

THE 3Q20 CYBERSECURITY MARKETING SNAPSHOT: IMPLICATIONS FOR 2021

An inside look at trends in Content, Events, Messaging, Data, LeadGen, Persona Development and Community.

10.13.2020



CYBER
THEORY

Key Earnings Call Insights

Company	Commentary
 CLOUDFLARE	<ul style="list-style-type: none"> ▪ Increase of stress on systems is driving engineering teams to enhance platform efficiency to improve network speed ▪ A Unified platform enables cost effective bundling of services that displace legacy vendors & improve savings ▪ The current environment is exposing the weaknesses of on-prem network hardware solutions such as firewall & VPN
 CROWDSTRIKE	<ul style="list-style-type: none"> ▪ The proliferation of ransomware attacks on SMBs is leading businesses to seek Cybersecurity solutions with flexible pricing models ▪ Vendor solutions need to act as a force multiplier to address the lack of Cyber personnel in a time of high-volume attacks ▪ Future product offerings will need to demonstrate the ability to protect businesses & its customers from home, office, or cloud environments
 okta	<ul style="list-style-type: none"> ▪ Disparate legacy identity systems cause friction for employees & contractors as employees shift to remote work & access ▪ Integration partnerships are enabling enterprises to combine endpoint risk detection with user identity to deliver unparalleled security ▪ The value of products is clearer than ever as organizations shift to a more decentralized work environment
 paloalto NETWORKS	<ul style="list-style-type: none"> ▪ Data breaches in cloud-delivered services will accelerate as InfoSec & DevOps organizations rush to the cloud without establishing their cloud security posture to the level of traditional data centers ▪ Cloud security investment spend will increase, especially in technologies that secure multi-cloud & hybrid cloud environments ▪ Moving away from relying primarily on physical offices & physical data centers to remote work & the cloud will prompt the redesign of WAN
 Qualys.	<ul style="list-style-type: none"> ▪ Entities will need to rethink their security and business continuity plans to include remote connectivity, accelerate their cloud migration plans and streamline and secure, if not reinvent, their supply and delivery chains ▪ Building a highly scalable cloud-based platform enables the unification of IT, security & compliance across the new hybrid environment ▪ Looking forward, companies will be more focused on reducing cost, while increasing business flexibility
 zscaler	<ul style="list-style-type: none"> ▪ Adaptation is key as COVID-19 is accelerating the digital transformation & resistance to change is dissipating ▪ Zero trust network adoption is increasing as network security can no longer be done in a perimeter-less world ▪ As COVID-19 persists, businesses are becoming increasingly cost conscious & are looking to consolidate best-of-breed platforms than rather best-of-breed point products

This report updates our earlier “2020 CYBERSECURITY MID-YEAR MARKETING SNAPSHOT” research with our experience over the last 90 days.

Our interaction with Cybersecurity vendors’ marketing professionals in over 350+ in-market campaigns reveals progress and challenges reaching and persuading the global CISO decision-maker community.

The impact of COVID-19 is obvious and doesn’t need further elaboration from our view.

What is maybe not so obvious is that the rate of spend on Cybersecurity initiatives during this period has increased somewhat dramatically compared to any prior period.

Many of our clients, including the top six performers on Momentum’s 2020 Half-time report, have experienced significant uplift in both market value and revenue growth.

All charts from
Momentum’s CYBERSECURITY MARKET REVIEW | 1H 2020

CHALLENGES:

Persona Development

First-Party Data

Messaging

Content

LeadGen

Virtual Events

Community



PERSONA DEVELOPMENT.

Many of our clients claimed that while reaching the CISO is still a top priority, marketing sights have been slightly lowered to target key influencers on the security team.

This owes to the fact that the CISO and ultimate decision-maker is almost impossible to reach, as s/he has self-imposed a non-response policy with regard to all external communication.

