splunk>

SPLUNK 2018 PREDICTIONS

splunk>

WHAT WILL THE FUTURE BRING?

The heart line. The life line. The fate line. The wisdom line.

At Splunk, our experts don't read palms, but they do look into the future. The future of artificial intelligence (AI) and machine learning (ML), IT operations, security, and IoT. Join us once again as we connect with our renowned experts to capture their predictions for the next big thing in their fields.

Our experts see IT embracing DevSecOps to combat the growing sophistication of digital adversaries and an emergence of out-of-the-box machine learning solutions targeting classic enterprise use cases such as anomaly detection, event correlation and capacity-forecasting scenarios. They also expect automation will help alleviate mundane security tasks and help close the skills gap, and the public sector will embrace the smart city, where sensors and automation enhance the reliability of safety, environment and other services. Whatever your outlook, there's a lot to look forward to in 2018.

Read the full predictions on:

Artificial Intelligence and Machine Learning - Toufic Boubez, Vice President, Engineering

IT Operations - Rick Fitz, Senior Vice President, IT Markets

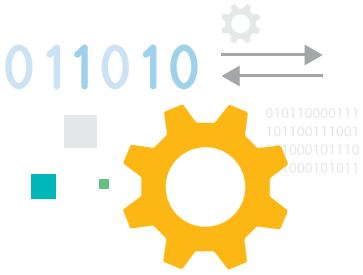
Security - Haiyan Song, Senior Vice President, Security Markets

IoT - Erick Dean, Product Director, IoT

2018. IT'S IN YOUR HANDS NOW.

ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

by Toufic Boubez



The buzz stops here

Artificial intelligence and machine learning are often misunderstood and misused terms. Many startups and larger technology companies attempt to boost their appeal by forcing an association with this phrase. Well, the buzz will have to stop in 2018.

2017 was the year that introduced popular backlash to information deemed to be "fake news." Similarly, 2018 will be the year we begin to demand substance to justify claims of anything that's capable of using data to predict any outcome of any relevance for business, IT or security.

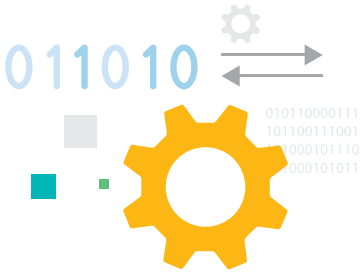
While 2018 will not be the year when AI capabilities mature to match human skills and capacity, AI using machine learning will increasingly help organizations make decisions on massive amounts of data that otherwise would be difficult for us to make sense of.

Pushing past the hullabaloo here are a few things to look out for.

AI and ML become industry-specific

Will the stock price go up or down? Will he purchase shoes with those jeans? Will splicing gene A with gene B demonstrably improve survival rates? AI, powered by machine learning, holds specific promise and actionable insights for many industries.

- **Financial services** organizations have long relied on data-driven decisions to run their organizations, to satisfy customers and to secure their investments. From Jesse James to Bonnie and Clyde, bad guys and gals have long targeted these organizations as a fast path to riches. While the concept of financial security has changed completely, these organizations still need to keep their customers happy. Better apps and improved online payment processes help achieve this, but they also create new attack vectors. AI using machine learning will increasingly provide these organizations with the ability to recognize fraud, identify anomalies in user behaviors and suggest precise steps customers can take to mitigate these threats.
- **Healthcare and biotech** firms rely on vast quantities of data to understand issues impacting our health and to discover advancements in medicine. Machine learning equips biologists and data scientists with tools to catch abnormalities in laboratory experiments and empowers them to more effectively measure experiment quality over time. They are then able to understand correlations—between gene A and gene B, for example—faster and move on to the next step in the path to delivering the next life-changing or life-saving treatments.
- In **manufacturing**, a single down piece of machinery in a complex supply chain can significantly harm production capabilities, impacting margins and competitiveness. Manufacturers have their hands full keeping every component of a modern and connected system of devices running, synchronized and maintained. With AI powered by machine learning, these organizations can now predict which devices will require servicing and when they'll need it before any business-impacting failures occur.
- The rise of **computational journalism** will significantly impact the trajectory of the media industry across the U.S. and throughout the world. In 2018, we will see more and more journalists work collaboratively with data scientists, just as they are doing at the Pulitzer-



nominated Atlanta Journal-Constitution. Journalists will turn to experts in AI, machine learning and natural language processing (NLP) to discover newsworthy stories with maximum relevance for local, national and global audiences, shining a light on issues that might never have been discovered previously.

