Highlights

Was Black Hat USA 2021 a victim of the COVID resurgence, or is it just losing relevance? In case you didn't go (probably smart given that Las Vegas is reportedly a COVID hotspot), the show this year was nearly a ghost town. I talked to a number of cybersecurity companies at Black Hat who said that half or more of their scheduled customer meetings for the week were cancelled. Floor traffic was also anemic, and room rates at the Mandalay Bay (where Black Hat USA 2021 was hosted) and the Delano (part of the Mandalay Bay complex) plunged from the $400-$500/night range a month ago to the $100 range this week. Now, all of those things would point to COVID being the primary cause. However, the other thing you would have noticed at Black Hat is that (at best) 20% of the floor space in the Mandalay Bay Convention Center had exhibitors on it, and only one company (Trend Micro) was reported to have pulled out of the show. Compare this to the RSA Conference, which always maxes out the Moscone Center in San Francisco.

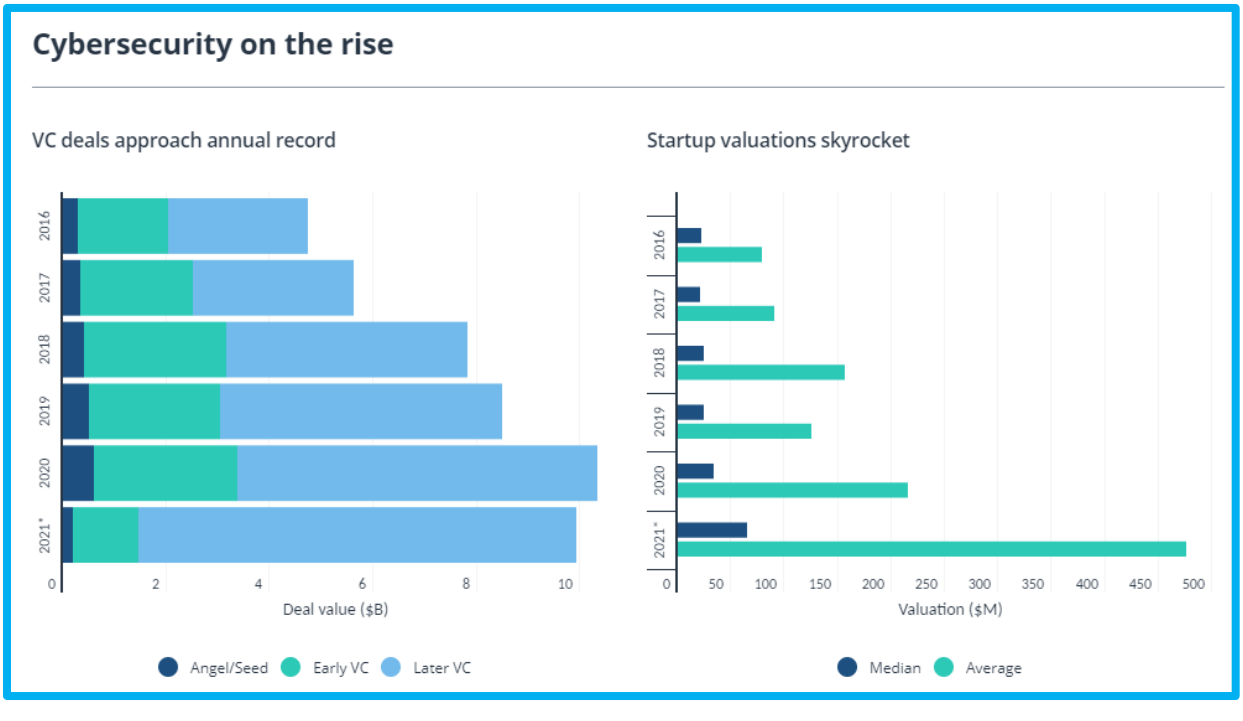
Black Hat has evolved over the last 25 years from a hacker-focused conference to one that now is squarely an enterprise cybersecurity show, alienating a large number of its original attendees. While there is clearly a significant need for more cybersecurity education and information (especially since attacks have increased during COVID), whether Informa should have canceled Black Hat USA 2021 given the negative attendance impacts is a question that they will need to answer. Whether Black Hat remains relevant (and in what form) is a question that the community will probably answer for them.

