splunk>

SPLUNK 2019 PREDICTIONS

splunk>

WHAT THE FUTURE HOLDS: TOP PREDICTIONS IN AI, SECURITY, IT OPS AND IOT FOR 2019

"The future is already here — it's just not evenly distributed." *—William Gibson*

We're always at the cusp of the next big thing, moments away from the next technological change that will affect us whether at work or at home — sometimes it just hasn't reached us yet.

At Splunk, we're working on shaping the future. Our experts are embracing new developments, focusing on the future of artificial intelligence (AI) and machine learning (ML), IT operations, security and IoT.

Pulling together insights from our thousands of customers and our dedicated research teams, our experts have assembled a shortlist of the top predictions for 2019.

Get a full grasp of what's to come for:

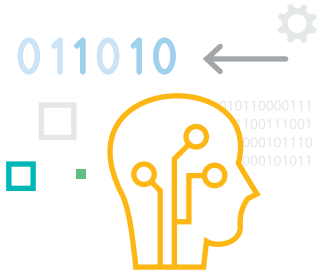
Artificial Intelligence and Machine Learning as it breaks out of the lab

Security in the wake of heightened compliance regulations and evolving digital environments

IT Operations as it transforms to focus on application mobility

IoT as it claims its stake in the modern organization

AI AND MACHINE LEARNING



Adoption will evolve from "let's check this out" to "let's roll this out"

For artificial intelligence and machine learning, the era of expansive hype and limited substance is swiftly coming to a close. Organizations big and small have progressed from researching AI and ML's potential to purchasing and deploying the technologies — confident that these investments will deliver substantive benefits.

Venture capital investment in AI now tops $3 billion annually, and the number of active startups in the U.S. that are developing AI technologies has gone up by a factor of 14 since 2000. Despite this momentum, the industry is still in the early days of delivering enterprise-relevant AI- and ML-backed solutions that are manageable and provide high ROI. Early adopters, however, are already achieving significant benefits. Deloitte surveyed 250 early adopters of AI and found that 83 percent said they "have already achieved either moderate or substantial benefits from their work with these technologies" across a wide spectrum of business activities. And 76 percent of those early adopters say cognitive technologies will transform their business in three years or less while only seven percent gave a timeline for transformation beyond five years.

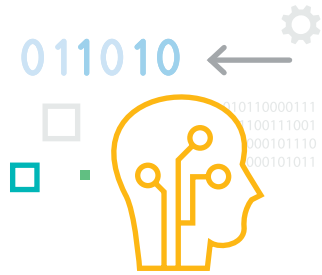
From fraud detection to IT optimization, AI and ML are delivering on years of promise — and 2019 will see wider adoption as "early adoption" gives way to "table stakes."

Open source systems and communities will become integral in AI and ML development

As AI- and ML-powered tools take center stage, they'll require a supporting cast of tools and communities. Larger volumes of data and projects focusing on building out AI- and ML-backed tools are essential. Open-source systems and communities create a haven for those willing to explore — and they open doors to affordable, accessible means of processing large data sets, usually via the cloud.

Forward-leaning organizations are already augmenting home-grown capabilities with open source software (OSS) systems and communities. TensorFlow and other OSS systems are useful for large-scale machine learning processes and deep insights (i.e., distinguishing spoken words from gibberish, or translating a word from one language to another). Other systems, such as Apache Spark, facilitate running repeat queries on data sets to sharpen and improve insights. OSS communities, such as GitHub, make it easier to share ideas and gain feedback across teams and organizations.

Expect this open collaboration to continue and pick up speed as organizations and researchers increasingly throw their hats into the AI ring. Working together toward widespread application of AI and ML is imperative if we want it to happen quickly and effectively. Doing the inverse will only stunt growth.



AI will create new ways of interacting with data (and machines)

Fear of AI and ML replacing workers abounds, but there's more to the narrative. The human in the loop (HITL) won't be eliminated; intuition, quality assurance and general training will remain vital to optimized AI and ML deployments. There are human tasks that technology can bolster but not quite replace.

HITL has emerged as a key design pattern for managing teams where people and machines collaborate. The goal is to manage the impact of AI and ML to be less jarring and more useful and accessible. It also allows AI to offload the edge cases it can't handle to humans the same way we offload monotonous tasks to machines.

So what is AI and ML taking out of the picture? Smart technology is taking on the complexity and load of tedious and data-heavy tasks so practitioners can focus on higher-order work. In the process, seen in the aggregate, jobs won't be eliminated, they will evolve. McKinsey suggests that by 2030, 375 million workers — 14 percent of the global workforce — will need to "switch occupational categories." Gartner predicts that AI will create 2.3 million jobs in 2020, while eliminating 1.8 million.