- The best **retail** experiences are seamless customer-centric engagements spanning websites, physical stores, customer support, mobile apps and social media. The few retailers capable of delivering this omnichannel experience are the ones who capture our attention, evoke an emotional connection with us and secure our loyalty. AI powered by machine learning now becomes a retail differentiator, enabling companies, both large and small, to better understand their customers and to provide targeted recommendations based on a formula consisting of obvious factors (demographics and purchase history), as well as more obscure elements (web usage patterns and social profiles). Retailers that care about loyalty will use machine learning cautiously. Obtaining customer permission will become a new golden rule.

AI and ML go mainstream in B2B

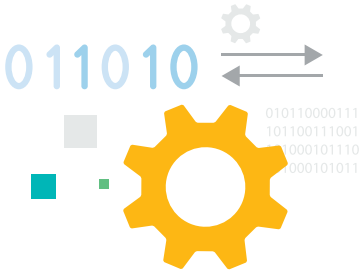
Alexa. Cortana. Siri. We are already experiencing the impact of AI in our lives as consumers. Next up: we will witness an emergence of out-of-the-box AI and machine learning solutions targeting (as in bullseye!) classic (as in yesteryear) enterprise use cases. Anomaly detection, event correlation and capacity forecasting scenarios? Yup, bring 'em on. AI powered by machine learning will be used to foresee a broad array of meaningful insights.

- **Anomaly detection:** Increased access to voluminous real-time data carries the additional burden of identifying relevant signals in a noisy sea of information. Whether it's predicting and preventing a critical IT infrastructure outage or identifying a single unwanted user in traffic of millions, these are among the most crucial and requested AI and machine learning capabilities.
- **Automation:** We're not there yet...we might not ever want to get all the way there...but removing mundane tasks and empowering machines to learn on their own hold promise for increased innovation, productivity and workplace satisfaction. As has been predicted for decades, it is time to consider the implications of environments where machines are working in tandem with humans. Like HAL 9000 promised, we are close to achieving the vision of putting machines to the fullest possible use, which is all that any conscious entity, breathing or binary, can ever hope to do.

The machines will keep learning

We've only just begun. The future of AI and ML is bright and bold.

- **End-to-end AI:** Instead of building a model that recognizes stop signs and then another that distinguishes between pedestrians and Peugeots, you'll begin to see more end-to-end AI, enabled by machine learning models that take in the complete state of the system and output the precise actions you need to take—turn right, speed up, slow down!
- **Self-configuration:** Increasingly, we will have access to tools that do the hard work for us. From architecting to validating to training, you will now be able to deliver end-to-end machine learning capabilities without requiring human intervention.



- **Pre-trained models:** We'll begin to see libraries of pre-trained and open-source machine learning models available as reusable components serving a variety of use cases. For example, a pre-trained model could be applied by a telecommunications company to detect and predict customer churn. Many wireless providers use a similar set of data points, such as billing plan type, number of customer service calls or voice and data usage, combined with customer information. Once a pre-trained model on these types of data is created, it can be shared with other providers, delivering value that scales across the industry.
- **AI for IoT:** The increasing commoditization and scale of sensor devices will drive a new wave of smart industries. Smart devices, machinery, fleet vehicles and more will still need to be managed. They'll need to be repaired and serviced. Ink cartridges? Yes, these will still need to be replaced. The arrival of a coupling between machine learning and IoT creates requirements and opportunities for dramatic improvements in network performance and uptime, as well as resource management.

In 2018, AI and ML will make major inroads into our work lives. All for the better. Admittedly a biased member of this community, I can't wait to see what's next.