Cheers! Mike Heumann

VCs Banking on Threats, Breaches, and Accelerating Cybersecurity Market

The cybersecurity market is flush with VC funding at a record high with over $7.8B invested in 2020. Cybersecurity venture funding has been increasing over the last decade with 1500 companies receiving funding since 2017, including 58% seed-stage opportunities. Over $3.7B has already been invested in by April of this year. Over 75% of 2020 funding went to US companies, at $5.9B.

Top investors include Accel, Insight Partners, Techstars, Y Combinator, Ten Eleven Ventures, Lightspeed Venture Partners, Clearsky, ForgePoint Capital, Intel Capital, Salesforce Ventures, and Sequoia Capital.



Netskope raised $340M at a valuation of $3B. More than thirty cybersecurity firms have become unicorns so far (companies valued at over $1B). These 13 companies have achieved billion dollar valuation since November Aqua, Axonius, BigID, Coalition, Feedzai, Forter, ID.me, Lacework, Orca, OwnBackup, Socure, Venafi, and Wiz (top 10 VC-back cybersecurity deals of 2021).

Black Hat

Analyzing Mistakes of Attackers Infrastructure Errors

Analyzing the Behavior of Victims Action Bias

Windows Facial Recognition Authentication Hacked – Easily

Analyzing Mistakes of Attackers Infrastructure Errors

The IBM X-Force Incident Response and Intelligence Team (IRIS) gained access to a server belonging to the suspected Iranian threat group ITG18, known as “Charming Kitten”, Phosphorous, and APT35. IRIS discovered over 40GB of video and data files being uploaded to a served that hosted ITG18 domains used in 2020 activity. The data included hacking training videos showing a Google account's data stolen in around four minutes and a Yahoo account compromised in under three minutes. Two members of the IBM X-Force, Allison Wikoff and Richard Emerson, presented their findings and provided insight into the group’s operations.

ITG18 has been active since at least 2013 and is linked to attacks on presidential campaigns, pharmaceutical companies, researchers developing vaccines for COVID, and nuclear scientists. The group targets individuals with an Iranian connection including members of the US Office of Foreign Assets Control which implements economic sanctions.

ITG18 consistently made the mistake of misconfiguring their servers to leave listable directories, yet; although there has been a lot of attention paid to this group, they have not changed their approach. IRIS calls the malware ITG18 uses to infect victims, “LittleLooter”.

The IBM X-Force IRIS Cyberattack Framework prepares organizations to defend against cybersecurity threats by looking at attacks from the perspective of the attacker. The preparation that goes into a sophisticated attack includes preparing an attack infrastructure. One basic defense strategy is to

"We don't get this kind of insight into how threat actors operate really ever." "When we talk about observing hands-on activity, it’s usually from incident-response engagements or endpoint monitoring tools. Very rarely do we actually see the adversary on their own desktop. It's a whole other level of 'hands-on-keyboard' observation."

Allison Wikoff, Senior Strategic Cyber Threat Analyst

purchase all the domains that are likely to be mistaken for your company's domain, including other common or misspellings. After a cybercriminal gains access to the network, they may escalate privileges, move laterally through the network, and conduct internal reconnaissance. The attacker will also hide the attack by deleting logs and hiding or disguising malicious code. IRIS also aids companies in managing their response to an attack, investigations, and in implementing remediation and recovery plans. IRIS found that multifactor authentication did dissuade this cybercriminal group from attempting further attacks. They also recommend not using the same password, no matter how strong, across different platforms. And, here are passwords that should never be used, but are very common.

Analyzing the Behavior of Victims Action Bias

A cool head could be the key to addressing cybersecurity challenges, but "action bias" pushes the employee to act, often "overreact" under a belief that action, any action, is better than inaction. Josiah Dykstra and Douglas Hough address the human response to react forcibly and quickly in response to a perceived crisis. They highlight the need to make reactions routine, through preparation, versus impulsive.

