Accenture Security Technology Vision 2018

RETHINKING THE FOUNDATIONS

OF THE INTELLIGENT ENTERPRISE

Foundational assumptions in our security programs are being upended. Core elements are being disrupted. That's why understanding what is new has never been more important than now. An approaching compute paradigm is set to throttle existing cryptography. A discovery around hardware vulnerabilities has dramatically exposed attack surfaces. And an upcoming regulation is poised to upset the innovation of security monitoring and automated intelligence.

To enable trust-based partnerships with people—customers, employees, business partners and governments—through technology upon which Intelligent Enterprises depend for growth, security executives must rethink the risks and take decisive action to address these changes—starting now.

THE TIPPING POINT FOR CRYPTOGRAPHY

Remember Y2K? Due to years of careful preparation, it mostly turned into a non-event. Now the security sector faces a much more massive, more disruptive event arising from quantum computing that will override existing cryptography methods and make current infrastructure and application protections irrelevant. Given the scale and scope of the issue, Intelligent Enterprises must prepare now with a comprehensive strategy and upgraded cryptographic infrastructure—while ensuring business partners and digital ecosystems are equally safeguarded.

As the countdown to the year 2000 began, business and IT executives around the globe held their breath, hoping that the years of work to locate and expand every truncated two-digit date to four digits—in every system and every application—would enable global commerce to keep functioning. The diligent planning and deep investment of time and energy paid off.

In the 18+ years hence, business and technology has accelerated at an astonishing rate, bringing with it cloud, data analytics, digital platforms and ecosystems, artificial intelligence, microservices, blockchain and, most recently, the realization of quantum computers.

As exciting as these technology advancements are, the emergence of quantum computing also brings a new and much larger type of security issue—one that will eclipse Y2K in terms of the scale and scope of impact on infrastructure and storage, business transactions and platforms, and business-to-business (B2B) and business-to-customer (B2C) applications.

Put simply, quantum computing presents a direct threat to modern cryptography and crypto systems. Existing cryptography methods—public key encryption, digital signatures and key exchanges—are on the verge of extinction because quantum computing jeopardizes the strength of the underlying math.

All three of these methods (public key encryption, digital signatures and key exchanges) are largely based on Diffie-Hellman, Rivest Shamir and Adleman (RSA) and elliptic curve cryptography. Protection or cryptographic strength is achieved by making the math problem (such as Integer Factorization and Discrete Log problems) difficult and cumbersome to solve. However, through the quantum properties of matter and energy, quantum computing can perform these calculations very efficiently, rendering the intractable task instantaneously and exposing businesses to threat actors globally.

As such, quantum computing presents a major security challenge that scholars, researchers and entities like NIST are actively assessing. But this is much larger than an academic issue; NIST estimates it took approximately 20 years to field the modern public key infrastructure that powers businesses today. While there are expected efficiencies in adopting new technologies going forward, companies should not underestimate the scale of the business challenge. Our existing cryptographic methods are the fabric of commerce, communications, identity and data protection at large—and all must be reviewed and potentially updated to continue conducting business safely and securely in a post-quantum world.

A "Key" Analogy

Think of a house that is protected by a front door with a lock. There is a unique key to unlock that door. For someone else to get into the house, they would need to test all possible keys from the manufacturer's key ring to find the one that will work. What quantum computing lets threat actors do is try every possible key at once, rendering the lock useless and the house unprotected.

Start planning for quantum-proof future

So how much time do we have? Each month a new milestone is broken—from Intel's Tangle Lake and Google's Bristlecone with 50- and 72-qubit hurdles—evidence of the race around error-corrected quantum compute with many companies investing in the promised processing efficiencies.

What do these benchmarks mean for digital businesses? The cryptography supporting the existing and new systems being put into production today will be broken by quantum. The foundations enabling and protecting the business—identity, signature, SSL certificates, blockchain identity and non-repudiation, encryption technologies for data protection—will be null and void.

Although it will take thousands of qubits to become a threat to cryptosystems, Accenture believes that national labs and nation states will quietly break that processing barrier within the next eight years—by 2025. Most estimates for commercially available quantum computing range from 10-20 years in the future due to the fragility of quantum computing, which requires an interference-free environment of nearly zero degrees Kelvin. However, businesses and industries that are targeted by nation state threat campaigns should anticipate the accelerated timeline because these accomplishments will be largely unreported.