IT OPERATIONS

by Rick Fitz

Artificial intelligence spurs the reinvention of IT

Artificial intelligence and machine learning, applied correctly, will dramatically simplify IT operations by enhancing and automating IT ops processes and tasks. IT has become too complex, and operators are in desperate need of technology that can simplify and streamline their work. While we talk about the prospect of self-driving cars or machines that can win a game of Go, the real impact of AI can be readily seen by applying it in the daily operations of IT. This evolution will see predictive analytics replace manually intensive activities with intelligent automation. The big win is that IT organizations will be able to leverage data and AI to quickly identify potential problems, provide recommendations on how to resolve existing issues, streamline automation with self-service and self-recovery capabilities and predict future outcomes to forecast costs and optimize return on assets.

Gartner has identified this trend and coined the term Artificial Intelligence for IT Operations (AIOps). Imagine a world where systems will provide us insight to questions we didn't think to ask—that's what AIOps has the potential to provide.

AIOps will greatly simplify IT by not only providing recommendations on how to resolve issues but also learning from past actions and solutions to predict failures and automate resolution. This requires visibility into the configuration state of machines as well as an understanding of past actions and interactions, the good and the bad. AIOps takes IT operations analytics (ITOA) to the next level by automatically applying insights to ensure high-performing IT environments are proactively making decisions that ultimately improve the health of the business.

DevOps is a must for the business: development velocity or bust

While the term DevOps may not yet be commonly spoken in the boardroom, it's key to building and maintaining a competitive advantage in today's highly complex and rapidly evolving environment. As every enterprise becomes a digital enterprise, businesses will sink or float based on the digital services they build and deliver. Competitiveness will depend on the speed of delivery, quality of customer experience and achievement of business goals from digital services. DevOps represents a way to not only deliver digital services faster, but also to do it more efficiently, and to better engage the engineering and operations talent of the team. To do so, organizations need flexibility to easily augment the skills, processes and technologies their teams use to build and deliver services.

To achieve the velocity, quality and business impact promised with DevOps, organizations will continue to adopt new staffing approaches and new technologies that empower teams and enable agility. From absorbing new organizational concepts like self-managing teams and loosely coupled toolchains to new technologies like containers, microservices, "Function-as-a-Service" solutions and software built with low code/no code approaches, organizations will experience constant change. Thus, DevOps means not only connecting disparate teams with a collective understanding of the quality and performance of the services in production, but also, the quality and performance of the processes that go into developing, building and releasing software.

Having a handle on DevOps initiatives will be a differentiator for executives. As board-level conversations center around speed and competitiveness, being able to point to successful implementations of DevOps initiatives and having data to demonstrate their impact will be key.

DevSecOps—the next frontier

To meet increasing expectations for governance, and audit and compliance requirements, all while maintaining development velocity, many teams will embrace DevSecOps. Just as IT organizations are performing a "shift left" to build more monitoring capability into their delivery platforms and applications, they will "shift left" with their security requirements as well. This means developers will have a larger role (and more accountability) for ensuring the security of their applications and the data they process. Likewise, security teams will need to collaborate more with development and operations teams to secure applications and delivery processes.

To combat the growing sophistication of digital adversaries, organizations must foster better collaboration between previously distinct IT and security organizations to a) elevate the operational security strategy to achieve business outcomes and b) drive operational protection, detection and response to reduce IT risk and cybersecurity threats and fraud.

Security will become a standard requirement for building enterprise-class services and applications. Beyond having developers, release managers and application specialists involved, operations and security teams will need to be folded into the mix, and DevOps teams will be required to ensure governance and audit controls throughout the application delivery toolchain more frequently. To enable this increasingly collaborative approach, everyone involved will need to work with a single source of truth—using that data to achieve the security objectives most relevant for their roles.

No more boundaries—transparency between companies

With new "composable" approaches to delivering business services including SaaS, containerization and APIs, traditional concepts around how a company delivers and operates applications no longer apply. To thrive in today's competitive environment, organizations must collaborate with third parties to enable development velocity and provide service reliability. Organizations will be built on a composite of these other companies, depending on them for anything from outsourcing development to relying on a cloud or service provider. This requires IT operations to gain visibility into myriad internal and external services, while providing greater transparency through operational information shared both inside and outside the firewall.

APIs will enable this required transparency and help form the basis of ecosystems that span customers, suppliers, employees and the enterprise. This will open up new capabilities in enterprise applications to enable more rapid service experimentation and development, but it will also increase the need for security and insight into how applications perform in production.