Except from a podcast with Joe McGonegal: *"Action bias is that it can be simply summarized-- don't just sit there, do something…A patient comes into a physician's office thinking that she has either the flu or bronchitis or something like that. And the physician examines her, says, yes, indeed, it's bronchitis. The patient says, well, give me something. Give me a pill. Give me an antibiotic. Give me a shot. Give me something. Well, every physician knows that most bronchitis is viral bronchitis, for which antibiotics do no good….And for the physician to have a happy patient, often the physician's going to have to prescribe that antibiotic even though they know that it is nothing more than a placebo... Framing has to do with the fact that how an issue is presented often determines how a decision is made. Now, for standard economists, that makes no sense whatsoever because the assumption is that a decision maker is going to see through those frames and is going to go down to the nut of the issue, whereas behavioral economists have discovered time and time again that how you frame an issue really determines how people make decisions… The physician has diagnosed the problem and realizes that there are two ways to go about things… And how the physician positions those two options really determines how a patient will make a decision as to which way to go. If they present the risks to the patient first, the patient's pretty much going to say, oh, I'm not going to have that, whereas if they*

present the benefits first, then what happens is that the patient is thinking, oh, man, I have this knee surgery, I'm going to be able to walk again." Douglas Hough, Senior Associate, John Hopkins U & author of Irrationality in Health Care: What Behavioral Economics Reveals about What We Do and Why

Studies of how non-IT people react to phishing emails found that when the nonexperts correctly identified the errant email request, they reported having a gut feeling something was not quite right, they knew what to expect in that email account and noticed abberrations, they took steps to investigate suspicious emails, and they were able to make good decisions. Delaying action is a critical component to successfully identifying and refraining from reacting to malicious emails.

There are times that immediate action is imperative and other times when taking a moment to reason through the situation can result in rational – and more effective – decisionmaking. The bias to respond is linked in part to the concern that inaction will be perceived as weakness. But, deliberate inaction can be the most strategic choice. And, people, while often not act irrationally, are irrational in predictable ways.

Josiah Dykstra, Technical Fellow, Cybersecurity Collaboration Center, cautions organizations to not put so much pressure on employees, noting that attacks are always going to happen, "Hackers are incentivized to keep trying. They will keep coming over and over again, but we don't need to let that lead to burnout. We can help build resilience in the people, and resilience in the processes that we have in our organizations, so it isn't so stressful in those situations — they know what to do; they've done it before."

Windows Facial Recognition Authentication Hacked – Easily

In May 2020, Microsoft reported that Windows Hello had over 150M users and that 84.7% of Windows10 users sign in using Windows Hello. This vast facial recognition user base drew the interest of CyberArk. The system works only with webcams that have an infrared sensor in addition to the regular RGB sensor, but does not even look at the RGB data.

"We created a full map of the Windows Hello facial-recognition flow and saw that the most convenient for an attacker would be to pretend to be the camera, because the whole system is relying on this input." "Our findings show that any USB device can be cloned, and any USB device can impersonate any other USB device. Identifying a USB device by a descriptor provided by the device is the main reason for this. The OS cannot validate such a device authenticity, at least not according to the USB specification."
Omer Tsarfati, Cyber Security Researcher, CyberArk

By using one straight-on infrared image of a target's face and one black frame, they were able to breach Windows Hello. An attacker would have to have physical access to the device to exploit it. Microsoft immediately released patches to correct the egregious error. CyberArk provides a proof-of-concept video demonstrating how they bypassed Windows Hello. They successfully hacked the program by capturing an image of someone, saving the captured frames, impersonating a USB camera device, and sending those frames to the system for verification. Because Windows Hello relies on external data sources, the program is exploitable. Because the host cannot identify which device is connected to the USB port, each device can subversively impersonate another. CyberArk completed the breach using an accurate infrared image of its target – paired with RGB frames of SpongeBob SquarePants.