If that isn't enough, exposure is not limited to business operations and data at some notional point eight years from now. Another dimension to the threat is the past. Adversaries who have collected intelligence and information from years of campaigns will also have the keys to a company's history—and it may be revealed. Security executives must ask: What information have nation states been collecting about their business, such as passwords, intellectual property or an understanding of business methods?

Companies must comprehend both the nature of the threat and threat actors to know what they are collecting now. Understanding threat actors' motivations is critical to understanding business exposure and prioritizing remediations around cryptographic methods and other means of protection. Threat intelligence is business intelligence. Threat intelligence managed service providers provide the deep knowledge and understanding of not only the threat actors and their sponsorship, but also the marketplace around a company's data on the dark web.

New Engine, New Math

This is the first time in computing that there is a different machine and computational engine based on different physics.

A quantum computer is a new form of computing technology that harnesses quantum mechanical phenomena rather than binary functions to perform computational operations. To learn more, visit www.accenture.com/quantum and read the Accenture point of view, Think Beyond Ones and Zeros: Quantum Computing Now.

Cyber-espionage campaigns are emanating from various nation state-aligned groups who seek to act in the interest of a particular country. These campaigns can include malicious email attachments, ransomware or financially motivated attacks. Organizations must understand how their footprint exposes them to nation state attacks based off geography, industry and affiliations. High-level threat groups from or affiliated with China, Russia and North Korea are important to keep an eye on. **To learn more, see the 2018 Cyber Threatscape Report, from iDefense, part of Accenture Security.**

Next moves for security executives

Clearly, the timeframe to begin strategic mitigation planning is now. With careful preparation, companies can reduce the exposure of cryptographic systems that provide authentication, integrity and confidentiality in business operations and communications by making existing enterprise systems more resilient and migrating away from enterprise systems where compromise is imminent. Those that begin the process now will be more likely to complete it before the inflection point when quantum computing is viable and capable of breaking our cryptographic protections. To get started, CISOs should take these steps:

1 **ASSESS THE CHALLENGE**

Gain a big picture understanding of where the risks are across the business. By knowing how business processes are enabled by cryptographic methods, it will be easier to grasp the scope of the challenge. In addition, perform a more detailed inventory to capture crypto method, key length and where the keys and methods are kept and used across storage, enterprise/business partner infrastructure and applications.

2 **DEVELOP QUANTUM MITIGATION STRATEGIES**

Update existing cryptographic methods, evaluate and use new standardized quantum-resistant methods when released, or turn to alternative controls to protect the data.

Several cryptography-as-a-service solutions have matured and should also be considered. Vendors that separate key from cryptographic method will position the business to transform quickly as emerging quantum-proof standards and cryptographic methods are developed, significantly reducing risk through the business transformation.

To learn more, read Accenture Labs' upcoming Quantum Cryptography technical white paper for security IT and administrators, which provides more context, research and analysis of the issue, along with short-term steps to bridge the gap and long-term steps to maintain new quantum-proof cryptographic standards.

HARD LESSONS ON HARDWARE

Although difficult to predict, the lessons from Meltdown and Spectre have become abundantly clear. The security community should have suspected hardware would be vulnerable and taken steps to mitigate the risk.

Companies got a rude awakening in early 2018 that shifted C-suite attention back to an unexpected place: hardware. The announcements about Meltdown and Spectre, CPU-level bugs in microprocessor design discovered by security researchers across industry and academia, jolted the complacent view that microprocessor technologies were inherently safe.

Although the idea of hardware attacks is not new, Meltdown and Spectre were unprecedented in their impact because of the tremendous scope of affected vendors and chipsets going all the way back to CPUs manufactured in 1995. (Note: GPUs were a bright spot during these dark days as they are fundamentally different in design, but that does not mean security executives can assume classes of hardware are future proof.)

The repercussions of Meltdown and Spectre to global businesses were far-reaching: the servers and affected hardware accelerators powering many enterprise systems and applications, internet of things sensors, desktops, laptops, tablets, smartphones and other devices were at risk—and may still be.

The vulnerabilities exposed a much broader attack surface to threat actors than ever before. While side channel attacks are a known security concern, and some may even exploit the CPU cache, none to date have been as severe. And because of the very nature of the vulnerabilities that Meltdown and Spectre present, it is highly unlikely that organizations will be able to readily detect whether a system has been successfully attacked.

