Splunk **Predictions 2020**

5G, AI, deepfakes and beyond: The future of IT and security

splunk> turn data into doing™

Contents

2020 and Beyond:
Emerging Possibilities, Emerging Threats

Algorithms may decide who gets a job interview. Automation could kill your org culture, or it can unlock human creativity. Security strategies that can spot last year's "imprtnant e-mail" from your CEO are not ready for next year's deepfake phone call.

These are just a few of the issues that will drive technology conversations in 2020, and every one of them revolves around data.

Organizations and individual consumers are facing a new wave of technologies that will generate, and allow us to manipulate, untold new quantities of data. This year, leaders and technologists at Splunk pooled their insights to discuss how this avalanche of data will manifest, and how alert organizations can stay one step ahead.

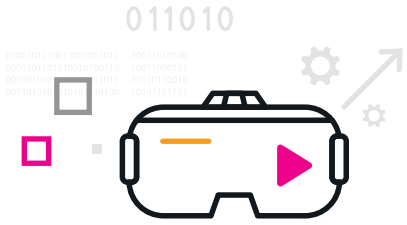
This report explores three areas: IT operations, IT security, and emerging technologies. We look at the near-term synergy of IoT and 5G technologies, and the long-term impact of ignoring user experience. And because leading companies will drive every decision with hard data, we look at the cost of leaving so much of your data in the dark.

From AI advances to automation strategies to the new default security framework, organizations that show foresight in 2020 will be best positioned to turn challenge into opportunity.

Here's what's coming:

Emerging Technologies

What the future holds for AI, IoT, blockchain and more in a world in which everything is truly connected.



The next decade will bring many global changes. Markets are shifting focus as technology and the data it produces continue to take over all industries — remaining analog isn't even a consideration anymore. But how we're transitioning into the latest evolution of the digital frontier is still being worked out.

Emerging technologies are being used, often experimentally, in a variety of ways. Artificial intelligence (AI) and machine learning (ML) are being applied to everything from IT to industrial operations. Virtual reality and augmented reality are breaking out of niche gaming uses into healthcare and manufacturing. Natural language processing (NLP) is going beyond smart assistants. Similarly, blockchain is now coming into its own, beyond cryptocurrency. And IoT and 5G are coming together to enable a lot of the above and much more.

We're at an inflection point that will manifest in transformative changes to how we work and live, driven by data technologies.

Natural Language Processing

Machines will have a bigger voice in our lives

Our jobs, financial markets and more will be affected by machines that read.

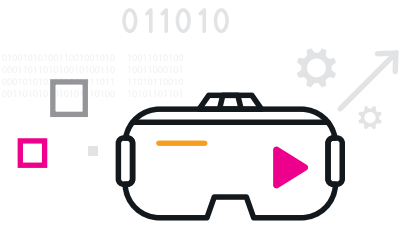
Natural language processing makes communication between human and machine easier than ever. Not only does NLP let us speak to our smart devices and get uncanny human-like responses — beyond trading jokes with Alexa and Siri, NLP today helps people with disabilities communicate, translates languages on the fly, parses through tons of unstructured data (in the form of the written word) for previously unnoticed insights, and more.

But are you ready for it to decide whether you get your next job? Beyond parsing resumes for keywords, NLP is being used to judge video of job applicants, with consumer goods giant Unilever saying it delivers six-figure savings annually. And AI is already grading college entrance exams (with mixed results). In the next five years, look for NLP to routinely assess creditworthiness, even without financial data. One company has potential borrowers download its app so that it can assess their entire "digital footprint" as a means of deciding whether you'd repay a loan on time.

At the business level, AI will increasingly make decisions that may be inscrutable to human observers, whether by analyzing stock data to make investment decisions, or parsing mountains of unstructured social media for broad sentiment analysis around a brand, or specific intelligence on whom to target for which product pitch.

But relying too heavily on technology in important decision-making is misguided. A Motherboard investigation points out: "[R]esearch from psychometricians — professionals who study testing — and AI experts, as well as documents obtained by Motherboard, show that these tools are susceptible to a flaw that has repeatedly sprung up in the AI world: bias against certain demographic groups. And as a Motherboard experiment demonstrated, some of the systems can be fooled by nonsense essays with sophisticated vocabulary."

The implications could be even worse than faulty grading. When artificial intelligence was used in criminal justice, computer algorithms that influenced sentencing decisions and defendants' freedom in general were twice as likely to wrongly flag black defendants as future criminals as they were to inaccurately label white defendants.



"Training is everything," says Eric Sammer, distinguished engineer at Splunk. "A lot of these algorithms are being trained on existing human practices that are inherently biased and problematic. It'd be naive to assume we can eliminate that from NLP algorithms at the outset."

NLP should never be seen as the final decision maker, but it can and should help humans make better decisions. Augmenting human capacity, with strong attention to ethical considerations, will be the right approach for this developing technology.