In the transition, effective AI and ML will require the development of new skills and the advent of new processes as humans take on the responsibility of overseer. The value of AI and ML will increase organically as this happens, as smart tools are fed more data and trained in new scenarios. The day-to-day consumer is already experiencing these organic AI benefits: Amazon continues to recommend great books; Siri conversations are becoming more natural; ESPN football predictions are increasingly accurate.

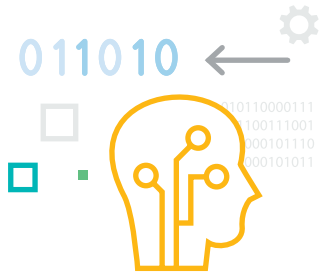
Additionally, engaging with most of these innovations will not, and cannot, require a doctorate degree in data science. There are not enough Ph.D.s available. Look for more intuitive interface options to emerge. From natural language search to prebuilt, point-and-click models, AI will no longer be the domain of the few. Expect more substantive and tangible results across an ever-expanding set of scenarios as a result — from spot-on sales forecasting, to accurate weather and traffic projections, to precise anomaly detection and automated remediation.

AI and ML will take off in healthcare and finance

Smart technology is now being launched and trained in specific business settings, and we can expect more of it in highly regulated industries.

In financial services:

- Unsupervised machine learning techniques will increasingly help banks and insurers segment their customers and offer personalized, targeted products. This technology will also improve speed and agility, helping organizations compete with specialized fintech firms through enhanced customer intelligence.
- Machine learning will boost regulatory compliance using automated reports, stress-testing solutions, and behavioral analysis of e-mails and phone records to identify



suspicious customer or employee behavior. It will also enhance fraud detection, improve anti-money laundering efforts and more effectively detect credit risk.

- Finally, by analyzing the constant data being generated by consumers with machine learning, financial services companies will be able to automate back-office operations, reduce errors and accelerate process execution in the year to come. This will allow insurers to improve and automate the handling of claims by recognizing patterns in pictures or individuals involved in damages, for example.

In healthcare:

- We know that the volume, variety and velocity of data have exploded in the healthcare industry in the past few years due to electronic health record (EHR) adoption. In parallel, that wealth of data brings opportunities to better predict and manage medical conditions. Already, the first AI-powered diagnosis of images was approved by the FDA in April. Many businesses have been working on continuing this trend. Expect even more precise results and recommendations, like tailored treatments, to become more accessible as researchers and physicians increasingly come to use AI and ML in their diagnostics processes.
- The natural progression of AI and ML adoption in the space means AI will affect a majority of U.S. patients — and most patients won't even know it. For example, U.S. patients will be unknowingly affected by the discreet AI solutions that their providers use for clinical decision support, by payers to predict their risk of hospitalization or by pharmaceutical companies using chatbots for managing patient engagement.

SECURITY

Interconnection will bring disconnection and risk

Despite the best of intentions, increasing interconnection among services and devices will open new vulnerabilities, widen the attack surface and create unforeseen challenges. Security is reaching an impasse as organizations look to both improve interoperability and efficiency and maintain enough segmentation for a strong security posture.

What does this mean for the year to come? The attack surface will keep increasing. In 2019, multi-cloud deployments instigated by the need to simplify workflows and augment cloud benefits will break down more walls between datasets and workflows. DevOps adoption will also increase the collaboration of once-siloed functions for greater digital and offline collaboration. APIs will continue to bring technologies together, looking to increase the productivity of users and yield greater benefits.

These collaborative technologies and methodologies will bring with them a host of problems, including disruption of services and server downtime. And while the benefits of interconnection far outweigh the pitfalls, organizations will need to proceed with caution to avoid falling victim to nefarious actors.

The rise of the virtual analyst

Security teams are greatly understaffed and overworked — and it's not about to change anytime soon. Experienced security talent is not only hard to come by, but the sheer volume of alerts, events and incidents make it nearly impossible for any organization to be sufficiently staffed on the security side. That is, of course, until the rise of the "virtual" analyst.

Big data platforms, machine learning-based analytics, and orchestration and automation technologies will augment once-understaffed security teams. We're just around the corner from virtual analysts that can help scale existing resources so that security pros can focus on more critical — and less tedious — tasks. It's already happening to an extent with simple automation for alerts and responses. But it's going to progress even faster as new machine learning techniques, like unsupervised machine learning, are able to generate their own (and accurate) patterns of risk with minimal to no human intervention.

