Cognizant

Digital Systems & Technology

Combating Cybersecurity Challenges with Advanced Analytics

Using an AI-powered analytics platform, IT organizations can shift from a reactive approach to security breaches, to proactively identifying increasingly sophisticated threat vectors and quickly resolving exploitable vulnerabilities.

July 2019

Executive Summary

Cyber crimes and security threats have grown at an exponential rate in recent years, and the momentum is only growing. According to Juniper Research, over 146 billion records will be exposed through criminal data breaches from 2018 to 2023, growing at a rate of 22.5% per year.[1]

This builds on the astounding number of data breaches reported over the past few years. In a recent report from Identity Theft Resource Center (ITRC), the number of breached customer records containing personally identifiable information (PII) skyrocketed by 126% from 2017 to 2018, with a staggering total of around 446 million records leaked.[2] Significant 2018 breaches include those experienced by Facebook,[3] Under Armour[4] and Marriott International.[5]

The wreckage of a cyber attack extends beyond the immediate capital losses and financial consequences to brand credibility, with damages persisting over several years. Facebook's shares are reported to have declined by as much as 19%, erasing $120 billion of the company's value in the second quarter of 2018.[6] A study by Ponemon Institute reports that the global average total cost of a data breach rose by 6.4% in 2018; in the U.S., the cost was $7.91 million.[7] The study also points out that the resulting customer churn from loss of brand reputation and consumer trust was a leading contributor to the increased indirect costs of a data breach.

Threat vectors are only multiplying as more enterprises move to digital approaches to doing business, and embrace a wide array of internet-connected devices, fledgling blockchain networks, cloud and social media. Even as organizations implement emerging technologies into their core businesses to safeguard their information crown jewels, malicious agents are also evolving, thereby increasing the nature of deceptive and automated cyber attacks.

Given the unprecedented levels of data and analysis involved in a hyper-converged networked world, we believe traditional defense mechanisms and siloed security tools are unequipped to address the ever-evolving cyber threat landscape. Cybersecurity now requires advanced analytics that keep pace with the speed and scale of digital business. This means IT organizations must leverage big data, cloud and streaming architecture paradigms in conjunction with artificial intelligence (AI)-powered analytics and edge analytics to provide predictive insights and threat protection.

This whitepaper examines the emerging cybersecurity challenges faced by digital businesses, the risk of continuing with conventional approaches, and the imperatives for adopting an intelligent and integrated strategy for holistic digital security by augmenting standard security tools with advanced machine learning-driven analytics and automation. We conclude with an outline of the significant architectural building blocks for a modern intelligent cyber analytics platform.

Cybersecurity now requires advanced analytics that keep pace with the speed and scale of digital business.

The current cyber threat landscape

As Figure 1 illustrates, cybersecurity vulnerabilities and attacks can be grouped under two broad threat patterns: internal and external.

A robust cybersecurity defense strategy needs to account for both of these threat vectors, as well as the more sophisticated attacks possible through the advent of IoT initiatives, cloud enablement, big data analytics, social media, mobile computing, cryptocurrencies, etc. New attack variants are continuously appearing, such as "formjacking" and "cryptojacking," and the list only keeps growing. According to the Ponemon report, the average global probability of a material breach in the next 24 months is 27.9%.

Top three data breach trends

Additionally, the current threat landscape is characterized by the following three trends:

- **Cyber attack targets aren't always what you'd think:** While it is typically assumed that banking and financial institutions are the primary target for cyber attacks, the business sector – which includes e-commerce/retail, hospitality and tourism, trade, transportation, utilities, supply chain business, etc. – sustained the highest percentage of overall data breaches in 2018, according to the ITRC study, at 46%. The medical/healthcare industry and banking/credit/financial sector followed in second and third places, respectively, with 29% and 11% of total reported breaches.
- **Associated costs are increasing.** According to Ponemon's cost analysis, the U.S. and Canada invested the most in resolving malicious or criminal attacks, at $258 and $213 per record, respectively. Without a security automation process, these costs will only rise. The cost of Equifax's data breach in 2017, for

A mix of cyber threats

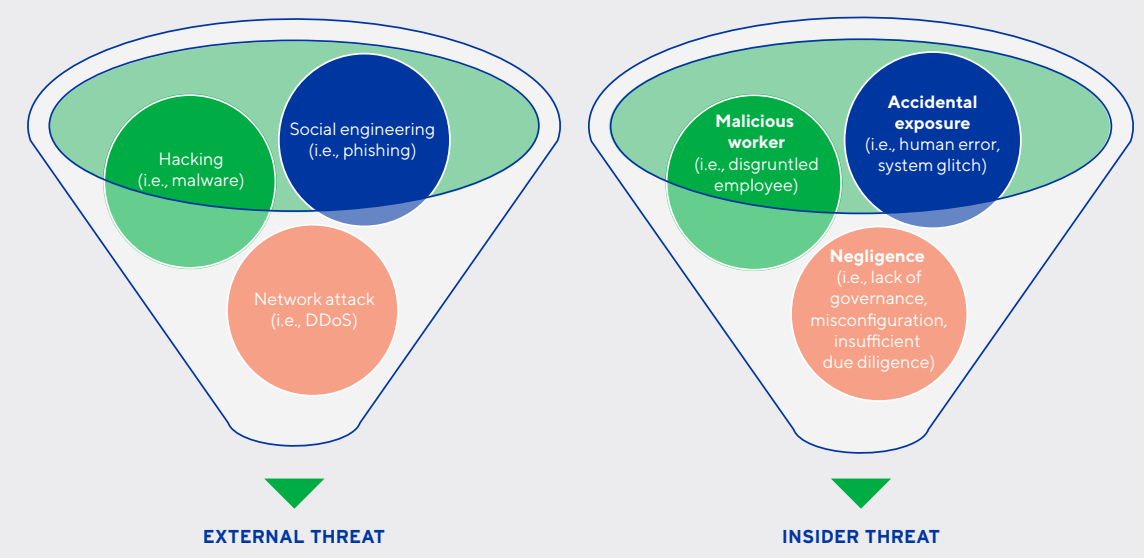


Figure 1

New attack variants are continuously appearing, such as "formjacking" and "cryptojacking," and the list only keeps growing. According to the Ponemon report, the average global probability of a material breach in the next 24 months is 27.9%.

example, was about $300 million.[8] Indirect costs resulting from organizational resources spent notifying victims and investigating the incident, as well as the loss of goodwill and customer churn, also have substantial financial consequences.