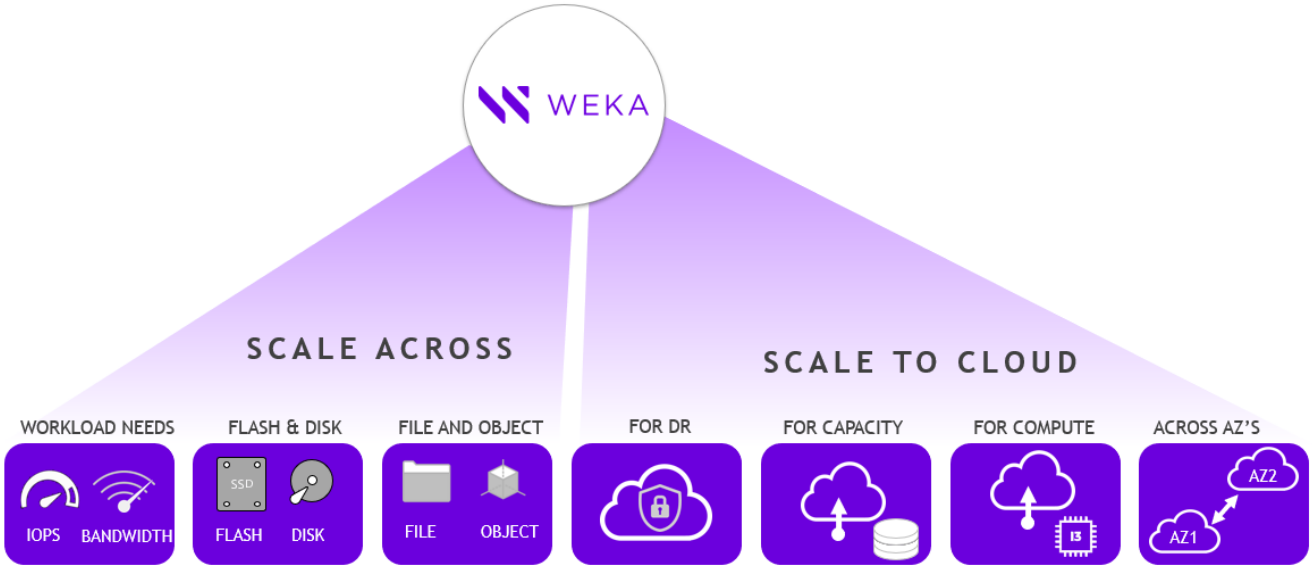
WekaIO Scalability for Disaster Recovery

Companies that pay ransom may get their data back but 46% of the time the data is either partly or completely corrupted. Vendors can move a copy of a company's data to the cloud but disaster recovery needs include recreating the environment to a pre-disaster business-mode.

WekaIO provides backup in the cloud, direct access in a disaster, and implementation in the cloud for business continuity in a crisis. The Limitless Data Platform automatically allows users to scale a NVMe tier for increased performance and scale an object tier for increased capacity by leveraging NVMe, NVMe-oF, NVIDIA Mellanox InfiniBand, 100 Gb Ethernet, and GPU acceleration. Customers have the advantage of managing data on a single platform which is integrated with Kubernetes, Rancher Labs, and Ansible for easier container deployment - with hardware options of AMD or Intel x86-based servers supporting PCIev4 doubling transmission speeds.

IDC Perspective, "Because most parallel file systems are deployed on top of block-based volume managers, it can be very difficult to create a recoverable copy of the entire file system environment (if it can be done at all). WekaFS includes a single click "snap to object" function that instantly creates a complete, recoverable copy of the front-end file-based data that includes all its own metadata (enabling recovery to and/or use from anywhere, not just its original source). The snapshots can then be recovered to a completely different system, even in a different data center or the public cloud."