AI/ML

Attackers will attack AI while it's still learning

As we empower our algorithms, the first "poisoned well" incident will shake our faith.

As artificial intelligence and machine learning drive more of our decisions, bad actors will focus on it as a new attack vector — sabotaging training data to disrupt decision-making.

We often don't think about how the algorithms around us are generating their insights or making their decisions. Today it's Amazon recommending an author we've never heard of, and tomorrow we'll doze while our cars self-navigate through rush-hour traffic — a level of technological sophistication long the stuff of fiction. But we can't just doze; we have to keep our eyes on how we train smart technology.

Algorithms learn from data. The algorithm will use a training dataset to identify patterns or predict outcomes. Sometimes it's trained with examples of target outcomes, and sometimes it's just directed to find patterns, without a desired result. This training process could present an enticing attack vector for motivated and sophisticated attackers as smart technology becomes further ingrained in our daily lives and infrastructure. By manipulating data, someone could throw off or break down entire learning models, hijacking them or rendering them useless.

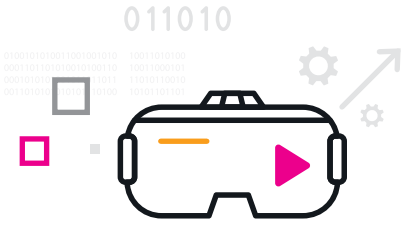
We've seen this already. Adversarial machine learning, the technique employed to fool models through malicious input, has tricked Google's AI into thinking a turtle was a rifle. That's funny, at least outside a security checkpoint. But imagine manipulating traffic signals so that smart vehicles don't realize they have to stop.

"Adversarial attacks have proven capable of tricking a machine learning model into incorrectly labelling a traffic stop sign as a speed sign, which could have disastrous effects in the real world," Richard Nock, a machine learning expert with the Australian government, told ZDNet in June.

Expect also to see attempts to poison the algorithm with specious data samples specifically designed to throw off the learning process of a machine learning algorithm. It's not just about duping smart technology, but making it so that the algorithm appears to work fine — while producing the wrong results.

"As we increasingly depend on smart technology, the door for sabotage keeps opening wider and wider," says Eric Sammer, distinguished engineer at Splunk. "The training needed to teach smart algorithms will be the perfect place for bad actors to take action against them. Data integrity has never been more important."

In 2020, we'll see more attempts at adversarial attacks that could lead to disastrous results. It could lead to industrial sabotage — think power stations or water treatment plants that depend on automated



processes. It could affect the financial stability of organizations and individuals. In this changing landscape humans will have to verify outputs and not take for granted what AI/ML provides us.

If history is any lesson, we know that if the opportunity presents itself, someone will take it, even if it's "for the lulz." Remember the chatbot gleefully taught to be racist by random social media users?

Blockchain

Blockchain leaves Bitcoin behind

A new data era pushes us toward a blockchain infrastructure.

In the next five years, blockchain will finally evolve beyond cryptocurrency to change security, industrial environments, even governance.

The value of blockchain is often conflated with the public understanding of Bitcoin. Although Bitcoin was the first instantiation of blockchain (and usually dominates news cycles around blockchain), digital ledger technology itself has far-reaching uses and implications — from securing assets to maintaining data integrity.

When data is committed onto a blockchain, it's permanent and nearly impossible to manipulate or hack because it depends not on people, but on the network of machines it's built upon. Businesses that adopt blockchain can operate more leanly and efficiently, with greater trust in their data, because every change in the network is recorded and validated on a block in the blockchain. As such, organizations are looking to use the technology for a wide range of problems, including quality assurance, accounting, contract management, supply chain management, data protection and much more.

"Blockchain truly is a mechanism to bring everyone to the highest degree of accountability," as futurist Ian Khan put it. "No more missed transactions, human or machine errors, or even an exchange that was not done with the consent of the parties involved."

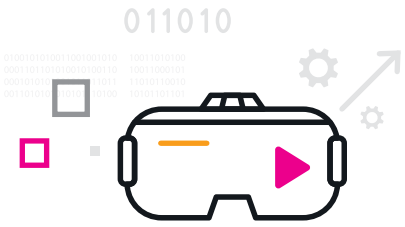
So how will we see blockchain used in the year to come?

Not surprisingly, finance is leading the charge on blockchain adoption. The financial sector has already started using blockchain — some testing it for cross-border remittances. Union Bank of the Philippines is making it easier for overseas Filipinos to send money back home. Blockchain also serves as a record of financial status for those receiving these funds — which normally fall outside the purview of traditional financial institutions.

But it doesn't stop there. It's also changing the construction industry. "Blockchain provides a platform for clearly cascading work products down the chain and holding everyone accountable for completing key tasks," according to Propulsion Consulting founder Marc Minnee. This is key, considering that 95% of building construction data gets lost on handover to the first owner.