A churn of 1% due to a data breach can result in an average total cost of $2.8 million, according to the Ponemon report. Moreover, regulatory changes such as the European Union's Global Data Protection Regulation (GDPR) and impending California Consumer Privacy Act (CCPA), will enforce strict penalties for any privacy lapse.

- **Hacking and insider threats are the most common sources of data breaches.** Hacking continues to be the most common type of cyber attack. According to the ITRC study, 39% of breaches involved hacking, while 30% were due to insider threats, and 21% from accidental exposure and negligence. These statistics are consistent with Ponemon's 2018 report, in which 48% of incidents were caused by criminal or malicious attacks, 27% by insider threats and negligence and 25% from system glitches.

Four major cybersecurity challenges and what to do about them

1 **Cybersecurity programs are failing to keep up with accelerating digital threats.** The pivot to digital introduces new technology and architecture patterns that upend legacy cybersecurity methods (see Figure 2). Roughly 84% of respondents in a recent McKinsey & Co. study feel companies are insufficiently prepared for the vulnerabilities caused by IoT initiatives,[9] and 49% of CIOs in a Gartner study say their enterprises have already changed their business models or are in the process of changing them.[10]

With connected technologies and IoT, companies must shift from managing security for thousands of network endpoints, to millions of connected devices. With the adoption of container technologies, IoT devices, mobile devices and cloud infrastructures, many organizations' security tools and processes lack visibility into the new resulting threat vectors.

Action item: Garner clear understanding of your emerging cyber risk portfolio and evolve legacy security policies. Businesses need to broaden the data points collected for real-time integration, and employ security automation to centralize management and enable rapid, flexible deployment.

Limitations of traditional cybersecurity approaches

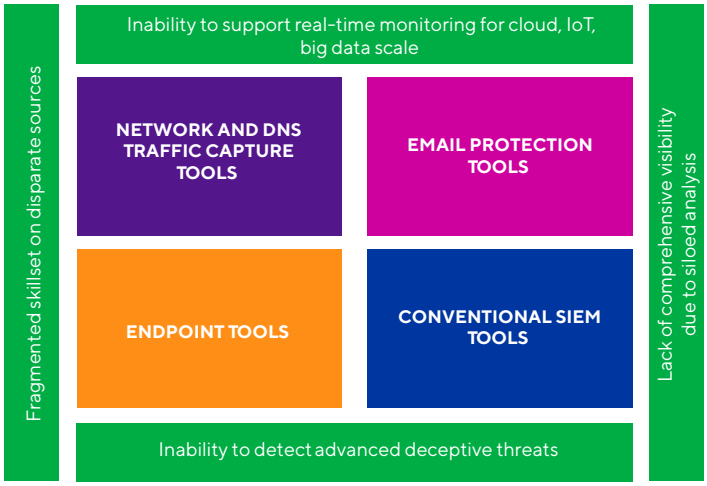


Figure 2

2 **Bots are a blessing and a curse.** While advanced analytics and AI are driving digital business change, malicious agents are reinventing attack algorithms, using AI to create new variants of old attack models. This adds to burgeoning problems with traditional security tools that rely on human intervention and manual investigations and don't always provide 360-degree cyber protection. The potential misuse of advanced analytics technologies can include automated hacking, email and

social media phishing attacks, speech synthesis to mimic human interaction, and turning consumer drones, connected devices[11][12] and autonomous vehicles into potential attack instruments. Without security automation to detect threats, the net cost difference of a data breach is $1.55 million, according to the 2018 Ponemon report.

Action item: Acknowledge the world of sophisticated threats and evolve from a reactive to a proactive strategy. Organizations need to employ advanced analytics powered by AI and machine learning to detect deception.

3 **Siloed data analysis generates too much noise.** Organizations typically use either traditional security information and event management (SIEM) solutions such as syslog servers and log managers, or they utilize multiple cybersecurity products that collect huge volumes of system and user activity events, independently. This results in disparate and disconnected systems that are not suited to today's digital models and fail to present the complete picture of the IT health and risk posture at any given point in time.