The next hardware-level vulnerabilities and subsequent exploits may already exist. Security executives need to operate with the assumption that this is the new normal in attack surface management and rethink the cyber resilience of business operations. As a result, companies will need to revisit every aspect of how they are delivering core and customer-facing business processes—down to the hardware and delivery platforms.

Technical view of Meltdown and Spectre

The Meltdown and Spectre attacks capitalized on two features in modern processors called speculative execution and caching. These features are used in most current CPUs to improve the processing time. The better performance is achieved through out-of-order instruction execution and branch prediction that speculative execution offers. Moreover, caching memory reads by speculative execution of instructions helps CPUs reduce the memory access time and increase the processing time significantly. Attackers use cache timing side-channel attacks to find out whether the data is cached or not, and consequently read kernel data stored in the cache. Since most of processors use speculative execution, attackers can use illegal read commands to store kernel data into cache and flush the cache before being blocked by the processing unit.

For more information, see Accenture Managing Malware **page.**

Aftermath of an attack

Since the news broke before the official embargo end date, CISOs across every industry have been challenged to navigate the landslide of vendor communications, provide oversight of remediation and triage the residual risk. There was a lot of uncertainty as many of these fixes were issued quickly in the days following the vulnerability announcement. Many product and vendor communications were not at the level of clarity needed, leading to reissuance of patches and confusion across the industry as to what patches to apply, where they were applying them—BIOS, CPU microcode, operating system or browser—and the effectiveness of remediation.

As of today, effective patches still are only available for a small subset of the chipsets affected while malwares samples and variant vulnerabilities have already emerged, including MeltdownPrime, SpectrePrime and SgxPectre. In particular, Spectre opened a new class of attacks, and it is still unclear whether the current patches will be enough to prevent the exploitation of other CPU features.

Redesigning hardware from the ground up

Even though impacted vendors had been working on patches since June 2017, at the end of the embargo in January 2018 there was only a patchwork of fixes and alternative methods to mitigate the exploits. And security executives will be managing these vulnerabilities until the next generation of "speculative-execution proofed" hardware arrives. Unlike the software development lifecycle, which is relatively quick with rapid update or patch cycles, hardware architecture design for the next generation of CPUs is a much longer process. Severe hardware vulnerabilities like Spectre require replacement, which is very costly and creates business disruption.

In short, the technology industry robbed security to get payout in processing performance. The pressure to improve performance on existing chipsets came at the cost of security. New methods to increase the experienced performance of the microprocessor cached sensitive code into an unprotected area of the CPU—clearly a usage of this space that was never anticipated by the hardware designers. A more holistic view is needed from now on, as the race for performance must be tempered with an understanding of how systems are exploited and how systems fail.

Fortunately, there may be some software design learnings that can be applied to hardware. Software security has long relied on the concept of least privileges and enforces segregation of data, role and security perimeter. Beyond the classic memory corruption vulnerabilities (e.g., buffer overflow, null pointers), most recent exploits rely on the instructions within the software's binary to mount sophisticated attacks known as return-oriented attacks. Recent prevention techniques against this class of attacks are known as control flow integrity (CFI) in which the software execution path is enforced, and the attack is detected if a violation of the excepted flow occurs with minimal performance overhead.

Recapping lessons learned

Businesses that moved to the cloud experienced much less disruption as large-scale cloud vendors—including Google, Microsoft, Amazon Web Services (AWS) and Oracle—who were informed during the embargo of Meltdown and Spectre. They were at the forefront of the solution with six months of lead time to prepare and execute patching windows on their managed servers.

Companies relying on the cloud were left with fewer devices to patch on their own and freed from day-to-day patch management, whereas those businesses with a larger footprint/investment in proprietary physical data centers did not have this head-start and were only notified when the embargo lifted. When disclosure of critical vulnerabilities is a cascade effect and not a firehose, businesses with early exposure may prove the most secure.

Companies also should not underestimate the value of hardware diversity. While CPUs were largely affected by Meltdown and Spectre, GPU/GPGPU hardware accelerators were not affected due to the fundamentally different way in which they manage processing. The same is true of other hardware accelerators like field programmable gate arrays (FPGAs), application-specific integrated circuits (ASICs) and custom hardware accelerators built by enterprises to run emerging technologies, such as virtual reality and augmented reality applications. While this does not mean these technologies are impervious to future attacks, the variety could provide an invaluable cross-defense in future hardware architectures.

The overarching takeaway for hardware and software developers is that they must rethink design and protection of core functionality and features across all product sets to contain these and other types of security issues in the future. In the meantime, security executives must dismantle some of their foundational beliefs about hardware, software, cloud and security overall—and take a harder line on hardware protections.