NEW DIMENSIONS OF SCALABILITY



"Scalability is no longer about the most cores, bites, or whatever unit of measure you want to apply to it, primarily because we've hit a diversity of workloads. There are many more things that an organization has to do now that they didn't have to do before. You can still do all of your traditional enterprise operations, like ERP and CRM on the IT side of the house, or on the HPC side of the house it involves things like finding new pharmaceuticals, finding oil, and making cars safer. All those applications still exist. However, if you go back to the big data and analytics from eight to 10 years ago, all of a sudden we've got many new analytics applications to bring into the mix. Now the big emphasis is all on machine learning, but no one has tripled my budget! I still have to do all of the things I did before, plus I have to do analytics and machine learning, and they're all part of the same environment. That's just on the one hand.

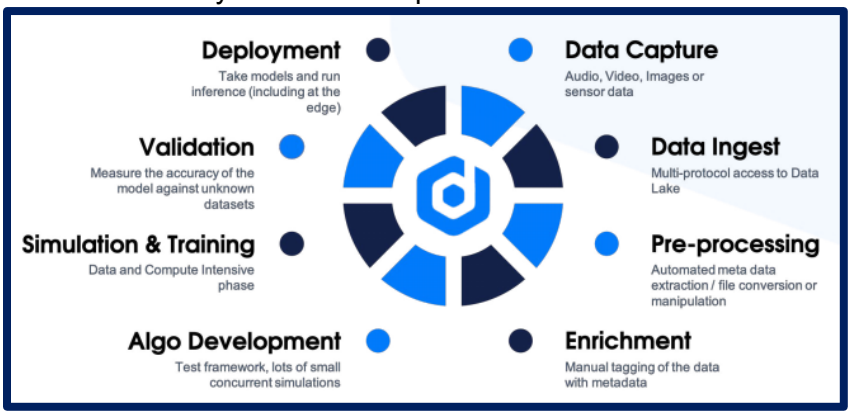
Addison Snell, CEO,
Intersect360 Research

On the other hand, the technology keeps changing, fueled by all of these new workloads. We brought in flash storage and all of these new tiers of storage. And now on the processor side you've got diversity as well, with not only competition among x86 processors, but Arm processors are coming into the mix with all types of accelerators, GPU computing, FPGAs, and custom coprocessors. I've got to manage all of those technologies and match them to all these different types of workloads. That's the New Scalability. It involves how I get all of those to match up, and that's before you even begin to talk about the cloud, which is the other major development here. So I'm left wondering, can I manage all of the different technologies, can I do it on premises and into the cloud and bring data in from the edge? To me, the New Scalability involves managing all of these things in an IT environment. It doesn't matter if I can make it bigger if I can't also have the flexibility to do all of the different things that I need and want to do."

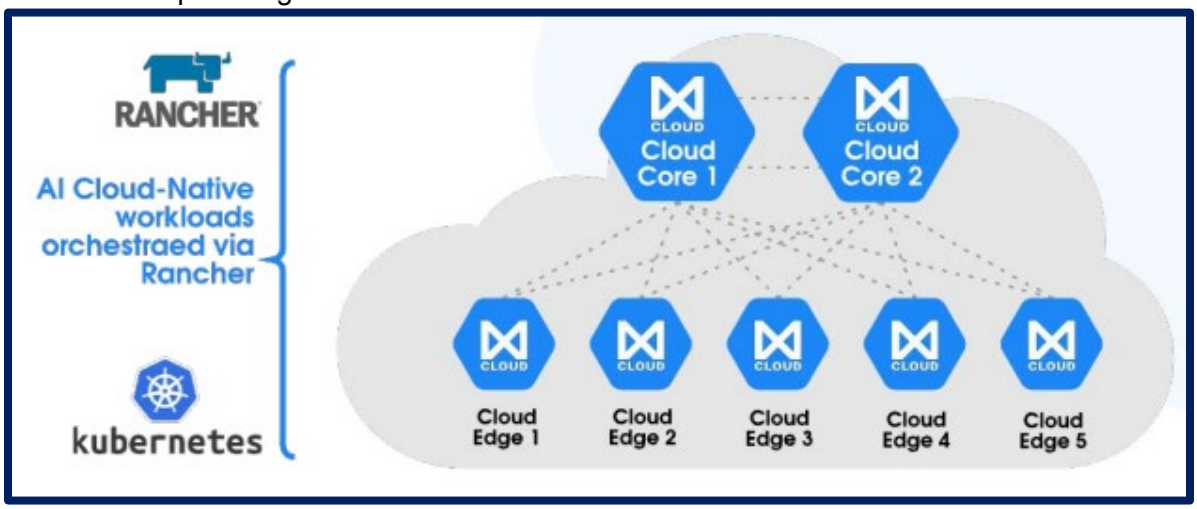
Excerpt, WekaIO blog post highlighting key points from their webinar "CIO Superhero vs HPC Warrior"