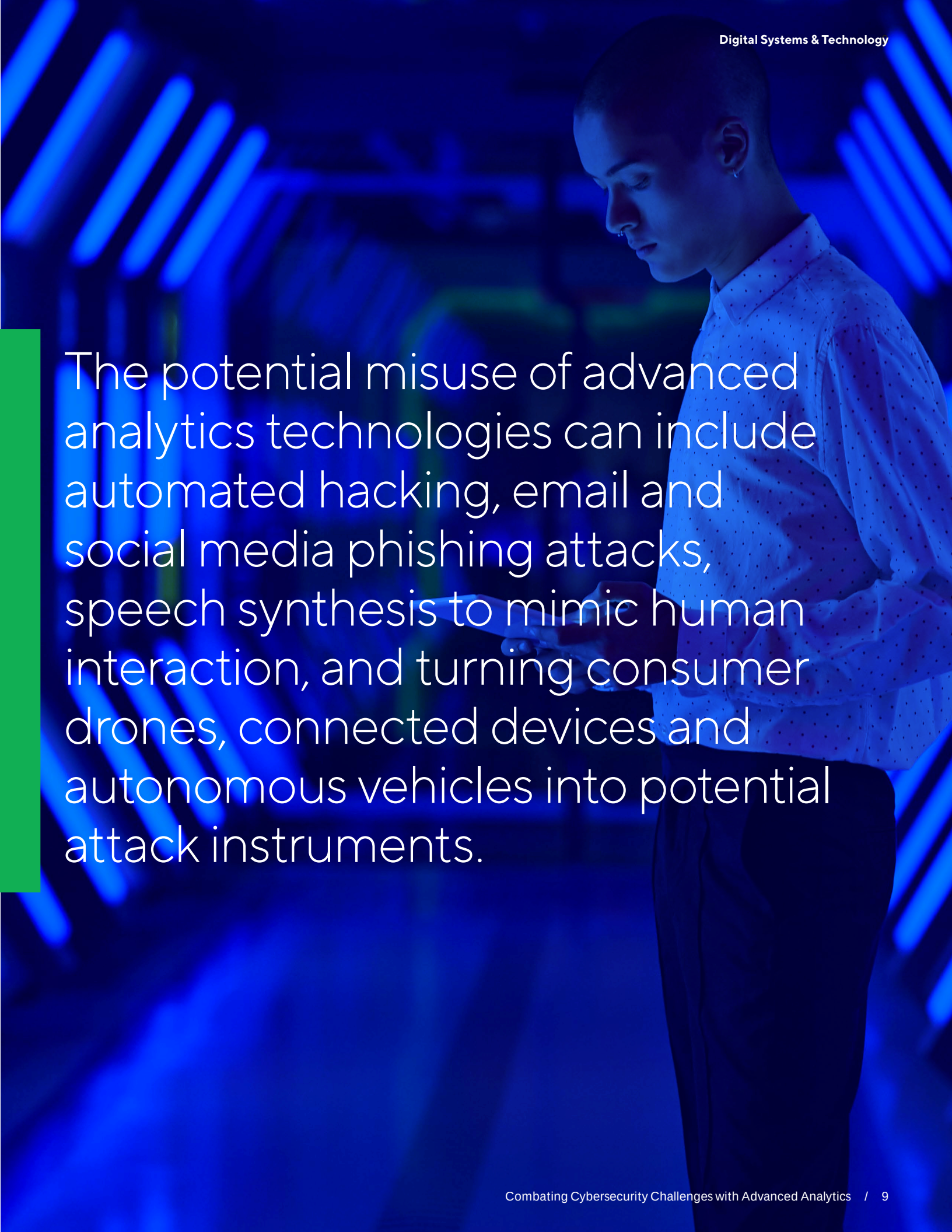
The analysis of huge volumes of fragmented data results in a lack of comprehensive visibility, false positives and inefficiency. The mean time to identify (MTTI) for a data breach in 2018 was 197 days, according to the Ponemon report. The failure to quickly detect and contain a data breach also has huge direct and indirect financial impacts.

Action item: Evolve from a piecemeal process of analysis. Organizations should adopt innovative thinking to intelligently integrate disparate data to radically increase insight generation and response.

4 **There's a lack of cyber skills and capabilities in the emerging technology landscape.** Given that the human factor is a significant cause of data breaches – 27% according to the Ponemon study – there is clearly a critical need to improve awareness among the broader employee community. Conventional education and standard procedures are simply not enough to face the mounting challenges in the digital world, where attack models are outpacing acquired skills.

Security operations center (SOC) analysts with knowledge limited to a specific security tool will struggle to put together a holistic picture from multiple security tools. This will make it difficult to realize the comprehensive event-chaining behavior and analysis of an incident or anomaly. A lack of skill and confidence in the cyber defense strategy can also hinder an organization's IT modernization and digital growth plans. According to a study by (ISC)^2, there are 2.93 million cybersecurity positions open and unfilled around the world,[13] and according to McAfee, 40% of IT leaders are slowing cloud adoption due to a shortage of cybersecurity skills.[14]

Action item: Inform, educate and upskill SOC analysts and avoid internal fragmentation of cybersecurity skill and knowledge. Organizations need to overcome the lack of human-driven intelligence with analytics-driven intelligence.



The potential misuse of advanced analytics technologies can include automated hacking, email and social media phishing attacks, speech synthesis to mimic human interaction, and turning consumer drones, connected devices and autonomous vehicles into potential attack instruments.

Many systems are inherently limited in terms of the amount of data they can store. Imagine the perplexity when a vulnerability is discovered 100 days after the fact, and the source data is purged every 30 days.

Five foundations for tackling cybersecurity challenges

In the current tech climate, it's not a question of "if" but "when" a data breach will happen. While it's important for organizations to continuously refine their security protocols and governance strategy to face emerging challenges, it's also imperative to build and deploy advanced threat protection models. This requires a transformative security analytics agenda that incorporates a cyber analytics platform that integrates disparate data in real-time, enriched with metadata and artificial intelligence/machine learning (AI/ML) analytics, as well as security orchestration automation and response (SOAR) for expedited threat handling.

As threats evolve in scale and sophistication, organizations need to ensure they're aware of the predominant security challenges they face and implement the key foundational building blocks to make data-driven, informed decisions and derive proactive critical insights. We advise organizations to take the following actions:

1 Broaden the data integration and management horizon.

- **Automate collection and ingestion of data at big data scale.**
- **Store data in a manageable manner, supporting data lake patterns.**
- **Break traditional information barriers with fast data retrieval and search.**

Cybersecurity defense is a moving target, and so is the data used for analysis. Isolating analysis to data generated by traditional information security tools and processing in predetermined ways creates rigid boundaries when the data sources are evolving and multiplying.

Cyber analytics platforms must be able to spot threats across a wide variety of data sources – both internal and external to the enterprise – be it real-time streaming data or batch data (i.e., structured, semi-structured and unstructured data formats). Most important, these platforms must work with data that is beyond the traditional purview of security operations teams, such as email content, social media feeds, user metadata from a human resources database, web server and system logs of user activity, as well as critical auditing databases managed by IT teams.

Furthermore, many systems are inherently limited in terms of the amount of data they can store, ranging from a week to a month in some cases. Imagine the perplexity when a vulnerability is discovered 100 days after the fact, and the source data is purged every 30 days. Adding to this is the data associated with mobile devices, IoT devices and cloud-based services, totaling thousands of gigabytes every second. Therefore, it is critical to anticipate potential future use cases and source the data in real-time and scale and store it in a manageable way. This will enable security teams to establish historical baselines to perform investigative data science experiments and retrospective analysis.