What may be most interesting is that government bodies are not far behind. Estonia has gone all in on being a digital society. From filing taxes to purchasing vehicles, it can all be done digitally. The security underpinning the integrity of the system? Blockchain. Dubai is another place betting big on blockchain, aiming to become the first blockchain-powered government.

"Blockchain is one of the most promising technologies to appear on the world stage in recent years," says Aisha Bint Butti Bin Bishr, director general of the



Smart Dubai Office, noting that Dubai's interest has included "launching a blockchain strategy and hosting international blockchain conferences that bring together influential international experts."

In the next year, expect Dubai and others to keep moving forward. Soon visa applications, bill payments, license renewals and more, will take place digitally using blockchain. And as governments and regions, like the United States, China and the European Union, continue to become more involved, it is likely to take an even more central role in terms of identity. Voting, government benefits and other systems may hinge on the security offered by blockchains.

Blockchain will also be big for the Internet of Things: The blockchain IoT market is expected to be worth more than $3 billion by 2024. Blockchain will let smart devices conduct automated microtransactions more quickly and cheaply — and more securely. Though the market will continue to grow in 2020, regulatory uncertainty will be a short-term drag.

"Blockchain will revolutionize how we leverage technology, on a par with the effects of mobile technology and the Internet itself," said Nate McKervey, head of blockchain at Splunk. "We're just starting, but once blockchain becomes well-organized in financial settings, the industrial and public sector applications will skyrocket."

IoT/5G

5G's IoT push previews the post-smartphone era

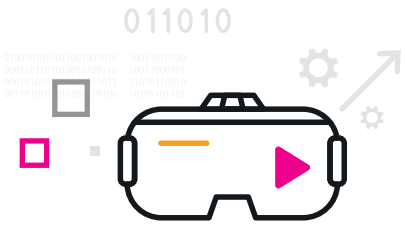
5G's impact will first be felt through the Internet of Things.

Already available in some cities, 5G is setting new standards for speed and bandwidth. Imagine downloading a movie in seconds — on your phone.

But 5G will bring more than super-fast phones. It will expand to encompass all sorts of "things," from autonomous cars to augmented reality glasses, as 5G's greater capacity and reduced latency enable a seamless, more efficient end-user experience. In 5G's wake, the IoT era will truly come into its own, having as big an impact on the daily world as the smartphone has in the 4G era.

Healthcare will be transformed by 5G. Machine-type communications will be used to monitor patients via massive sensor networks, to power smart pills that can record drug ingestion, and to monitor care for insurers. Ultra-reliable low latency communications (URLLC) will power telemedicine, remote recovery, augmented reality physical therapy and even remote surgery. The world's first 5G remote operation occurred when a surgeon in China used 5G technology to operate from 30 miles away on a laboratory test animal.

Remote surgery won't become widespread in 2020, but medical students are already practicing surgical operations on virtual models. Augmented reality and virtual reality will also be used for training in other fields, and will increasingly be used in shopping and retail, letting customers view properties and try on clothes virtually.



In 2020, 5G will take hold in the industrial space, providing more efficient services, better safety and new use cases. Low latency will improve remote control of heavy machinery, reducing risks and expanding the types of environments in which machinery can operate. In an early example, Ericsson's first 5G smart manufacturing factory in the United States will begin operations in early 2020 and feature automated assembly, packing and product handling. Estimates that 5G will enable $12.3 trillion of global economic output by 2035 expect manufacturing to account for more than $3.3 billion.

All the benefits won't come without some risk. IoT devices often lack solid security design, and there's an inherent risk in creating new, connected 5G networks that could expose sensitive information. Organizations will need to take a layered approach to security that covers these gaps. End-to-end security will be critical in protecting communication paths between devices, users and the core network. DNS intelligence will also be important.

Dark Data

2020 will be the year of dark data

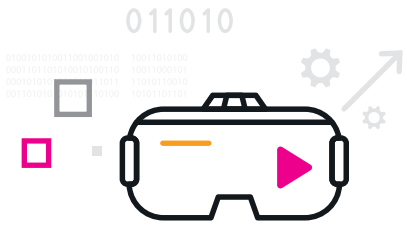
If you think you've joined the data revolution, you may only be half right.

With the advent of AI, augmented reality, 5G networks and other new, transformative technologies, organizations must prioritize bringing their data to bear. These technologies will drive leading companies to prioritize the proper management and use of all their data. Which brings up an essential problem — companies aren't doing a good job of that.

A 2019 dark data study commissioned by Splunk showed that 55% of an organization's total data is dark, meaning the organization either doesn't know the data exists or doesn't know how to find, analyze and use it. Various published estimates that try to calculate the value of dark data in a particular vertical (the travel industry, for instance, or marketing technology) put the figure in the billions of dollars. Not surprising, when you realize that learning how to use dark data would nearly double the amount of information for the average organization.