Next moves for security executives

To prepare for the next unexpected (but inevitable) incident, companies should consider expanding attack simulations and threat modeling to include hardware vulnerabilities, not just software vulnerabilities and malware. In instances where there is very little credible attack information to use, it's still necessary to make decisions as quickly and correctly as possible. A more rigorous risk management approach across these areas is vital:

1 REVISIT HARDWARE

Recommit to resilience and agility across all underlying technologies supporting core enterprise and customer-facing business processes. Start with a good, hard look at the whole stack of CPU, GPU and microcontroller processing mechanisms in the existing hardware infrastructure—both inside the enterprise as well as distributed across critical third- and fourth-parties and cloud and managed service providers.

2 STRENGTHEN DISASTER RECOVERY

Reinforce disaster recovery processes to make sure all parties have methods in place to not only withstand attacks, but also recover business-critical systems quickly. For example, a company's network defense team can plan out which systems need to be brought down and in which order to minimize the damage from downtime. This assumes there will be techniques available to detect the active exploitation of vulnerabilities on various infrastructures. Hence, detection strategies require the ability to gather solid intelligence about what malicious attackers are doing.

Being on an active lookout for exploitation is a 24/7/365 job. Engaging an external cyber threat intelligence service that can raise the alarm as soon as signs of active exploitation emerge, combined with an enterprise data intelligence practice focused on Data Veracity, will play a valuable role as businesses consider moving to a risk-aligned patch strategy that leverages expert assessment and threat modeling of hardware and software vulnerabilities, addressing their ability to be exploited and potential level of impact on the business.

From here on out, hardware security is just as important as software security. CISOs and CIOs must collaborate to optimize both enterprise-level hardware and software interactions and architectures.

3 REFRESH HARDWARE CYCLES MORE FREQUENTLY

Another core aspect of a resilient strategy for microprocessor-based events is lifecycle management—not just software licensing, but also hardware inventory. The organizations that were hardest hit by Meltdown and Spectre had the oldest microprocessors. Boosting the hardware refresh cycles will help companies keep up with ever-accelerating technology.

4 DIVERSIFY HARDWARE TO BALANCE PERFORMANCE WITH SECURITY

At the same time, security executives must proceed with caution in their technology acquisition strategy. Does the business want to deploy hardware or devices with inherent vulnerabilities to Meltdown and Spectre? Millions of post-production devices were also susceptible. Diversifying across different types of hardware (CPU, GPU, FPGA, ASIC, custom) and scrutinizing how performance is achieved going forward will be critical steps.

5 COMMIT TO JOURNEY TO CLOUD

Perhaps the ultimate diversification for IT and security executives is to consider moving to the cloud. Cloud providers were ready, systems were largely patched. This risk transference strategy has additional benefits in that companies do not need to worry about hardware failures, upgrades or even patching, while gaining access to agile software development through microservices. Further benefits to cloud include reducing total cost of ownership and gaining infrastructure scalability on demand.

Taking a hard-core stance on hardware protection and improving enterprise resilience across all aspects of business operations will help security executives make sure the lesson sticks this time.

BUILDING EXPLAINABLE SECURITY PROGRAMS UNDER GDPR

Complying with the European Union's General Data Protection Regulation (GDPR) is just the beginning. The new standard for Intelligent Enterprises will be to create and maintain transparent and explainable security programs globally—and proactively share them with customers, employees and business partners to reinforce trust. Future business growth will depend upon it.

Even as companies finalize their GDPR compliance policies and procedures, a bigger question looms: What's next on the horizon? There's no doubt that stricter data privacy regulations will continue to emerge. At each juncture, security executives will need to aim for the "high-water mark" to make their company regulation-resilient and 100 percent ready to conduct business.

In the meantime, business leaders must accept that GDPR, a regional regulation that nonetheless affects European citizen data wherever it is located, is the new norm—and its highly enforceable. Global companies that serve a global customer base must step up to this more rigorous standard, regardless of where they operate.

Among other things, GDPR requires organizations to implement appropriate technical safeguards to protect data classification, data loss prevention and encryption for any personal data. The timeframe to notify relevant supervisory authorities of a breach has been compressed to a 72-hour window and failing to report in the prescribed timeframe could result in steep financial penalties—up to 4 percent of global operating revenue.