2 Utilize an integrated advanced analytics-driven platform.

- **De-fragment and reconcile siloed data for rapid insight generation.**
- **Power analysis with ML and other advanced forms of AI.**
- **Use AI and automation to close skills gaps.**

Fragmented data results in fragmented investigation and forensic analysis. Cybersecurity requires an integrated and intelligent analytics-based platform that can automate scanning at the scale and speed required to process increasingly agile digital data and workload patterns.

The cyber analytics platform must be able to crunch through massive volumes of disparate data and derive meaningful insights, convert data into intelligent information and detect advanced threats using data science, deep learning, edge analytics and AI. By applying advanced analytics technologies to threat data at big data scale, this type of platform could enable automated correlation of events from multiple data sources across hundreds of dimensions and generate deep intelligent insights such as event-chaining, user behavior and risk quotients; activity patterns and deviation from a normal sequence; proactive identification of vulnerability gaps and weak links; and use of social media data to track potential local security incidents.

Automated orchestration is critically needed in the case of zero-day exploits. A platform that goes beyond traditional analyst tools and capabilities can bridge the gaps that human efforts struggle to fill.

Cybersecurity requires an integrated and intelligent analytics-based platform that can automate scanning at the scale and speed required to process increasingly agile digital data and workload patterns.

3 Seek real-time data enrichment.

- **Add structure and context with metadata such as geo-IP lookups.**
- **Correlate disparate data to derive meaning.**
- **Add streaming analytics for real-time alerts.**

Simply collecting large volumes of data without preparing it for analysis can result in a data deluge. The cyber analytics platform must be able to correlate patterns among disparate sources of data, using the required metadata to connect the dots.

For example, legacy systems often send data with timestamps but no indication of time zone. Without that information, SOC analysts cannot be certain of where and when an event was triggered to correlate it with events from other sources with different time zones. If there is inherent system latency, the analysis is completely skewed.

It isn't viable to create a comprehensive master database in a networked world. With the large data payloads generated by the cloud and IoT, absence of sufficient metadata elements can lead to ineffective triaging of an incident. The cyber analytics platform must enrich enterprise event data by tagging critical metadata such as unique host names, geolocation, time zone, etc. as soon as it is ingested. Real-time metadata tagging is critical to understanding the context of an incident and determining the complete picture surrounding the data.

4 Apply intelligent visualization.

- **Create a customizable command center view for holistic security.**
- **Facilitate egress integrations for business intelligence tools.**
- **Enable seamless collaboration with the data scientist community**.

With traditional SOC dashboards and vendor-specific information security tools, incident analysis involves switching between several consoles and user interfaces, and performing manual checks and static analysis on data to determine root cause while maintaining chain of custody. Each step needs to be repeated for each triggered alert. This manual method of analysis and reporting is highly time-consuming, prone to human error and limited in the amount of data available for analysis at any given point in time.

It takes dedicated personnel to maintain and monitor such siloed dashboards and perform analysis. An SOC analyst specializing in an individual vendor-based information security tool may not be able to correlate the events from a parallel source of information from a different tool. Search capabilities are inherently limited in terms of the amount of historical data that can be queried for analysis and the ability to collaborate easily with fellow members of the team.

The cyber analytics platform must provide SOC analysts with a single view of current IT risk and health scores, as well as a digital map connecting the dots between thousands of people, machines and devices and their interactions. It must also provide the flexibility to create purpose-built dashboards that present intelligent information from correlated data and insights derived from advanced analytics such as real-time behavior profiling.

Interactive development tools such as notebook interfaces (i.e., web-based collaboration tools for data engineers and data scientists) can be used to provide capabilities for real-time and ad hoc AI/ML model creation.

5 Expand the security analysis surface via the cloud.

- Extend the boundaries of data gathering.
- Augment security by deploying cloud-native security tools.
- Cross-validate with in-house data to get a comprehensive view.

As enterprise perimeters expand to the cloud via IoT, IT organizations need solid cloud security protocols and a holistic view of the user and system activity patterns across on-premises and cloud environments. With immature security auditing and governance capabilities in the cloud, threat vectors for data leakage and exfiltration can increase substantially.

Consider a scenario in which an employee uploads data and files from the office laptop to cloud storage that is open to public access. Without end-to-end visibility of the event chain, vulnerability checks and analysis would be inaccurate and time-consuming. Simply leaving the liability in the hands of cloud service provider expands the risk of cyber threats to a whole new level.

Security and compliance analysis can be augmented with cloud-native security products feeding cloud event data into the cyber analytics platform. The result is a comprehensive picture of overall user and system behavior, which helps to minimize the attack surface and protect against vulnerabilities, identify theft and data loss.

With cloud-native security products, organizations can better identify cloud assets, which is critical when dealing with vague cloud-generated private IPs across multiple cloud accounts.

Bringing it all together

Figure 3 depicts an end-state high-level reference architecture of a conceptual next-gen cyber analytics platform.

Such a platform can now be conceived and built easily by integrating industry-standard advanced analytics tools and big data technology. This is even more possible today with rapid advancement in advanced analytics technology in community-driven development, commercial products and public cloud services.

Organizations can leverage available tools to prototype and validate best-of-breed technologies to quickly deliver on the cyber analytics platform vision while also addressing business priorities. These include a plethora of options available for an on-premise model, such as Apache open source products, and cloud-native products such as Databricks and Snowflake. Competitive options are also available from popular public cloud vendors such as IBM QRadar on cloud, AWS SageMaker, Azure Analysis Services and Google Cloud ML.

Our Cyber Threat Defense is one such envisioned platform available as a service with ready-to-use threat analytics providing actionable insights. (For more insight, please visit us at our website.)