The sales and marketing noise level has increased exponentially during the COVID-19 era, and the attempts to reach this persona have contributed to increased cost of marketing outreach while failing to produce many convertible results.

In the COVID-19 era, business objectives are much more closely aligned with Cybersecurity, hence decision-making has become more multidisciplinary.

Creating intrigue and interest among influencers and adjacent team members is both easier and from a leadgen perspective, more efficient.

The tradeoff is a longer nourishment campaign, but the results far out-perform the traditional targeting approach.

FIRST-PARTY DATA.

There was a time when third-party data was golden and cheap. But in today's reality, first-party data, which is behavioral and intent-implicit is irreplaceable as a way to enrich identity data and to create a more personalized customer and prospect interaction and to target messaging with greater precision.

The problem with third-party data has always been that while it is inexpensive and easy to come by, it lacks context.

Building campaigns on context-free data does not produce the kind of campaign results that marketers seek.

With third-party cookies soon making their exit, and with GDPR and CCPA tightening the rules around which data brands are allowed to use, the value of opted-in first-party data is higher than ever before.

While many of our clients' marketers understand the value of first-party data, there appears to be some debate about how best to leverage it.

Today's biggest challenges in the Cybersecurity markets seem to be getting the right story aligned with first-party data to create individualized experiences for the target audience and combining first party data with other data sources to tease out product, service or topical intent.

Most of our clients have concluded that trying to optimize targeted campaigns using a blend of various data sources is a difficult and time-consuming process, often resulting in missed targets and low conversion rates.

But, those companies who partner with marketing firms who have mastered first-party data and are turning it into experiences that enrich their prospecting outreach are seeing an immediate transformation into competitive advantage.

MESSAGING.

Today's wall of noise is challenging to even the most seasoned marketing executives.

Most of today's messaging is falling flat as it becomes more difficult to distinguish one company's amazing products from another.

Our Customer Advisory Board and CyberEd Board are now comprised of over 150 working CISOs.

They advise on positioning and messaging for our clients and have reviewed dozens of campaign briefs over this past quarter.

We know for certain that the key to audience penetration is to deliver fact-based marketing that resonates with the intended audience and speaks in an authentic voice.

Increasingly, in this era when we are bombarded with inbound sound-alike messaging, Cybersecurity professionals see through misinformation within seconds.

Your marketing collateral and brand messaging must critically deliver accurate and fact-based information.

The objective is to assure our organizations are seen as trustworthy and credible sources.

Cyber professionals have no appetite or patience when presented with aggressive marketing tactics that oversell or allege to solve all of their problems.

Short, direct, to-the-point messaging that says what your product or service does in easily consumable language and what value it brings works with today's security practitioners.

Messaging that wraps word salad around bumper stickers and buzzwords does not.