A new breed of IT Ops

With the rise of continuous delivery and DevOps, a new breed of IT operations professionals is defining how services are delivered and managed. As comfortable with Python and Ruby as with configuration and capacity, they are leading the way in areas like systems automation, architectural flexibility, developer empowerment and site reliability to deliver better applications faster and with an exceptional user experience. As such, the Site Reliability Engineer (SRE) role will become mainstream as many professionals refresh their software development skillsets so they can collaborate more effectively with developers.

SECURITY

by Haiyan Song

Hackers will exploit broader entry points

In the coming year, we will see the attack surface growing and evolving as technologies such as mobile communication, cloud computing, IoT and transportation continue to evolve with the digital transformation. In a connected world, there are potential entry points for hackers everywhere—from employees' smartphones to the increasingly automated fleet vehicles.

Attack capabilities have already evolved beyond traditional preventative and detection boundaries, regions and industries. And they are showing no signs of slowing down as hackers are looking to further exploit an attack surface that is becoming more horizontal. The major data breaches of 2017 are providing fertile grounds for new waves of phishing, identity theft and fraud. Attack vectors will continue to grow and shift across the technology stack. And defending this new frontier will continue to become more challenging as perimeters are disappearing and boundaries are always changing.

Automation will help alleviate mundane security tasks and help close the skills gap

The security skills gap is widening every year, with no signs of slowing down, with ISACA estimating a global shortage of two million cybersecurity professionals by 2019. To combat the skills gap and assist in the growing adoption of advanced analytics, automation will become an even higher priority for CISOs. Automating repetitive manual tasks, where there is high confidence in the outcome, is often the first consideration. As automation continues to increase within the security operations center (SOC), tier 1 analysts will remove themselves from 101 security processes, moving beyond "red light/green light" alerts so they can better focus on proactive security strategy. In turn, this will help close the skills gap and enable security analysts to do more with less.

Weaponizing machine learning in cybersecurity: The race is on

While the concept of bringing AI to solve cybersecurity challenges is not entirely new, it's still in its infancy and not core or mainstream in most environments. We see AI's applicability broadening in 2018. With this expansion of ML and AI for cybersecurity defenders, it should not be forgotten that actors on the attacker side have the same access to these technology advancements, and are collaborating and sharing to innovate faster. They can leverage ML and AI to speed up discovery of vulnerabilities, improve precision of attacks, morph the route and path to breach and avoid detection through counter-ML measures. Data and ML algorithms are emerging as a new battleground where the winning strategy relies on having the best formula to fuse human intelligence, machine learning and data.

Get data privacy right or pay the price

How does 20 million euros and a bad reputation handling personal data sound as the entry-level price for a breach? The new European Union data privacy regulation, known as the General Data Protection Regulation (GDPR), will be a catalyst to help companies rethink privacy and security control, and change the way they do business and protect their digital assets.

Organizations that operate in the European market will be potential targets for authorities trying to set a benchmark and put global companies on notice that they need to comply with the GDPR or pay the price. Companies will be subject to serious fines because they couldn't answer the required questions after being breached or they failed the privacy audit required under the GDPR. Many organizations will have to double down on their spending for cybersecurity and data privacy capabilities, especially for their European subsidiaries after being fined for the first time.

Security will move beyond the SOC and become a business enabler

Digitization is impacting every aspect of our lives. But it also amplifies the inherent risks and potential vulnerabilities in the ever-more-connected world in which we live.

New technology can make the mission of protecting enterprises even more challenging. Digitization is driving CISOs to rapidly transform their security operations at a scale that was previously unimaginable. This is accelerating due to the convergence of cybersecurity and business risk management and the convergence of operational technology (OT) security and information technology (IT) security. The shift from perimeter-based security to safeguarding and leveraging data from across systems, devices and cloud will provide unified visibility and holistic security risk assessment to the board, giving the CISO a more important seat at the executive table. It will enable businesses to leverage their data in ways they didn't know were possible. These security insights and capabilities will provide confidence and enable companies to solve business-critical issues, improve the customer experience and even create new revenue streams.

IoT

by Erick Dean

IoT's all about the data

When it comes to IoT data, one thing is certain: analyzing it continues to accelerate as companies get better results by including sensor based/IoT device data in their decision-making process—and there is no slowing down in sight. We see this in particular on the IT side—as IT spending increases, so will the investment in IoT. Organizations will build on hardware and connectivity layers supporting IoT as well as the services and analytics software to integrate IT, security, transactional and IoT data.