Envisioning a next-gen cyber analytics platform

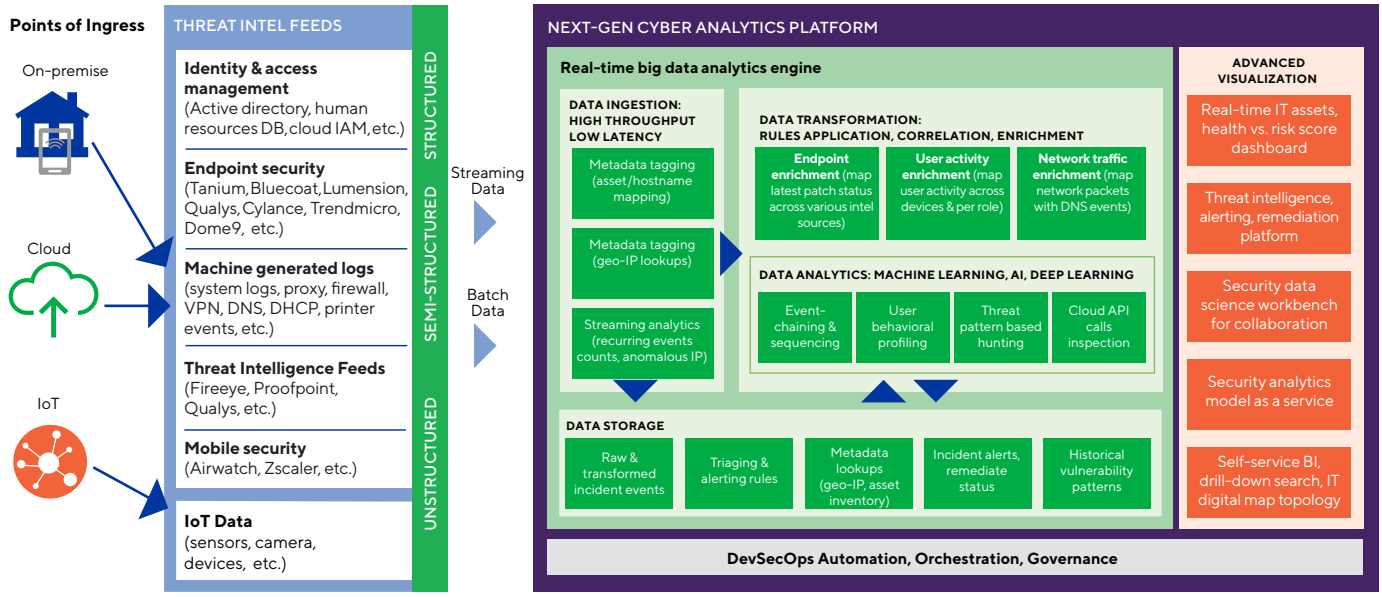


Figure 3

Next-gen analytics platform in action

Let's look at how organizations can solve two prominent security use cases using a next-gen analytics-based paradigm.

Endpoint reconciliation

The majority of attacks occur at the enterprise endpoint level. With bring your own device (BYOD), remote/mobile employees and cloud initiatives, the network security perimeter for most enterprises has all but dissolved. It's critical to establish an effective endpoint security measure and understand the complete picture of endpoint security health at any given point to prevent cyber attacks.

Using security products such as Tanium, Cylance, Cisco AMP and Qualys as agents in endpoint devices (on-premises and cloud), organizations can monitor and capture the vulnerability and compliance status of the device in real-time, along with last-logged-in user identification. Microsoft's System Center Configuration Manager (SCCM) handles Windows patch management and anti-malware policies, while Dome9 gathers cloud traffic data. These tools together generate millions of events in real-time.

Identifying system health and user access at any given time is time-consuming when the data from these tools is not integrated. The cyber analytics platform can help to automatically identify and holistically visualize enterprise security and IT health by providing a single-view dashboard of the IT assets' health status and vulnerability score generated using advanced analytics.

Organizations can improve risk analysis and make faster decisions by automatically capturing, integrating and correlating real-time event data with the look-up data from an enterprise asset inventory master database and human resources data (see Figure 4). They can also incorporate a single-view dashboard of the IT assets' health vs. risk score.

Endpoint reconciliation via a next-gen cyber analytics architecture

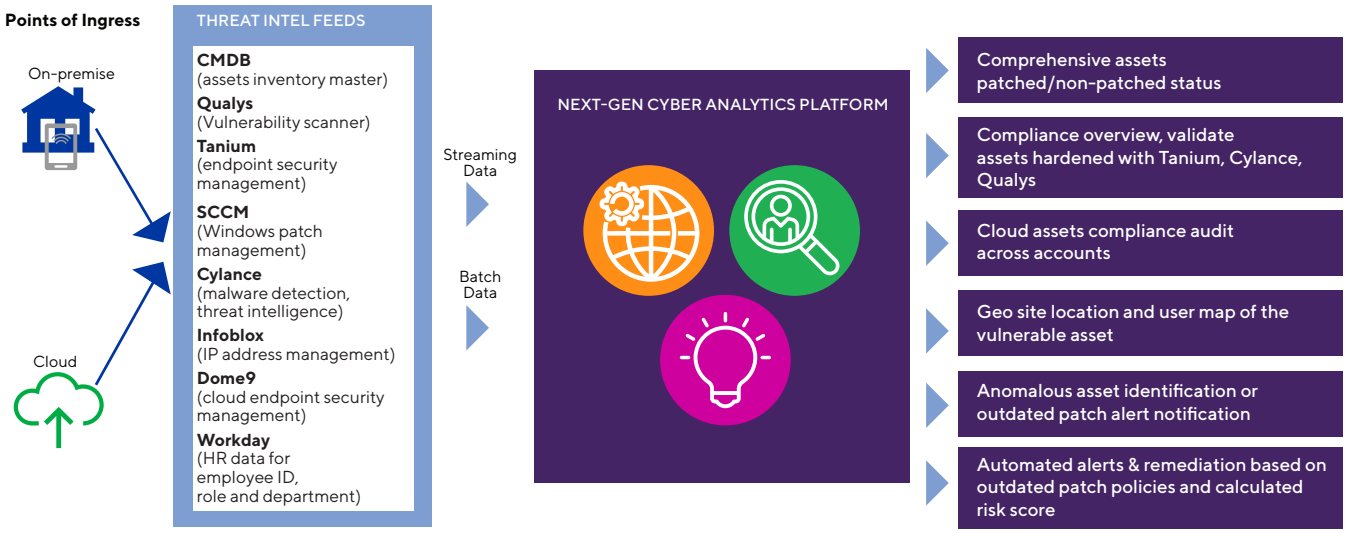


Figure 4

It's critical to establish an effective endpoint security measure and understand the complete picture of endpoint security health at any given point to prevent cyber attacks.