Public Company Trading Analysis

High-Growth & Low-Growth Cybersecurity

Company	Stock Price	LTM Price Performance	Market Cap (\$M)	Enterprise Value (\$M)	Revenue Growth			EV / Revenue			EV / EBITDA			P / E	
					LTM	2019A-2020E	2020E-2021E	LTM	CY 2020E	CY 2021E	LTM	CY 2020E	CY 2021E	LTM	CY 2020E
High-Growth Cybersecurity (>20% 2018A – 2021E CAGR)															
okta	\$200.23	63.6%	\$24,583	\$24,284	46.0%	32.7%	30.3%	37.7x	31.2x	24.0x	NM	NM	NM	NM	NM
crowdstrike	\$100.29	58.7%	21,383	20,419	88.7%	60.1%	31.9%	36.2x	26.5x	20.1x	NM	NM	NM	NM	NM
zscaler	\$109.50	42.9%	14,164	13,814	43.5%	35.6%	28.5%	35.3x	28.3x	22.0x	NM	NM	NM	NM	NM
elastic	\$35.95	139.7%	10,917	10,376	48.9%	36.7%	30.9%	32.8x	26.4x	20.2x	NM	NM	NM	NM	NM
tenable	\$29.81	3.9%	2,983	2,802	30.6%	20.6%	20.0%	7.4x	6.6x	5.5x	NM	NM	NM	NM	NM
rapid7	\$51.02	(11.7%)	2,577	2,604	32.5%	19.7%	18.5%	7.5x	6.7x	5.6x	NM	NM	NM	NM	NM
				Mean	48.4%	34.2%	26.7%	26.2x	20.9x	16.2x	NM	NM	NM	NM	NM
				Median	44.7%	34.1%	29.4%	34.0x	26.5x	20.1x	NM	NM	NM	NM	NM
Low-Growth Cybersecurity (<20% 2018A – 2021E CAGR)															
splunk	\$198.70	58.5%	\$31,567	\$31,968	23.6%	2.9%	24.9%	13.5x	13.2x	10.5x	NM	NM	NM	NM	NM
fortinet	\$137.27	77.8%	22,189	20,831	20.6%	16.0%	15.9%	9.2x	8.3x	7.2x	33.4x	30.0x	25.4x	52.6x	48.7x
paloalto	\$229.67	11.7%	22,155	21,995	18.6%	16.8%	17.6%	6.7x	6.0x	5.1x	28.4x	27.2x	23.0x	47.1x	44.8x
checkpoint	\$107.43	(8.8%)	15,062	13,318	3.8%	1.0%	3.0%	6.6x	6.6x	6.4x	13.1x	13.5x	13.2x	17.2x	16.9x
hpe	\$56.01	25.5%	7,794	6,332	3.7%	5.1%	4.9%	4.1x	3.9x	3.7x	12.3x	12.5x	11.9x	28.0x	29.5x
avast	\$6.61	70.0%	6,658	7,543	7.8%	1.1%	6.7%	8.7x	8.5x	8.0x	15.6x	15.1x	14.4x	44.0x	19.9x
proofpoint	\$111.12	(8.8%)	6,368	6,237	23.4%	15.0%	17.5%	6.7x	6.1x	5.2x	39.0x	43.7x	29.5x	61.7x	73.8x
solarwinds	\$17.67	(1.8%)	5,510	7,292	13.1%	7.7%	10.3%	7.6x	7.2x	6.5x	15.9x	15.6x	13.9x	20.8x	20.4x
qualys	\$104.02	20.2%	4,053	3,770	14.9%	11.2%	13.2%	11.3x	10.5x	9.3x	25.4x	24.8x	21.5x	41.6x	41.8x
cyberark	\$99.27	(22.1%)	3,794	3,194	21.1%	5.0%	19.7%	7.2x	7.0x	5.9x	24.6x	34.7x	25.2x	36.6x	53.7x
blackberry	\$4.89	(32.2%)	2,717	2,553	8.7%	(8.1%)	7.8%	2.4x	2.6x	2.4x	17.5x	21.4x	20.6x	34.9x	37.6x
fireeye	\$12.18	(18.2%)	2,713	2,843	7.2%	0.1%	7.2%	3.1x	3.2x	3.0x	23.9x	34.3x	26.4x	NM	57.8x
mimecast	\$41.66	(10.8%)	2,604	2,659	25.4%	15.1%	15.9%	6.2x	5.7x	4.9x	34.1x	28.3x	25.0x	83.3x	66.7x
hpe	\$32.09	113.9%	2,570	2,569	25.6%	0.7%	20.9%	10.1x	10.5x	8.7x	NM	NM	NM	NM	80.3x
sailpoint	\$26.47	32.3%	2,387	2,280	16.4%	9.7%	13.1%	7.5x	7.2x	6.4x	NM	NM	NM	NM	NM
onespan	\$27.93	99.5%	1,126	1,036	22.8%	1.2%	9.3%	3.9x	4.0x	3.7x	25.7x	40.3x	25.5x	40.5x	62.3x
secureworks	\$11.43	(8.8%)	932	805	6.8%	1.4%	6.3%	1.4x	1.4x	1.4x	NM	NM	40.6x	NM	NM
secure	\$3.25	14.3%	513	528	8.9%	0.2%	6.7%	2.1x	2.1x	2.0x	18.4x	18.8x	14.6x	73.2x	71.8x
tufin	\$9.55	(64.3%)	336	241	14.0%	(5.4%)	19.8%	2.4x	2.5x	2.1x	NM	NM	NM	NM	NM
				Mean	15.1%	5.1%	12.7%	6.4x	6.1x	5.4x	23.4x	25.7x	22.1x	44.7x	45.2x
				Median	14.9%	2.9%	13.1%	6.7x	6.1x	5.2x	24.2x	26.0x	23.0x	41.6x	44.8x