An interesting finding in Splunk's dark data report was that respondents in China, a hypercompetitive and fast-changing economy, were the only ones who voiced a strong understanding of dark data, and claimed to be ready to deal with it. The more data you have, and use, the more effective your organization; cutting-edge organizations already know this.

When you declare a year of something, you can't say that every single company will embrace the rallying cry. 2020 will not be every company's year



of dark data, but every company will need to have a year of dark data, and soon. If it's not 2020 or 2021, they'll be playing catchup in 2022 as competitors making better uses of data-fueled technologies find innovative ways to understand their customers and improve products and services.

Dawn of a connected decade

The next few years will bring massive steps toward a more fully connected and immersive world. With smarter algorithms, rampant connectivity and networked devices we'll be able to achieve feats ranging from remote surgery to digitally contextualized real-world experiences (i.e., imagine historical facts overlayed old buildings).

The new decade will be the one in which AI/ML, NLP, augmented reality, IoT and 5G mature and become both commonplace and transformative. There are still uncertainties, and the one that's most in your control is whether you and your organization will be ready.

IT Security

Deepfakes, infrastructure attacks and other crazy-scary things that will keep you up all decade.

"It does not do to leave a live dragon out of your calculations, if you live near him." — J. R. R. Tolkien

In cybersecurity, you'll inevitably meet a dragon. The question is: How will you defend yourself when that day comes?

Security professionals, from the tier 1 analyst to the chief information security officer (CISO), spend their days (and nights) watching for dragons and preparing for inevitable attacks. But the risks change all the time. We adopt new technologies that expand and change our attack surface. Hackers adopt new technologies and techniques to get past old defenses. Years of fine-tuning their attacks, growing their knowledge and succeeding without repercussion have only emboldened malicious actors to go bigger. It doesn't matter what the motive is — ransomware for money, nation-state sabotage or stealing specific information — the results are the same, and significantly damaging.

From highly sophisticated nation-state attacks to individual hackers whose weapons are charm and guile, here are the cybersecurity dynamics we're keeping our eye on in 2020.

Social Engineering

Deepfakes will uplevel the danger of social engineering

New ways to lie make it more imperative to instill a strong security culture.

If you thought social engineering was passé, here's a new word for you: Deepfakes.

But before we get to that new wrinkle, let's make sure you didn't think social engineering was passé simply because it has been a security challenge for decades.

Tricking humans, rather than hacking their technology, is a well-worn strategy, but it's in no way in decline. Verizon's 2019 Data Breach Investigations Report found that, between 2013 and 2019, the percentage of incidents using social engineering virtually doubled (from 17% to 35%), while hacking and malware incidents declined slightly.

In late 2018, EY reported that there were 6.4 billion fake emails sent every day, and 550 million emails had gone out in a single phishing campaign. Their survey found that security leaders in 34% of organizations identified "careless/unaware employees" as their single biggest vulnerability. (The firm also reported that nearly 1,500 government officials were using Password123 as their password in just one U.S. state, so … point made.)

It's popular because it's comparatively easy.

"(Social engineering) doesn't require technical knowledge of particular or specific systems, databases, zero-day exploits or other traditional, computer-based methods of fooling a target victim," says cybersecurity reporter Dan Patterson, a senior producer at CNET embedded at CBS News, who recently did a deep dive into the rise of social engineering.

The challenge for cybersecurity experts: How do you defend against a threat that isn't digital?

"Ironically, the Achilles' heel of IT security is the one thing that can never truly be eliminated: the human factor," says Keith Kops, Splunk's global head of security. "When employees click on a phishing email, open the door for a friendly stranger or leave their laptops unlocked while they take a quick restroom break, they're unwittingly inviting the threats inside."

Now let's talk about deepfakes, technologically altered audio or video that convincingly puts someone else's words in a person's mouth. Altered video made the news in 2019, first when a primitive alteration maligned U.S. House Speaker Nancy Pelosi, and then when researchers released a deepfake video that made Facebook CEO Mark Zuckerberg sound just a little megalomaniacal. Now imagine the CFO who's too clever to fall for an "urgent email" from her CEO when she picks up her phone and hears her CEO's voice ordering her to make some imprudent move.

Actually, there's no need to imagine it. *The Wall Street Journal* reports a CEO falling for a deepfake, to the tune of more than $240,000. According to *The Washington Post*, security firm Symantec says three companies have been swindled — in one case, of millions of dollars — by deepfakes of executive voices.

"This is a technology that would have sounded exotic in the extreme 10 years ago, now being well within the range of any lay criminal who's got creativity to spare," Andrew Grotto, a fellow at Stanford University's Cyber Policy Center, told the Post in that September story.

So to 1) the detectable rise in old-school social engineering and 2) there being no detectable confidence that organizations have successfully smartened up their employees to fend off ordinary phishing schemes, add 3) the rise of deepfake technology, which today can fake a voice, and may one day be able to fake video live (as this early experiment tests out).