This approach could have prevented the worldwide WannaCry worm cyberattack in May 2017, in which over 300,000 systems running the Microsoft Windows operating system were compromised.[15] The exploitation – which impacted major organizations including FedEx, Nissan and Britain's National Health Service – was caused by a Windows vulnerability in the implementation of the Server Message Block (SMB) protocol.

A month before the outbreak, Microsoft discovered and released a security patch for the vulnerability; however, organizations that failed to update their patches were exposed.

An intelligent and integrated cyber analytics platform could have helped identify such a lapse at an early stage by proactively tracking and managing endpoint reconciliation, enabling faster security control measures (In this case, either decommissioning the outdated machine or updating the OS patches) to better protect the enterprise.

Data loss prevention

Enterprise endpoints are points of egress for business data. It is critical, therefore, to monitor endpoints for user behavior patterns and prevent insider threats causing data exfiltration or accidental data leakage or exposure. Cloud, mobile and BYOD adds complexity to this problem.

In hybrid environments, millions of user activity data points collected over thousands of endpoints and devices by disparate security monitoring tools do not reveal the sequence of events in a comprehensive way. Tracing the data loss to a specific employee and device creates a needle in the haystack situation for SOC analysts.

A cyber analytics platform can mitigate this visibility gap by enabling collection, aggregation and correlation of events from multiple data sources, providing a better representation of malicious or negligent insider behavior.

By incorporating advanced analytics such as deep learning and AI, it is now possible to identify and isolate anomalous user behavior when compared with past behavioral patterns and current role privileges.

For example, a cyber analytics platform can combine internet activity data from proxy monitoring tools such as ZScaler with user activity data from Microsoft Sharepoint, OneDrive and other cloud collaboration tools and add intelligence from endpoint user activity monitoring security agents. Such agents include Lumension, which tracks universal serial bus (USB) security, and Varonis, which detects unauthorized access to file servers, email systems and Microsoft Active Directory.

Organizations can further enrich this data with VPN and geolocation data to check remote access by users and human resources data to validate users' authorized role and department. This helps to create a comprehensive user behavior analysis and validate operational sequences of an employee in real-time.

By incorporating advanced analytics such as deep learning and AI, it is now possible to identify and isolate anomalous user behavior when compared with past behavioral patterns and current role privileges. This approach of user and entity behavior analytics (UEBA) helps organizations quickly identify and classify high-risk activities and user accounts. Automated security policies can be integrated to notify or suspend high-risk user accounts or change vulnerable security access controls for the user.

Data loss prevention using a next-gen cyber analytics architecture

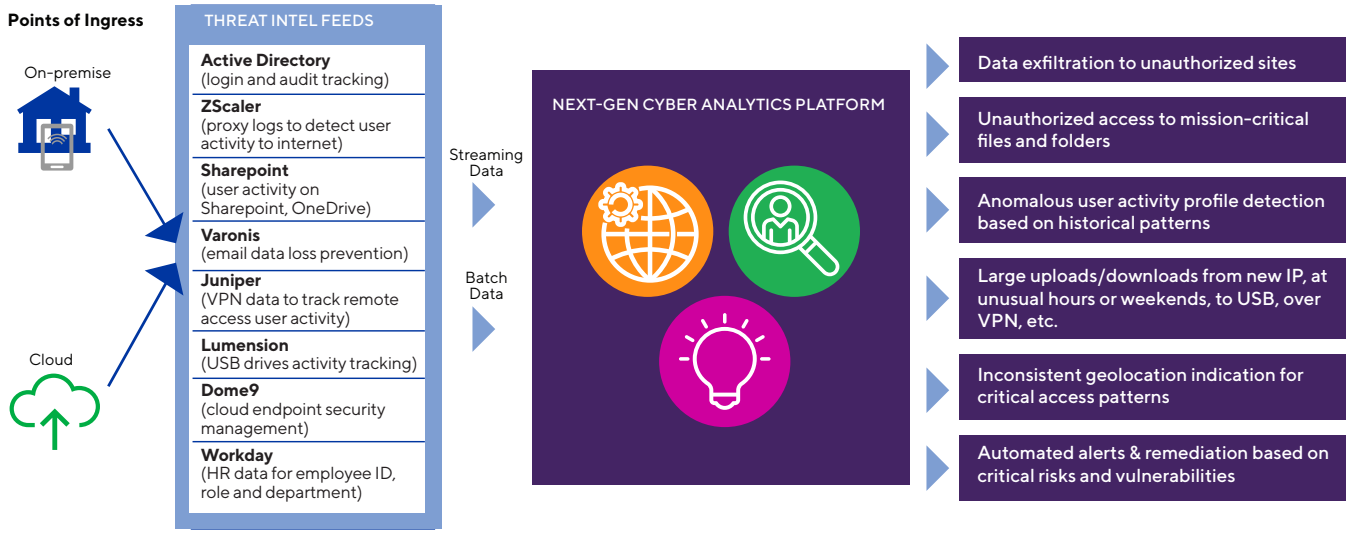


Figure 5

Quick Take

Taking a data science approach to security

In recent years, the topic of security analytics has become closely interrelated with SIEM products, with most vendors in this space launching products built around native AI and ML analytics capabilities, such as the Cylance AI platform. Concurrently, security analytics players are launching into the SIEM market.

In the early days of security analytics, the platform had to be developed from scratch. But as a result of the challenges outlined in this white paper, organizations invariably struggled to build and maintain these environments. In fact, some have been inching away from ground-up custom analytics platforms to commercial o□-the-shelf (COTS) solutions.

By far, the greatest failure is not clearly defining the security control use cases for analytics. Entire companies have been founded to address this need with commercial threat intelligence services such as Anomali, which generates up-to-date blacklists to refine the event data in the platform. Customers also struggle to not just detect but also respond to the overwhelming number of security incidents, so the connection to security orchestration automation and response (SOAR) is the future, at least circa 2019.