Reading between the lines, the security program and security services are now at the center of business prosperity, ensuring the company's ability to operate in the age of new regulations—and technology trends like Citizen AI.

Conforming to the high-water mark

Multi-national corporations that operate within GDPR participating countries will be faced with two options: either silo data based on the locality it originated from or comply with the standards set by GDPR across their organization.

There are tradeoffs with each option. Siloed data will result in duplicate data retention costs with different data processes in each locality, adding complexity to the data governance and precluding any cross-locality analysis. Complying with GDPR across localities will standardize an organization's data governance process but will result in additional cost for security controls in localities with more lax standards.

It is important to note that other non-EU localities, such as Japan, are now structuring their data security laws to be similar to the current GDPR standards. Therefore, compliance will be the easier route in the long term, which means raising the minimum level of security across the entire organization.

Think "acrylic box"

Additionally, GDPR provides a clear signal that the days of arbitrary data collection and unbridled profiling are gone. The onus is now on business leaders to create and maintain explainable programs that clarify not only what customer or employee data a company is collecting, monitoring or analyzing for insights, but also why it is doing so in the first place. In other words: black box is out; acrylic box is in.

This is especially important with the influx of AI and deep learning technologies being applied across business processes. With the new GDPR standard, companies must proceed with purpose—and with explainable artificial intelligence (AI). Where business processes use AI on customers' or employees' data, they must be prepared to disclose the purpose, mechanisms and insights gained through AI. These activities must also comply with consent agreements for business operation—all while emphasizing people first.

This presents a conundrum for security executives who are charged with defending the business. Security monitoring and insider threat programs heavily leverage behavioral, temporal and spatial monitoring to identify outliers or unusual activity. The who, what, where, when, why and how of security event management is predicated on being able to assemble the picture–situational awareness–of what assets—people and things—are doing on the network without the ability to describe or predict the anomalous behavior ahead of time. Situational awareness is based on a very broad and deep understanding of normal. So, what happens when the "who" is an employee? Or a customer?

For example, under GDPR if a CISO uses AI-based or other monitoring to infer behavioral insights, as to whether the account activity is normal or whether the insights derived would indicate that the account has been compromised, she will have to defend the data use and security purpose of this process in her cyber defense program. Thus, security programs need to be reinterpreted with GDPR in mind, and clearly articulated in terms of the nature and purpose of cyber defense processes. Correlating security program activities to how they ultimately protect customers or employees will be of the utmost importance. To do this, security executives will need to work closely with the new GDPR-required Data Protection Officer, anti-fraud officers and other business leaders, to review how specific security processes support the protection of customers, employees and the business.

This elevated level of transparency into data collection practices will enable Intelligent Enterprises to build and reinforce trust with people, knowing that the companies they choose to do business with are appropriately protecting and maintaining their data.

> **GDPR is upping the ante, but the scope is well beyond data privacy protections. Creating explainable and transparent security programs that use the concept of least privilege will help engender trust with customers, employees, business partners and governments.**

Next moves for security executives

Making data collection programs explainable is easier said than done. It requires new methods to secure and monitor the breadth and depth of data collection, retention and purging practices. Collaborating with a GDPR-compliant security company as a first line of defense can help. In addition, CISOs should consider the following:

1 UPDATE SECURITY OPERATION PROCESSES

GDPR specifies that companies must accommodate the right of individuals to receive an explanation for decisions based on automated processing. This will require creating new data governance processes and approaching algorithms differently. Some security analytics and process automation will benefit by having a human in the loop for outcomes that impact customers or employees.

For instance, if a company has a process to revoke access to a system, it may need to convert from a fully automated process to a partially automated process that uses an interpretable analytic algorithm. This algorithm would need to either alert a security analyst to confirm the results or generate a paper trail that explains the conclusion of the algorithm.

2 STRENGTHEN CONSENT MANAGEMENT FRAMEWORKS

By now, most GDPR-compliant companies have restructured customer and employee consent agreements to specify exactly what purpose current data is being used for—and ideally to outline possible future use cases or applications of the data beyond the original purpose. Since GDPR requires companies to regain consent with each new data set collected with personally identifiable information (PII), which includes IP and MAC addresses, it makes sense to create a repeatable, automated process for obtaining this consent. A better long-term strategy may be for the chief Data Protection Officer, in conjunction with the CISO, to regularly refresh the company's consent management framework both inside and outside the enterprise.