"The bottom line is that when it comes to cybersecurity, the human element remains a major threat vector," says Haiyan Song, Splunk's senior vice president for security markets. "Attackers will evolve from targeted email schemes to using new tools like deepfake technology to continue what has always been the easiest way to circumvent security: people."

Organizations must continue to invest in the technology to close down software vulnerabilities and automate against incoming attacks, but not to the neglect of training and vigilance around simple human weakness. And whatever you're doing to teach employees to stop clicking on sketchy links, also build in a response to unexpected calls from apparent execs making strange demands.

In 2020, we expect social engineering's role in cyberattacks to continue to rise, with the advancement of technologies like deepfake and its potential impact on the masses, and we'd be very surprised if a deepfake attack doesn't make the headlines in this election year.

Critical Infrastructure

Cyber attacks will hit home (literally)

Hackers and nation-state attackers are targeting systems that run our day-to-day lives, and they're already succeeding. It'll only get worse in an election year.

Since 2017's WannaCry attack made ransomware a front-page headline, criminals have continued to strike, hitting Atlanta, Baltimore and other cities, as well as healthcare systems and state agencies, causing significant disruption and expense. Attacks on critical infrastructure, traced to both criminal organizations and nation-state actors, are becoming a part of municipal life. In 2016, San Francisco's Municipal Railway was attacked by hackers demanding 100 Bitcoins (then about $73,000), leaving the transportation system in a state of chaos. The attack compromised more than 2,000 servers — giving the hackers 30 gigs of Muni's internal data.

"Cyberattacks can destroy a transit agency's physical systems, render them inoperable, hand over control of those systems to an outside entity or jeopardize the privacy of employee or customer data," cautioned the American Public Transportation Association. Unsurprisingly, transit systems are an easy target thanks to outdated infrastructure, as well as lack of funding (and incentive) to invest in security upgrades.

And it doesn't end there. In 2018, the FBI warned that nation-state hackers were attacking sensitive U.S. infrastructure such as electrical systems, water processing plants, nuclear power plants and air facilities. In early 2019, an attack on a U.S. power grid created blind spots at a control center and several power generation sites, reported the North American Electric Reliability Corp. This was the first-ever recorded "disruptive cyber event" for the U.S. grid network.

Industry experts say these attacks are merely a harbinger of things to come.

The combination of for-profit cybercrime and political skullduggery, heading into a U.S. election year no less, present heightened risks. "There's persistent espionage, criminal activity and other 'hacking' to pre-position certain capabilities in case of war," says Tim Junio, CEO and co-founder of Expanse. Junio knows the area well. His cybersecurity startup was seeded by the Defense Advanced Research Projects Agency (DARPA) to prototype new large-scale data science and computer network operations technologies for the U.S. military.

And so, as cybercrime grows in volume and complexity, the question looms: What do we do? Strengthening our cyberdefenses across public and government services has become increasingly critical. A haphazard approach to security, in which tools and systems are piecemealed together — in addition to antiquated, legacy systems across healthcare, education, energy and countless other sectors — weaken cybersecurity in the increasingly connected and digitized world, resulting in asymmetric cyber attacks on our everyday lives.

Worse yet, the challenges around these types of cybersecurity risks have implications not only for the agencies involved, but for companies that do business with them, like cloud providers and other technology partners.

"We need a multi-layered approach to bring visibility and help mitigate these types of threats," says Splunk SVP of Security Markets Haiyan Song. It would include a security operation platform anchored on analytics and automation, with tools that can adapt to different sectors and industries. "We need to safeguard public services and infrastructure against high-impact, targeted attacks — before adversaries strike."

Cloud Security

Hackers will find new low-hanging fruit in the cloud

The most advanced (and potentially devastating) cloud attacks will occur at machine speed in 2020.

Most attacks in which cloud was the vector have succeeded because of misconfiguration — a human error that created a vulnerability. For example, the prominent 2019 hack on a major U.S. bank involved a former insider, but it was due to a misconfiguration that she was able to steal the data.

As the majority of enterprises continue their steady migration to the cloud, many of them ask, "Are we safe in the cloud?" The conventional answer has been that the cloud is safe if you take some basic precautions. In 2020, it will become clear that this is an incomplete answer at best as attackers adopt new favored approaches.

"Cloud misconfiguration has been a path of least resistance for attackers. As better automation eliminates that problem, cybercriminals will have to identify a new 'easy route,'" says Splunk's Haiyan Song. "Going forward, cybercriminals will exploit the emerging vectors brought to bear by cloud native technologies such as containers and Kubernetes, taking advantage of organizations' learning curves to launch new attacks at a scale and speed we have not seen in the on-prem world."

Expect to see the cloud become a more prominent vector for versatile attacks. And expect organizations that automate and orchestrate their security posture to fare better in an increasingly challenging environment.