LMX AI Architecture – NVIDIA DGX A100 + Lightbits LightOS

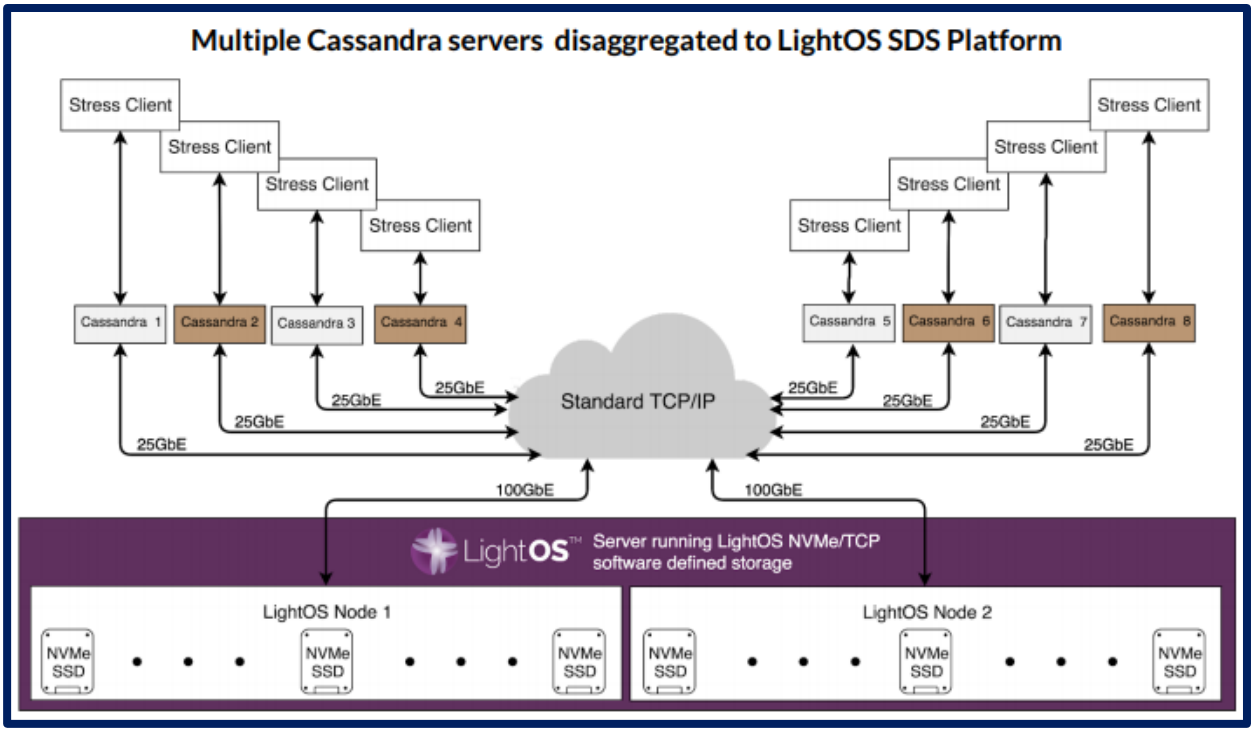
As we move toward more reliance on AI solutions, there is increasing pressure on infrastructure. Continually upgrading hardware is costly and potentially cumbersome. The AI life-cycle includes capturing data that is in a variety of formats and from many sources. The process of "enrichment" is the manual process of adding additional meta data to the datasets and enriching the data with information to train the neural network.