This will allow security teams to operate at machine speed, from detection all the way to response, accelerating previously manual security workflows and increasing precision in repetitive tasks that are prone to human error. Processes will also start running autonomously, at all times of day, ensuring the most secure environment even when human handlers are not around.

New trends and technology will mean new roles and opportunities

Security analysts, fear not: The rise of the virtual analyst does not mean the replacement of the real human analyst. In fact, new AI-driven technologies will create new roles and opportunities for security professionals. From security content developers to automation engineers, these new roles will focus

on optimizing the security workflow and its tools, whether through more accurate and insightful custom dashboards and algorithms, or through playbooks that suit specific response scenarios and streamline new tools and their processes.

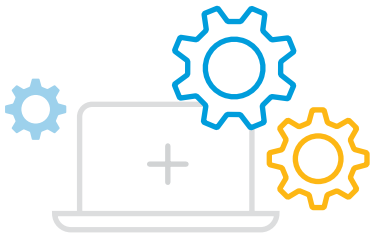
Enforcement will make compliance an even greater priority

The deadline to comply with the E.U. General Data Protection Regulation (GDPR) in May 2018 came and went with far less uproar and enforcement than originally expected. But this may simply be the quiet before the storm. GDPR turns one in 2019, with the expectation that organizations doing business in Europe will have adopted compliant practices.

We anticipate greater enforcement of the regulation in 2019, where larger fines and negative publicity will drive CISOs at noncompliant organizations (to say nothing of the full C-suite and board) to truly prioritize compliance. Organizations will invest in technologies and processes that set them up for better breach detection and response, as well as capabilities that make it simple to prove that their data is safe and the technology processing it is securely deployed and compliant. No one wants to pay the high cost that comes with the breach of compliance regulations.

Further, enforcement of GDPR may trigger a domino effect, leading regulators of data privacy regimes such as HIPAA and PCI-DSS to level up their enforcement game, making compliance an even greater driver of security processes and investments in 2019. It will likely trigger similar laws and regulations in other regions, putting more pressure on organizations.

IT OPERATIONS



Multi-cloud deployments will march forward in the enterprise

Multi-cloud deployments will become a must, especially among large organizations. But managing and measuring performance across a multi-cloud infrastructure presents challenges, which will drive more AI and ML adoption.

As their footprints in scale of operations grow larger, organizations will require more flexibility from the services they employ. Shifting workloads between cloud deployments (sometimes hosted by different providers) has become key for accessibility and cost efficiency. And there is plenty to say about disaster recovery and the benefit that comes from not having all your eggs in one basket. Not to mention, bigger enterprise players can't avoid the reality of multi-cloud when thinking about different business units or the infrastructure maturity across them. It's not uncommon for workloads to be housed with different providers.

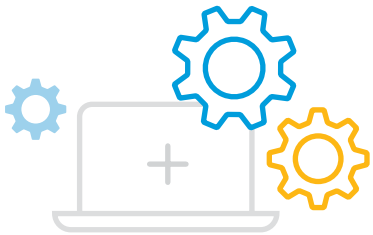
But a multi-cloud deployment is no easy feat — especially for those just getting into the cloud. Abstracting a management layer above cloud deployments puts a greater burden on operations teams. There is also the question of security and compliance.

In this environment, it will be paramount for an organization to know what's happening from a performance, availability and observability angle across all the providers while being able to correlate it across the stack. From a data perspective, this will mean having a way to unify meaningful insights from across a variety of data types and sources. AI-powered solutions that can identify patterns from any data source to reveal issues, dynamically help manage capacity and predict possible issues will be key in this journey.

Need for mobility will increase container use in production

Container adoption will increase as application mobility across environments becomes a must, though data management costs may still be a limiter. Containerized workloads allow developers to work in different environments without too much upfront building and cost (apart from some GPU dependencies and the like). Additionally, containers lend themselves to continuous integration/continuous deployment (CI/CD), making it easier to build code into shared repositories that can be leveraged for fast application deployments across environments.

The rise in container use couldn't come at a better time, as deployments demand ever-increasing speed, flexibility and quality. Insatiable customer hunger for new features and enhancements demands a quick dev cycle, and containers are a great way to help keep up. By abstracting applications from the deployment environment, teams can deploy applications more consistently, regardless of environment. Not only is the application isolation valuable, the lightweight nature of containers also makes deployment easier, creating less overhead. It allows developers to focus on application logic and ITOps to focus on deployment. This becomes highly valuable as you think about multi-cloud environments.