Thus, organizations should continue to focus on security basics as they transition to the cloud. As migration to the cloud presents a new beginning, it's a good time to invest both in end-to-end instrumentation for monitoring the full cloud stack and in security automation. Prudent steps will allow your organization to move at scale while also securing at scale.

Threat Intelligence

MITRE ATT&CK will become the go-to framework and common vocabulary for every SOC

The real-world knowledge base has made tremendous gains in security circles, and deservedly so.

Leading-edge security teams already know and use the MITRE ATT&CK framework. This knowledge base of cybercriminal techniques draws from years of threat intelligence to give organizations a better view of the threats they face, and the strategies and tactics to thwart attackers. Once the province of the most forward-thinking organizations, in 2020 MITRE ATT&CK will emerge as an essential lens that all security professionals use to understand and defend against attacks, whether from profit-motivated criminals or nation-state actors.

The MITRE Corp., a not-for-profit organization that works closely with the U.S. government on security issues, began developing ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) in 2013, and released the first version of the framework in 2015. Its purpose is to understand and classify attacks to figure out how adversaries operate, and how to best respond to an active attack and remediate afterward.

"The framework gives people a great perspective on many attack vectors in a single point of reference," notes Monzy Merza, Splunk's head of security research. "That lets you focus your security efforts on the areas of greatest impact and need for your organization. It also offers a consistent and common approach to help you triage alerts and strategize your response to actual threats as they arise."

For organizations required to have the most aggressive stances on security, such as financial services and healthcare, ATT&CK is already the go-to framework. In 2020, it will become a basis of conversation for security operations center (SOC) teams in other industries, including retail and manufacturing, as they mature their security postures.

Because the ATT&CK framework has been increasingly adopted by the security industry, it will be incorporated into more products and solutions in 2020, effectively becoming the foundation of every security discussion.

"The increased adoption of the ATT&CK framework will help organizations improve their security posture," Merza says. "We also know that having a common vocabulary and lens enable better collaboration and sharing for the cybersecurity industry."

The road goes ever on

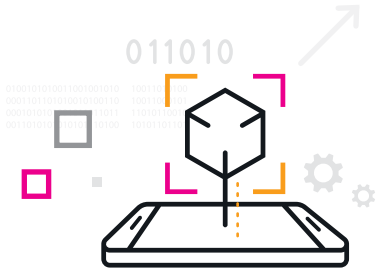
Transformative technologies continue to redesign every aspect of how we live and work. They also, by necessity, redefine how we protect the essential element of our privacy and our businesses: our data. That means constant vigilance and an ability to recognize shifting winds.

"Being aware of the latest threats is just one way to keep ourselves safe," Splunk's Song says. "But we also need to evolve our technologies and how we fundamentally look at security challenges."

Automation eliminates the vast swaths of the security workload that's mundane and repetitive, letting analysts focus on what matters: defending against the dragons.

IT Operations

Virtual interfaces and human inspiration are among the factors that will shape the IT experience for leading organizations.



Technology changes constantly, creating new opportunities and challenges every day. Information technology professionals have a unique responsibility to keep their organizations running smoothly, delivering results to their users while evolving and advancing to meet new requirements and anticipate future growth.

But as expectations placed on the IT department continue to rise, IT leaders face a broader set of challenges, many of which have less to do with the technology itself and more with how it's applied, and its ramifications for the entire organization. Whether it's to empower innovation, improve user experience or investigate forgotten data assets, enterprise IT in 2020 will turn its attention to forces of fundamental change in the technology world.

AR/VR

The world will continue to go beyond mice and touch with augmented and virtual reality

B2B enhancements of everyday experiences will lead to a consumer wearables revolution.

"The mirrorworld doesn't yet fully exist, but it is coming. Someday soon, every place and thing in the real world — every street, lamppost, building, and room — will have its full-size digital twin in the mirrorworld." — Kevin Kelley, Wired, Feb. 2019

When most people think of virtual and augmented reality, games like Pokémon Go probably come to mind. The first surge in consumer AR hit gaming and entertainment, a trail blazed by Pokémon Go and Harry Potter: Wizards Unite. Commercial and business applications are also in use today for product design and engineering. And retailers are experimenting with technology that can let shoppers experience products before purchase.

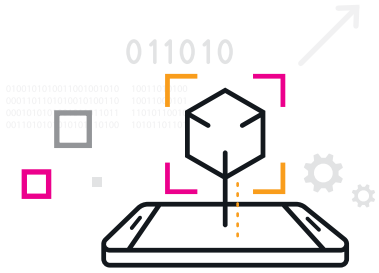
In 2020, we'll see virtual reality (VR) and augmented reality (AR) expand beyond gaming headsets and the design lab. Organizations from governments to healthcare providers are using AR and VR in compelling ways that will pave the way for better mass-market applications. In 2020, AR and VR will grow in the enterprise market, setting the stage for a consumer explosion.