Define Tech has an AI Reference Architecture with NVIDIA DGX A100GPUs, LMX AI optimized cloud software, and Lightbits LightOS NVMe storage. The platform includes NVIDIA Mellanox Spectrum ethernet, NVIDIA Mellanox Quantum InfiniBand switches, pre-integrated with frameworks such as Tensorflow, Caffe, and Theano. The LMX Cloud is pre-integated with NVIDIA GPU Cloud.



LightOS is designed to disaggregate storage from compute that provides, among other things, safe data management. Data is protected from SSD failures using an optimized Erasure Coding (EC) algorithm managed in concert with the high-performance LightOS Global FTL, streamlining data management across the pool of SSDs, increasing performance and ensuring data is safe. Lightbits and Intel have partnered for an ADQ-accelerated NVME/TCP solution. LightOS addresses target server failover, data reduction, and erasure coding protection.



AI, GPUs, and Storage Use Cases in Healthcare

with sponsors NVIDIA, Weka, KIOXIA, Datyra

How large are your organization's AI/ML training data sets? (check one):

Greater than 5 PB:	0%
Between 1PB and 5PB:	7%
Between 250TB and 1PB:	13%
Between 50TB and 250TB:	13%
Less than 50TB:	67%

What are your greatest concerns when building very large AI/ML training data sets? (check one):

The amount of time to run training data through the model:	39%
The cost of the hardware required to run the training model:	33%
Managing the various training and verification datasets:	6%
Managing and archiving the results of training runs:	11%
Other issues:	0%
No opinion:	11%

G2M Research Multi-Vendor Webinar Series

Our webinar, Tuesday, July 13 “Computational Storage vs Virtualized Computation/Storage in the Datacenter – And The Winner Is?” sponsored by ScaleFlux, Achronix, and Pliops is available to view. Register for our webinars and we will send these recordings directly to you. Over 1300 registrants for this webinar!

View the recording here and/or download a PDF of the slides. Our webinar schedule is below- Click on any of the topics to get more information about that specific webinar. Interested in Sponsoring a webinar? Contact **G2M** for a prospectus.

You can view all our webinars and access slide deck presentations.

G2M RESEARCH

Aug 17:	AI/ML Storage - Distributed vs Centralized Architectures
Sept 14:	Cybersecurity: Measuring (and Countering) Third Party Risk
Oct 12:	Cloud Service Providers: Is Public Cloud, Private Datacenter, or a Hybrid Model Right for You?
Nov 9:	The Radiometry Data Explosion: Can Storage Keep Pace?
Dec 14:	2021 Enterprise Storage Wrap-up Panel Discussion

AI & Cybersecurity Events

August 10	ISMG Virtual Cybersecurity Summit: Brazil
August 15-19	CRYPTO 2021
August 16-19	Data Center World
August 17-18	ISMG Cybersecurity Summit: Fraud &Payments Security
August 17-19	WorldFestival
August 17-19	Ai4 2021
August 19	FutureCon Overland Park
August 23-25	AcceleRISE
August 23-26	IEEE BigDataService 2021
August 24	Chicago 2021 Virtual Cyber Security Summit
September 1	FutureCon San Diego
September 2-3	IntelliSys 2021
September 6-7	AI & Big Data Expo- Global
September 7	ESCON 2021
September 8-10	Women in Cybersecurity
September 15-16	ODSC APAC
September 16	Miami/South Florida Virtual Cyber Security Summit
September 16	Interface Sacramento Reno
September 16-17	Cyber Security Summit & Hacker Conference
September 16-18	Global Artificial Intelligence Conference
September 20-22	Gartner Security & Risk Management Summit
September 22-23	The AI Summit London 2021
September 23	SecureWorld Great Lakes Virtual Conference
September 29-30	AI & Big Data Expo – North America

G2M RESEARCH

Effective Marketing & Communications
with Quantifiable Results