Source: Capital IQ. Market data updated as of June 30th, 2020.
Note: NM – Not Meaningful, NA – Not Available. *Price performance from IPO price.

[Return To Table Of Contents](#)

74

Many market observers have been surprised to witness Cybersecurity spending maintain its momentum through the pandemic.

The 6 market leaders are not the only ones affected.

Nineteen other companies have averaged over 12% revenue growth and increased their market share during the COVID-19 lockdown.

We know them well.

Every one of these companies is a client of ours and all have increased their market spend during the last 6 months.

As a result, they've all increased market share too.



CONTENT.

Similarly, content must be relevant to real-world problems.

Much of the content we audit tends to either be overly analytic and full of technical jargon, implying we suppose that the company is to be taken seriously, or vapid and generalized, providing little if any information of value. These appear as if a product team needed to throw something together to satisfy some short term volume goals.

CISOs see through both and if they could, would demand their money back in terms of wasted time.

When supporting a highly technical industry like Cybersecurity, it's easy to get lost in a world of technical jargon, acronyms and covert terminology.

Across many organizations, the temptation is for marketing teams to use “marketing speak” to transform what technical teams create into buzzword bingo. The objective is to appear savvy to readers. It never works.

Real-world case studies are the highest-value and best-performing assets bar none. Brief and to the point, these are easily consumable and shred the available time roadblocks. Going beyond the “our product is awesome” yadayada and demonstrating how you solved a frequent real-life problem and drove results has enormous value.

However, in our world, you will rarely get a chance to share a company's sensitive vulnerabilities and damaging effects by name.

MORE ON. CONTENT.

The good news is that everyone understands this, so anonymized case studies find greater receptivity in these markets and can deliver strong industry and brand adhesion. The trick is in the strength of story, the identification of a narrow industrial classification (e.g. Large Texas Healthcare provider) and quantification of measurable results.

Marketing teams must remember that we are marketing across the entire human spectrum. At CyberTheory we are passionate advocates for D2H (direct-to-human) marketing. While, at times, we need to produce technical data sheets and solution briefs, we also need to communicate with a broad range of consumers, from those in the C-suite to individual buyers.

Engineering documents are completely appropriate for technical departmental influencers as they must make a determination as to the architectural soundness of the product, but content whose purpose is to create intrigue and interest must be designed to incite emotion and curiosity.

Without hyperbole.

As one of our CISOs remarked on a recent marketing leadership panel discussion, “Just tell me what you do and how it benefits me. Drop all the silly-speak”

We have found that the absolute best way to determine whether your content is ringing bells anywhere in your markets is to engage advanced analytics to compare your content performance against market consumption trends and sentiment and your competitors' content performance.

LAST WORDS ON CONTENT.

We run our clients' content out across a range of media publishing and competitor sites against a set of topics and sub-topics to determine gaps in coverage, share of voice and share of engagement.

The results enable corrections for the gaps and white spaces and then we return back to those same domains to assess the efficacy of the corrected content while measuring progress toward market share and competitor dominance.

The beauty of the process is that it completely removes opinion and emotion from the content creation and targeting cycle, replacing it with pure empirical data.