The entire VR/AR market is expected to reach $210 billion by 2022, with AR a significant portion. In 2020, we'll see continued adoption of AR across manufacturing, search and rescue, healthcare and retail. It is increasingly common for workers in the field to use AR technology to access instructional and metric overlays that color their environments. Search and rescue missions will become less dangerous as teams start preparing with 3D maps and overlays of dangerous environments and scenarios.

Speaking of 3D, medical imaging will be widely enhanced with 3D models of patients for more precise clinical knowledge. Johns Hopkins has already developed an AR solution to train brain surgeons for delicate procedures.

Splunk Chief Technology Officer Tim Tully sees several factors holding back consumer applications of AR, including the infrastructure. He expects that only with widespread rollout of 5G will AR come into its own, much as smartphones and 4G enabled on-the-go video streaming and instant-order apps like Uber and Lyft.

Another major limiting factor, Tully says, is the lack of consumer-focused design. Even as enterprise and industrial applications evolve, they're not yet consumer-friendly enough for daily users. Tim champions consumer-centric design that truly works for the user.



"Existing AR applications aren't created with much empathy for the consumer and the tasks they're out to accomplish in their everyday lives," he says. The AR devices that provide a better user experience across everyday tasks have massive potential.

Empathy for the consumer also requires an understanding of what value they get from a product. As augmented reality matures, we'll see more and more applications that make work and play more engaging and more rewarding. Ultimately, the goal with AR for application developers should be to blend important data with the physical world.

Access — in terms of both tech and money — will be key in this process. Technologically, today's mobile phones might not be immersive enough to provide a true AR experience; actual wearables where the AR experience can be seamlessly blended with the real world will perfect the experience. As will reduction in cost, which can price out the average consumer. As with most technology, prices will go down with rising competition and the availability of cheaper, newer components.

A lot of this is here already, or just around the corner. Soon, more compelling AR Cloud applications could play a large part in enabling the mirrorworld: Imagine walking down the street, wearing your smart contacts (Samsung has a patent), and getting a constant feed of context and information about the real world around you. We already have a primitive version of that via Yelp's monocle feature and Google Lens. Expect it to more thoroughly permeate our reality in the next five years.

Automation

Companies using automation to replace employees will lose to companies using automation to empower them

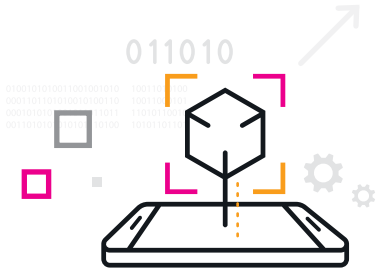
Efficiency will only take you so far. Use automation to drive innovation.

Companies that race headlong to embrace new technologies — especially technologies that automate jobs previously held by people — may actually be sabotaging their long-term success rather than enhancing it.

Deloitte's State of AI in the Enterprise report concludes that enterprise software is the easiest and most popular path to artificial intelligence, with 59% of respondents saying their company uses it. The survey also presents a troubling dichotomy; while 79% of respondents say AI technologies empower people to make better decisions, 63% say their company wants to cut costs by automating as many jobs as possible.

The efficiencies offered by automation are attractive, but companies that prioritize cost reduction above all else are only seeing half the potential. Doing the same work you're doing today faster and cheaper may make sense on a spreadsheet, but not if it keeps you from evolving and growing in a marketplace driven by innovation and disruption.

AI-powered automation can take over repetitive tasks that demand less creativity and insight. AI-powered analytical tools can derive new insights from vast amounts of data, in everything from IT operations and cybersecurity to business operations and supply chain management. The companies that will get the most value out of AI are the ones that consider the whole opportunity: delivering new insight while freeing up your best minds



to make new contributions that raise the top line, as well as reduce overhead.

There's also the hit companies take when they make their workers feel disposable. Strong culture and high employee engagement are essential to high-performing organizations. People can understand a company's evolution, even painful ones, if they feel that the workforce is still valued in the new reality.

Deepak Giridharagopal, CTO of Puppet, predicts that 2020 will kick off a new era of introspection when it comes to the balance between people and technology, especially when it comes to automation.

"One camp sees a human being and says, 'That human being should be replaced with a Roomba,'" Giridharagopal says. "The humanity inherent in that job is not important."

That can be a very seductive mindset for companies that see digital transformation solely in dollars and cents. "Roombas are cheaper than humans, so why not replace the latter with the former?" Giridharagopal adds. "I see this 'substitution bias' in cost-obsessed and scale-obsessed companies. They fixate on supplanting employees with automation, when in reality humans are rarely fungible."

"No matter how far technology has advanced," says Splunk Chief Product Officer Sendur Sellakumar, "organizations are still built and grown by people. Leaders who don't understand the fundamental humanity of the enterprise are doomed to fail."