3 FEDERATE AND AUTOMATE ERASURE PROCESS

GDPR grants individuals the right to erasure (aka the right to be forgotten), which means customers or employees can request the removal of their personal data where there is no strong reason for its continued processing. To accommodate these erasure requests, companies will need to develop a business process that first validates the legitimacy of the request, and second vets the identity of the person requesting the erasure of data using strong authentication mechanisms.

Keep in mind this erasure must happen not just for a specific transaction or service, but across all lines of business, which will require a federated capability and cross-functional view of enterprise systems. A CISO assuming this responsibility will need agile tools to mine the data quickly, either redact or remove it entirely, and confirm it is truly deleted.

Automating this process is possible if controlled tightly and monitored closely, as it requires high privileges to access and edit some of the organization's most valuable data. To avoid purging large amounts of data, CISOs should consider installing security mechanisms such as rate limiting.

4 REVISIT DIGITAL TRUST ACROSS ECOSYSTEM AND THIRD-PARTY PLATFORMS

One of the challenging requirements of GDPR is that companies are now responsible for data breaches that occur on their third-party contractors' watch, whether business partners, vendors, consulting companies or accounting firms. By the same token, companies are responsible for honoring erasure requests of data that has been shared with third parties.

To comply, CISOs will need to inventory every single third-party organization their company works with, and review or update agreements to ensure GDPR compliance and ability to honor data erasure requests. Those that can live up to this ecosystem-wide accountability measure will be much more likely to succeed.

5 CONSIDER TOTAL COST OF OWNERSHIP

GDPR exempts specific types of encrypted datasets from the 72-hour reporting requirements for breaches or data loss, making encryption an appealing choice to mitigate some of the financial penalty risks. However, encrypting endpoints and data will result in additional overhead and costs. Security executives will need to balance the short-term costs of adequately protecting data through encryption versus the long-term gains of improving their ability to explain and demonstrate that data has not been accessed or exposed. The latter may be a better choice for ongoing security program maintenance.

Regardless of the evolving regulatory landscape, companies that commit to transparent and explainable security programs will build the resilience and trust they need to keep growing.

Relating our security trends to the Accenture Technology Vision 2018

Security underpins the five trends in this year's Tech Vision:

Citizen AI

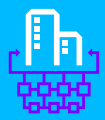
Raising artificial intelligence to be a responsible member of society

Extended Reality

Effectively applying virtual/augmented reality in the business

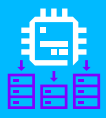
Data Veracity

Maximizing data quality in operations



Frictionless Business

Creating modular and trust-based architectures



Internet of Thinking

Balancing cloud with edge analytics and computing

Each of these exponential technology advancements represents vast potential for business. And all of them require a deeper commitment to security.

Using secure technology-enabled access at each level of the enterprise—from strategy through operations—is providing companies with opportunities to grow exponentially by building deeper, more trust-based partnerships with people. It's also introducing new obligations for companies to step up to a more central role in society itself that prioritizes trust and greater responsibility. Getting this combination right is what will unleash Intelligent Enterprises and enable them to grow.

Security will make each of these relationships with people—customers, employees, business partners and governments—possible, enabling access, fortifying trust and significantly improving performance.

AUTHORS

Lisa O'Connor
Managing Director, Cybersecurity R&D,
Accenture Labs
lisa.oconnor@accenture.com

Josh Ray
Managing Director, Global Cyber Intelligence,
Accenture Security
joshua.a.ray@accenture.com

Tom Parker
Group Technology Officer, Accenture Security
tom.parker@accenture.com

CONTRIBUTORS BY CHAPTER

Quantum: Louis DiValentin, Nahid Farhady, Carl Dukatz, Charles C. Watson

Hardware: Azzedine Benameur, Amin Hassanzadeh, Rikki George, Deapesh Misra

GDPR: Louis DiValentin, Malek Ben Salem, David Cooper

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 442,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com

ABOUT ACCENTURE LABS

Accenture Labs incubates and prototypes new concepts through applied R&D projects that are expected to have a significant strategic impact on clients' businesses. Our dedicated team of technologists and researchers work with leaders across the company to invest in, incubate and deliver breakthrough ideas and solutions that help our clients create new sources of business advantage. Accenture Labs is located in seven key research hubs around the world and collaborates extensively with Accenture's network of nearly 400 innovation centers, studios and centers of excellence globally to deliver cutting-edge research, insights and solutions to clients where they operate and live. For more information, please visit www.accenture.com/labs.

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.