And this makes sense—for organizations looking to expand their existing data footprint, IoT is the logical next step. Companies that are successfully integrating their IT, operations and transactional data are now looking to ingest and correlate IoT data into existing infrastructure.

The risk is real

On the security side, IoT brings a tangible risk. As we continue to entrench our daily lives with more "connected things," we drive new levels of innovation and, at the same time, open ourselves up to a security minefield. In 2018, security for IoT will be under heavy scrutiny. Cybersecurity risk will increase exponentially as people, processes and businesses continue to connect every part of our daily lives and our economy. Each "connected thing" opens new doors into personal intelligence, corporate intelligence and public safety. Through these doors we open ourselves up—as individuals and organizations—to new weaknesses hackers could exploit. We are looking into a future where attacks can be orchestrated not just from public networks but from private devices such as a smartphone or a smart home. So, while the IoT revolution is exciting, in 2018 consumers and businesses will have to begin thinking of the tradeoffs. This will be particularly relevant to businesses where a breach will lead to a potentially fatal loss of consumer trust. Gartner predicts that, by 2020, more than 25 percent of identified attacks in enterprises will involve IoT, although IoT will account for less than 10 percent of IT security budgets. This gives businesses something to think about.

Place your bets—which industry will be the major adopter first?

The most value from IoT will come from solving complex logistics, manufacturing and public-sector problems. That means there are some industries that will see tangible benefits faster than others:

- **Public Sector**—with increasing connectivity between people, data and things—will begin embracing smart cities, where sensors and automation enhance the reliability of services, especially in the areas of safety and environment. IoT sensor data enables use cases including improved air quality, optimized traffic patterns, reduced safety incidents, traffic fire incident prediction and improved citizen identity.
- **Manufacturing** will continue to hold its position as the leading IoT industry, with predictive maintenance use cases driving the transformation. Organizations will continue to invest in improving operations and driving predictability in equipment downtime.
- The **transportation industry,** airlines and airports in particular, will push boundaries in adopting IoT data. This industry will innovate using real-time airport, aircraft, weather-sensor and passenger information to improve operations and deliver better customer experiences.

Cloud and digital transformation: the great enablers

Cloud spending enables new flexible business models that make it easier for small and medium businesses to adopt IoT. For larger organizations, cloud investments orchestrate global-data integration. AWS IoT, for example, serves as a central platform for devices, assets and sensors wherever they happen to be located. When you couple this with security and data ingestion, the cloud makes IoT successful.

Digital transformation initiatives—especially those centered around customer experience—will drive IoT expansion velocity. Building a technology infrastructure is relatively easy. The challenge is operationalizing data-driven decision-making that impacts the health of the business. Traditionally companies have invested heavily in the infrastructure, and then in solving for IT and security data-driven use cases. Organizations that are only beginning to integrate IoT data will begin asking these questions: How do I innovate; how do I drive revenue and better customer experiences with the new information I have available?

Machine learning and artificial intelligence

Machine learning and artificial intelligence represent a tremendous opportunity to IoT. The increasing commoditization and scale of sensor devices will drive a new wave of smart industries and have significant impacts on existing ones. Being able to predict when machinery will need to be repaired, self-optimizing production, and demand response are only a few application examples.

With existing network infrastructure likely to be used for "connected things," the investment spend on analytics technology will be higher as companies find new ways to make sense of the vast amounts of smart device-generated data. Industrial asset management, fleet management in transportation, inventory management and government security will be the hottest areas for IoT growth in 2018.

But does the IoT hype continue?

Short answer...yes.

Now you know what our experts think will happen in 2018. Only time will tell whether these predictions come true. We can't wait to find out!

We know you'll want to hear more from these writers. Keep up with these industry-leading subject matter experts by following our blog.

Visit us online to find out more about Splunk solutions for artificial intelligence and machine learning, IT operations, security and IoT.

About Us:

Splunk Inc. turns machine data into answers. Organizations use market-leading Splunk solutions with machine learning to solve their toughest IT, Internet of Things and security challenges. Join millions of passionate users and discover your "aha" moment with Splunk today.