While this flexibility is great, there are a few challenges. How do you monitor things that are ephemeral? Teams will need a way to extract the relevant information in an equally dynamic way to be able to achieve observability, ensuring performance and availability. Given the on-demand nature of these applications, having the right data and AI/ML-backed tool will be key in achieving the level of observability required.

There's also a cost with the ability to manage the data that those applications are accessing. As applications spin up and spin down, IT has to keep track of what data is being used and/or needs to be available. This will also require smarter technology to achieve.

IT teams and roles will evolve quickly

The IT department must continue to evolve from building and managing infrastructure/apps to largely acquiring and managing external applications and services. Expect a tremendous increase in product managers in IT organizations as a result. Additionally, to keep up with rapid innovations in the space, businesses will need to adapt their cultures to be more flexible to accommodate and take advantage of the changes — both in roles and technology adoption.

There will be considerable need for solutions that promote collaboration and communication. Collaboration and communication is key between developers and ITOps (even security), especially when thinking about DevOps and DevSecOps. This transparency will also have to encompass increasing adoption of third-party vendors environments such as public clouds.

On the technology end, vendors of AI- and ML-backed solutions that let users leverage their data without being data scientists will win big. IT pros need to cut through the noise to better strategize, so they'll embrace tools that provide observability and flexibility at machine speed.

IoT

IoT and ML will combine to dominate businesses

The buzz around the Internet of Things (IoT) has been constant, but the spotlight has been focused on the consumer end for too long. This is changing in 2019.

Today, IoT provides a competitive edge to a subset of businesses. Expect that group to grow in the coming year as more businesses realize the value of sensor data. In a data-driven age, any new data dimension added to existing IT and security information can improve business outcomes and security. The integration of IoT and ML technologies with products and services will deliver value. As such, organizations will invest in corporate-wide initiatives to monitor and harness data like never before — deploying security protocols, live dashboards, anomaly detection, process automation, relevant generation of key performance indicators and hundreds other features.

Globally, IoT will continue to draw considerable attention — and investment — in the year to come. Expect a focus on cloud services and APIs that enable the rapid proliferation of new applications and data-gathering methodologies. Edge computing and massive-scale analytics will quickly evolve to become key to this effort, enabling organizations to better manage IoT and address the associated security risks.

Discrete manufacturing, transportation and logistics will remain at the forefront in the adoption of IoT to address their biggest challenges around OT (Operational Technology). But expect a similar trend to span into other industries as well.

The CIO will bridge the divide between IT and OT

The convergence of IT, operational technology (OT) and IoT is real, and is changing the scope of the CIO's office. In 2019, for heavy industrial companies, CIOs will drive OT transformation because of the technology's critical role.

For years, IT and OT have lived separate lives, with OT dominating manufacturing and transportation. But that is about to change. You can no longer have IT without OT if you want to compete. For instance, data coming from sensors and OT devices on the factory floor can be a boon to IT operations as the optimize workloads and bolster security. OT now has a seat at the table — a legitimate stakeholder, especially in industrial settings.

The CIO will have to step up and become buyers and architects of new uses of OT technology in their environments.

IoT security becomes very real

While OT and IT convergence is enabling new business models, it introduces significant new risks, for which many organizations are unprepared. As healthcare, transportation and process control industries devise their plans for the future and incorporate IoT transformation, organizations will have to make a concerted effort to ensure that data from every device and every machine is secure regardless of environment or state.

For processes spanning plant floor logistics to product quality, organizations will look to improve their security posture with proactive analytics and advanced investigation. To incorporate these rapid innovations while keeping operations secure, businesses will have to become more flexible.

Notably, the uniqueness of OT will require organizations to focus on standards most critical to protecting their assets and SCADA/ICS systems while investing in IoT-specific security expertise in-house. Like IT, this will require collaboration and communication that creates transparency between typically disjointed parts of an organization.

splunk>

CONCLUSION

Now that you know what we see coming down the pipeline for 2019, make sure you join us in shaping the future.

Follow our blog to stay in the loop and find out about the latest developments as they happen.

Visit us online to find out more about Splunk solutions for AI and machine learning, ITOps, security and IoT.

About Us:

Splunk Inc. helps organizations ask questions, get answers, take actions and achieve business outcomes from their data. Organizations use market-leading Splunk solutions with machine learning to monitor, investigate and act on all forms of business, IT, security and Internet of Things data. Join millions of passionate users and try Splunk for free today.