They are typically built as customized projects with a combination of separate products (each with a separate codebase and product roadmap), therefore upgrades are painful and costly.

REQUIRE EXTENSIVE CUSTOMIZATION:

Modifying generic business intelligence and data analytics software to try to address the nuanced and specific needs of security teams, such as case management workflows and security permissions, requires extensive customization. Not only is this very costly, but the results are usually less than optimal.

DEPENDENT ON THIRD PARTIES:

Adding sources and making ongoing changes requires professional services and coding by external contractors/vendors, thus preventing organizations from reacting quickly to new threats and changes in their mandate.

TO ADDRESS THESE LIMITATIONS, SECURITY ORGANIZATIONS INCREASINGLY REQUIRE, AND ARE DEPLOYING, OPEN ANALYTICS SOFTWARE PLATFORMS THAT:

Allow them to **fuse massive amounts of data** from many diverse sources.

Can be **easily integrated** with other systems in their IT environments.

Provide analytics insights such as detecting anomalies, suspicious patterns and hidden connections between entities.

Can be **frequently updated** with the latest analytics and artificial intelligence technologies.

Enable seamless collaboration and information sharing across teams and accelerate investigations with automated case management capabilities.

> In order for security organizations to gain the upper hand over adversaries, the CIA's CIO John Edwards said it best: **"Data is the new tip of the spear - Our operational advantage will be determined by the speed at which we sense, collect, ingest, condition, analyze and characterize data…"**[12]

With the right platform in place, security organizations can rapidly extract high-value, actionable insights they need to make better and faster data-driven decisions. With these insights, teams will have shorter investigation cycles, reach more effective resolutions, and respond to events and indicators in minimal time.

TODAY'S ORGANIZATIONS NEED OPEN SECURITY ANALYTICS PLATFORMS TO KEEP PACE WITH THE DIGITAL AGE, PREVENT TRAGIC EVENTS FROM TAKING PLACE AND KEEP THE WORLD SAFER.

ABOUT COGNYTE

Cognyte is a global leader in security analytics software that empowers governments and enterprises with Actionable Intelligence for a safer world. Our open software fuses, analyzes and visualizes disparate data sets at scale to help security organizations find the needles in the haystacks. Over 1,000 government and enterprise customers in more than 100 countries rely on Cognyte's solutions to accelerate security investigations and connect the dots to successfully identify, neutralize, and prevent national security, business continuity and cyber security.

CONTACT US

FOOTNOTES

[1] https://www.europol.europa.eu/socta/2017/drivers-of-crime.html

[2] https://go.chainalysis.com/rs/503-FAP-074/images/2020-Crypto-Crime-Report.pdf

[3] https://www.researchgate.net/publication/227273142_Devious_Chatbots_-_Interactive_Malware_with_a_Plot

[4] https://www.fbi.gov/news/testimony/worldwide-threats-to-the-homeland-092420

[5] https://info.claroty.com/the-critical-convergence-of-it-and-ot-security-in-a-global-crisis

[6] Power to the People: How Open Technological Innovation is Arming Tomorrow's Terrorists

[7] John Naisbitt, Megatrends: Ten New Directions Transforming Our Lives (Warner Books, 1982)

[8] https://www.seagate.com/our-story/data-age-2025/

[9] https://www.idc.com/getdoc.jsp?containerId=prUS46286020

[10] https://www.tampabay.com/news/military/macdill/SOCom-leader-wanted-to-toss-Google-exec-from-car-Because he-was-right-_167629195/

[11] https://fas.org/sgp/crs/natsec/R45178.pdf

[12] https://fedtechmagazine.com/article/2018/12/cia-cio-sees-data-tip-spear-intelligence

[13] https://www.theguardian.com/world/2020/nov/04/police-investigate-if-vienna-attacker-was-part-of-wider-network

[14] https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1566262/intelligence-in-a-data-driven-age

Unauthorized use, duplication, or modification of this document in whole or in part without the written consent of Cognyte Software Ltd. is strictly prohibited. By providing this document, Cognyte Software Ltd. is not making any representations regarding the correctness or completeness of its contents and reserves the right to alter this document at any time without notice. Features listed in this document are subject to change. Contact your Cognyte representative for current product features and specifications. All marks referenced herein with the ® or TM symbol are registered trademarks or trademarks of Cognyte Software Ltd. or its subsidiaries. All rights reserved. All other marks are trademarks of their respective owners.

Cognyte
Formerly a Verint company