Data never lies.

We call our content analytics engine Darwin as it forces measurement, improvement and evolution, revealing the deficiencies that, if not addressed, will ultimately lead toward less optimum results.

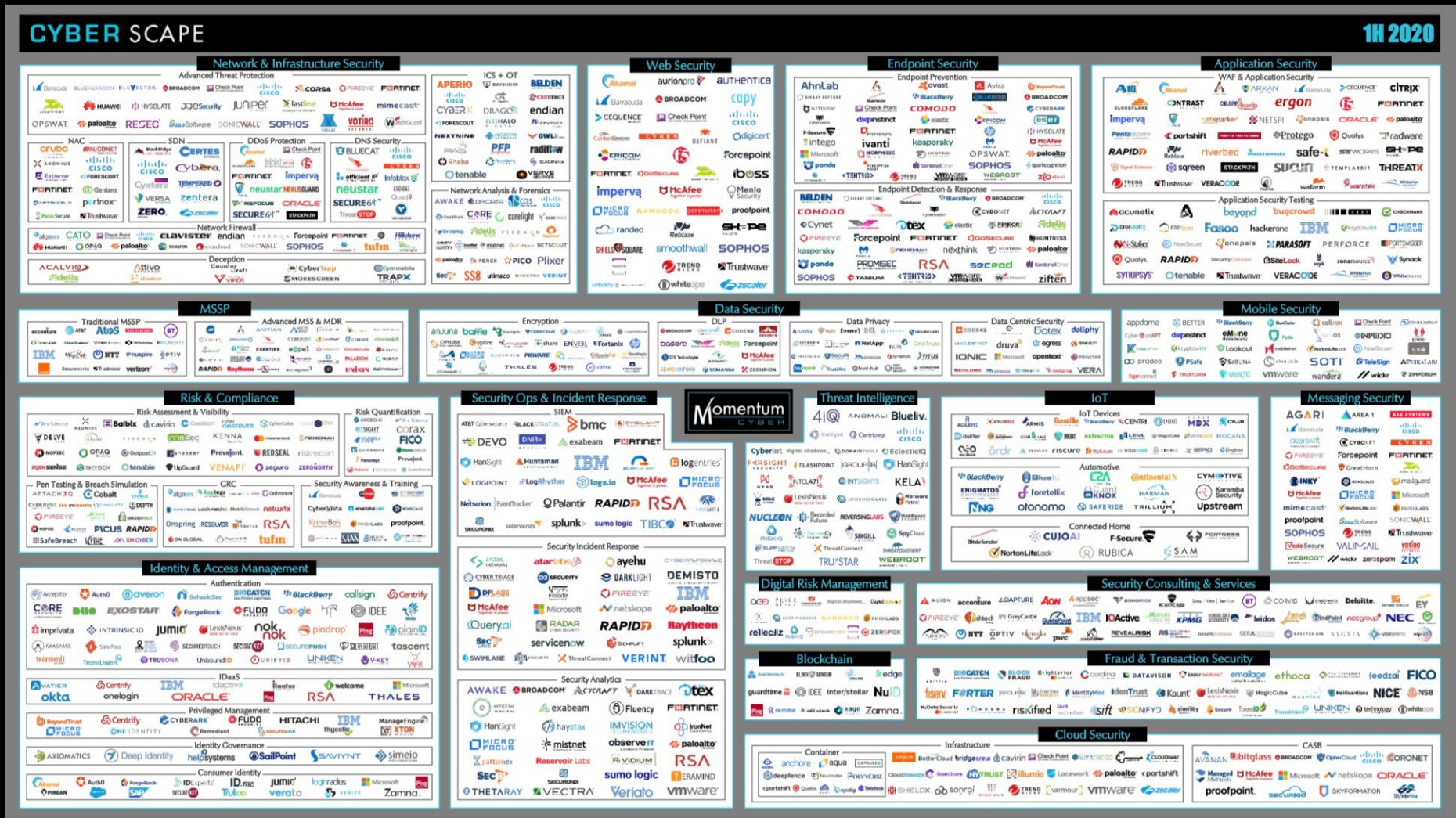
There are over 3,500 Cybersecurity vendors in the market today and dozens of startups are raising substantial seed and A rounds weekly.