Designing these kinds of technologies is not as simple as previously considered. Recruiting data science expertise to mine the data lake is di□cult – this skillset is one of the rarest and most expensive in the industry. This can be easily avoided if an organization focuses on addressing the security events rather than analyzing and detecting them, which can easily be handed o□ to a more specialized partner or vendor.

Therefore, we recommend applying the next-gen cyber analytics building blocks where it makes sense and extending these with COTS solutions.

Finally, fully managed security services, which provide organizations with business outcome-driven, orchestrated security operations based on multi-tenant analytics platforms, such as our Cyber Threat Defense, provide an e□ective response for organizations that have struggled with implementation of analytics platforms.

Looking ahead

Organizations need to assess their cyber risk from an organizational, cultural, structural and talent perspective and evolve their security practices and polices to weather the cybersecurity storm and be positioned for success.

- **By adopting an AI-driven security automation framework, organizations can align their cybersecurity maturity with digital maturity.** Such a platform must be able to crunch and correlate threat patterns on massive volumes of disparate data, which introduces opportunities for advanced cybersecurity without business disruption. Using sophisticated alerts and prescriptive analytics for dynamic policies to address identified risks, organizations can speed deployment of threat-blocking measures – thereby increasing the agility of security operations.
- **Security automation can help mitigate skill gaps and cybersecurity knowledge fragmentation.** This can expedite threat hunting, insight generation and remediation. Moreover, organizations must cross-train SOC analysts and upskill team members to face digital threats and elevate security best practices and awareness among the broader employee community.
- **The current threat environment requires a more proactive and adaptive approach that incorporates continuous monitoring and real-time assessments.** Guidelines recommended by industry-standard risk assessment frameworks like the National Institute of Standards and Technology (NIST) CyberSecurity Framework provide best practices to manage cybersecurity-related risk.[16]
- **Cybersecurity is an evolving and moving objective.** Organizations must continuously adapt their cybersecurity models to improve their preparedness and build confidence in their ability to face, detect and thwart potential cyber threats.

Digital business requires digital cybersecurity that makes the best use of advanced analytics and intelligent automation to achieve their digital objectives at a pace and scale that outsmarts threat vectors.

Endnotes

1 "Juniper Research: Cybersecurity Breaches to Result in Over 146 Billion Records Being Stolen by 2023," MarketWatch, Aug. 8, 2018, https://www.marketwatch.com/press-release/juniper-research-cybersecurity-breaches-to-result-in-over-146-billion-records-being-stolen-by-2023-2018-08-08.

2 "2018 End-of-Year Data Breach Report," Identity Theft Resource Center, 2019, https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

3 Louise Matsakis and Issie Lapowsky, "Everything We Know About Facebook's Massive Security Breach," *Wired*, Sept. 28, 2018, https://www.wired.com/story/facebook-security-breach-50-million-accounts/.

4 Tony Bradley, "Security Experts Weigh In On Massive Data Breach of 150 Million MyFitnessPaul Accounts," *Forbes*, March 30, 2018, https://www.forbes.com/sites/tonybradley/2018/03/30/security-experts-weigh-in-on-massive-data-breach-of-150-million-myfitnesspal-accounts/#16776e223bba.

5 "Marriott Announces Starwood Guest Reservation Database Security Incident," Marriott International, Nov. 30, 2018, https://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident/#.

6 Vibhuti Sharma and Munsif Vengattil, "Zuckerberg Loses More than $15 Billion in Record Facebook Fall," Reuters, July 26, 2018, https://www.reuters.com/article/us-facebook-results-stock/facebook-braces-for-stock-wipeout-as-lower-margins-loom-idUSKBN1KG1TN.

7 "Cost of a Data Breach Study," Ponemon Institute, IBM, July 2018, https://www.ibm.com/security/data-breach.

8 Jeremy C. Owens, "The Equifax Data Breach, In One Chart," MarketWatch, Sept. 10, 2018, https://www.marketwatch.com/story/the-equifax-data-breach-in-one-chart-2018-09-07.

9 "Six Ways CEOs Can Promote Cybersecurity in the IoT Age," McKinsey, 2017, https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/six-ways-ceos-can-promote-cybersecurity-in-the-iot-age.

10 "CIO Agenda 2019: Digital Maturity Reaches a Tipping Point," Gartner, 2018, https://www.gartner.com/smarterwithgartner/cio-agenda-2019-digital-maturity-reaches-a-tipping-point/.

11 Mark Austin, "Hackers Broke Into a Casino's High-Roller Database through a Fish Tank," Digital Trends, April 15, 2018, https://www.digitaltrends.com/home/casino-iot-hackers-fish-tank/.

12 Jeff John Roberts, "Killer Car Wash: Hackers Can Trap and Attack Vehicles," *Fortune*, July 27, 2017, http://fortune.com/2017/07/27/car-wash-hack/.

13 "Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens," $(ISC)^2$, 2018, https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study.ashx?la=en&hash=4E09681D0FB51698D9BA6BF13EEABFA48BD17DB0\h.

14 "Navigating a Cloudy Sky," McAfee, 2018, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-navigating-cloudy-sky.pdf.

15 Chris Graham, "NHS Cyber Attack: Everything You Need to Know About 'Biggest Ransomware' Offensive in History," The Telegraph, May 20, 2017, https://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-o□ensive/.