Giridharagopal and Sellakumar agree that automation is a way to enhance the working experience for employees and allow each to contribute at a higher level, and should not be used to drive efficiency at the cost of innovation.

"I don't want to replace you with a Roomba," Giridharagopal says. "I want to build you an Iron Man suit."

UX/Consumerization

2020 will be the year of the indulgent user experience

Enterprise software doesn't have to be a boring slog. There. We said it.

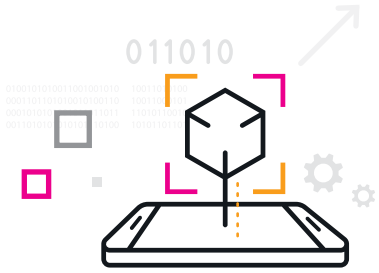
Ever since "consumerization of the enterprise" became a trending topic, enterprise software companies have been saying they place a high value on design and user experience (UX). But the fact is that many of them don't. Enterprise employees spend their days jumping back and forth from modern, design-forward apps to dull, monolithic programs with fundamentally unfriendly UXs that haven't changed for years.

Splunk CTO Tim Tully is passionate about design and the potential it has to enhance the lives of enterprise employees. He has elevated the focus on design at Splunk to drive a completely new user experience — one so focused on providing a rich and rewarding UX that he calls it indulgent.

According to Tully, 2020 will be the year of the "indulgent user experience." And that doesn't bode well for the holdouts.

"For decades, enterprise software users have been beaten down by the monotony and tedium of the software they are forced by their teams to use," Tully says. "But enterprise software companies had little incentive to do anything different."

Their priority was selling as many seats as possible and keeping the user experience consistent in favor of functionality, he says. But that attitude led



to stagnation. Users accepted a dull or awkward experience — and the poor outcomes that resulted — because they had no alternative.

"Enterprise customers become so reliant upon bad, yet functional, software that they'll buy it no matter what its user experience is like," Tully says.

But enterprise users have more choices now. They may still find themselves spending a lot of time bogged down in dull or difficult interfaces, but they also have a growing list of exciting, engaging apps in their tech stack — apps like Slack.

It's hard for users to accept poorly designed apps once they've experienced well-designed ones. For one thing, an app built with the user experience in mind is easier to use.

"Design should communicate function," Tully says. A well-designed product, physical or digital, tells the user how to use it, without an instruction manual. In that way, design provides a measurable, practical benefit to users: better outcomes.

Tully also believes that quality design, mixing function with elegance, gives users confidence.

"Elegant design pulls you forward," he says. "It gives you an edge to tackle whatever action is in front of you. Using a well-designed product feels more like a motivation than a chore."

Enterprise software companies who are still producing dull user experiences will find it harder to keep their users loyal, Tully says, and will be even more vulnerable to disruption. He points to startups in financial and HR software categories that have made significant inroads against more monolithic legacy competitors.

"This is about improving something fundamental," Tully says, "Splunk is improving the way people act on information."

"When it comes to enterprise UX," Tully says, "the companies that will succeed are the visionaries that design software to make people's entire experience better."

The human impact

When trying to predict the future of IT, the easiest path is to single out particular technologies and trends that are on the rise, and to predict that their rise will continue. That approach has value for IT decision-makers who need to plan for headcount, for instance, or infrastructure. The bigger challenge is to identify the macro trends that will shape the way IT departments address their fundamental business challenges.

In 2020 (and beyond), the IT leaders who will have the biggest impact on their organizations are the ones who focus on how their technology decisions intersect with their people decisions. For many, the best practice would be to seek a balance between the two.

Data Shapes our Future

In the digital age, every year feels like the dawn of a new decade. But there is no question that we're on the cusp of a third consecutive decade of enormous transformation. Think about where the Internet was in 1999, and how it evolved in the decade that followed. Think about where cell phones were in 2009 and where they've gone since. Now look at where 5G, AI and VR are today, and try to imagine what's next. Feels like the moment at the top of the roller coaster before that first big plunge, right?

Technology drives culture, and everything moves at the speed of data, which makes prognostication a tough gig. On the one hand, few of us saw exactly how transformative smartphones would be when they debuted just over a decade ago. (A decade ago, the only way to hail a taxi was to stand on a street corner waving your arms around. Now there are apps to get your dry cleaning delivered.) On the other hand, plenty of last year's predictions for 2019 saw technology fall short, as, for instance, quantum computing and foldable smartphones failed to make anticipated market headway.

In preparing for the future of your organization, the broadest, and smartest, prediction is that data will continue to open up new possibilities. Predicting specific futures is a valuable exercise. But the exercise is less about betting the farm on one trend or outcome, and more about building broader resilience into your organization. Smart leaders are prepared to weather adverse change, and to seize the initiative when the stars align.

splunk> turn data into doing™