16 NIST cybersecurity framework: https://www.nist.gov/cyberframework.

About the author

Archana Rao

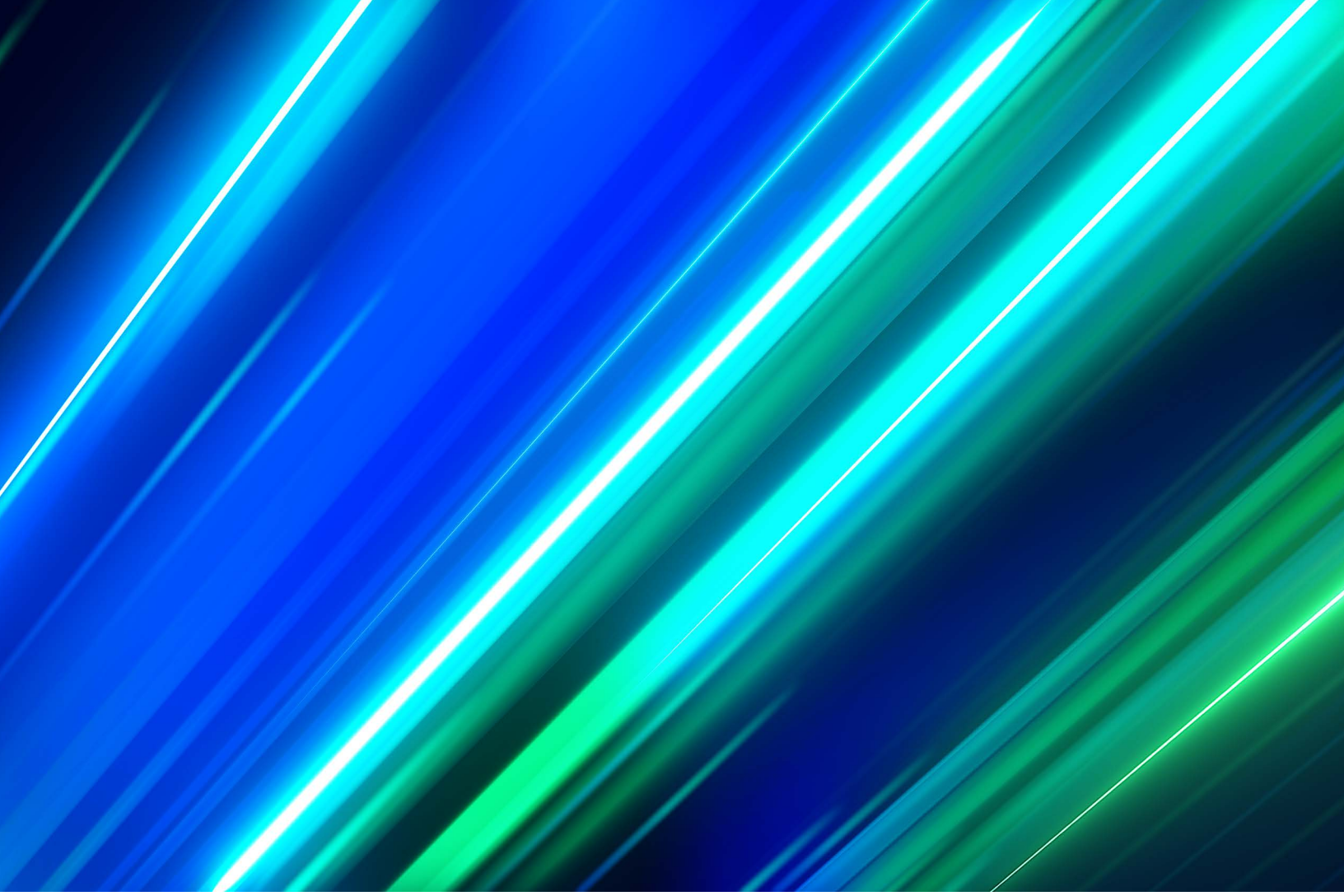
Principal Architect, Cognizant Digital Technology Consulting

Archana Rao is a Principal Architect within Cognizant Digital Technology Consulting. She has 15-plus years of cross-industry IT experience, developing and providing solutions focused on architecture and design of enterprise high-performance computing and analytics applications using big data, AI/ML and public cloud native services, to help clients implement strategic technology initiatives. Archana has considerable experience involving batch and streaming architecture patterns serving high-throughput/low-latency requirements, including architecting a next-gen cyber analytics platform on AWS public cloud for a large car manufacturer in the U.S. She holds a B.E. in electrical engineering and electronics from University of Madras, Chennai. Archana can be reached at Archana.Rao2@cognizant.com | Twitter: https://twitter.com/ArchanaRA0 | LinkedIn: www.linkedin.com/in/raoarchana/.

Acknowledgments

The author would like to thank Alan Alper, Vice President, Cognizant Thought Leadership programs, and subject matter experts within the Cognizant Digital Security Practice for their valuable contributions to this white paper, including Harry Bannister, CISSP, CCSP, Associate Director, Portfolio Strategy and Positioning, and Sam Dillingham, CISSP, Associate Director, Managed Security Services Strategy & Product Positioning.

Special thanks also to Cognizant Digital Technology Consulting's Mahadevan Krishnamoorthy, Assistant Vice President, and Sathish Kumar Muthukaruppan, Senior Director, for their guidance in the writing of this white paper.



Digital Systems & Technology Consulting

Cognizant's Digital Technology Consulting (DTC) Practice provides advisory consulting infused with cross-functional capabilities to enable enterprise-wide digital transformation. DTC's core capabilities span the software and platform landscape. We leverage Agile/DevOps, security and automation to enable businesses to unlock digital capabilities across their front, middle and back offices. Our objective is to help clients eradicate release weekends by enabling continuous delivery. This ultimately helps them to achieve improved end-customer experiences, lower operating costs, improve time to market, enhance operational stability and create a happier workplace. To learn more, visit us at www.cognizant.com/consulting.

About Cognizant

Cognizant (Nasdaq-100: CTSH) is one of the world's leading professional services companies, transforming clients' business, operating and technology models for the digital era. Our unique industry-based, consultative approach helps clients envision, build and run more innovative and efficient businesses. Headquartered in the U.S., Cognizant is ranked 193 on the Fortune 500 and is consistently listed among the most admired companies in the world. Learn how Cognizant helps clients lead with digital at www.cognizant.com or follow us @Cognizant.

Cognizant

World Headquarters

500 Frank W. Burr Blvd.
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters

1 Kingdom Street
Paddington Central
London W2 6BD England
Phone: +44 (0) 20 7297 7600
Fax: +44 (0) 20 7121 0102

India Operations Headquarters

#5/535 Old Mahabalipuram Road
Okkiyam Pettai, Thoraipakkam
Chennai, 600 096 India
Phone: +91 (0) 44 4209 6000
Fax: +91 (0) 44 4209 6060

Codex 4588