Today's wall of noise is challenging to even the most seasoned marketing executives.

Messaging and content matters now more than ever before.

Investing in content that doesn't hit its mark or find resonance with its targets is money poorly spent.

In an era of tight budgets and limited resources, it is critical to get these right.



LEAD GENERATION.

Focusing on CPL as a metric for marketing efficiency is an old school attempt at controlling the costs of raw MQLs.

This practice was based on the correct assumption that raw MQLs had little value as they topped off the lead development process.

They weren't worth very much, so one shouldn't pay much for them.

In the current era, where raw MQLs are able to be enhanced by strong intent analytics and first-party data, these leads have become powerful footprints of intent and those who draw twice in content download send strong intent signals that they are indeed interested in both the topic and, in particular, your company's approach to tackling it.

The current era requires a shift in focus from CPL to ROI.

The point after all is to engineer a leadgen machine that converts rapidly to wins, and the only metric that matters now is revenue conversion and CAC.

In a standard single download content syndication campaign, the average cost of a raw MQL is hovering around \$65. The conversion rate to an SQL for this class of leads is averaging just under 3%. Those conversions lead to an average of 1 appointment for every 5 SQLs or 20% and leads take between 100-150 days to progress through the funnel.

With today's fully burdened SDR costs and performance averages being what they are, when all of the MQL to SQL conversion elements are taken into account, we are approaching very expensive customer acquisition costs and long time frames to get to closed deals.

MORE LEAD GENERATION.

As we head into the last quarter of this year, most clients are seeking lead generation programs that convert in the range of 10-12% and move much faster through the funnel.

Our clients' keys to success with content syndication leadgen campaigns are double touch content, direct dial harvesting, tele verification of intent, effective call scripts, well-trained sales development reps, and an auto-dialing platform that can accelerate outbound calling by 12X.

By taking the broader view that includes speed and runway extension into account, our clients have been able to easily make the ROI case.

The faster an enhanced lead moves to conclusion, the more runway exists for sales conversions.

The more sales conversions, the higher the ROI.

VIRTUAL EVENTS: 1

We have conducted 174 virtual executive roundtable events since the beginning of COVID-19 and have scheduled 96 more for the balance of this year. We have also hosted 11 virtual summits, regularly registering over 1,500 attendees for each.

Virtual events are extremely popular with many marketers who now understand and agree that the remote dynamics actually contribute to their popularity. No need to travel to and from a restaurant or conference facility, wrestle with the challenges of parking and traffic, and contend with the distractions of a physical meeting with peers.

The benefits are myriad and include increased and more focused interaction with peers and industry solution architects, underscoring both the purpose and value of education and continued learning.

Clients who have attempted to produce these events themselves have struggled with both pre- and post-event effectiveness in the areas of generating registrations and attendees, working against short timeframes, underperforming emails and ads, the inability to reach the right audience, and lacking consistent messaging to market the event.

Only 18% of clients claim that they are effective at continuing to generate engagement post-event. Some popular tactics are on-demand recordings, event-specific nurture flows, and repurposed content, but very few clients reported the meaningful engagement with attendees that they had anticipated.

Four in ten say they cannot determine what event content resonated best with attendees and one third admit they lack the right data to effectively measure virtual event engagement at all.

VIRTUAL EVENTS: 2

Most virtual event attendees report that having opportunities to participate and interact with the speakers and other attendees creates an inclination to stay, listen, and engage.

Very few of the CISOs (less than one in ten) we polled report that having virtual booths as a part of an event actually keeps them engaged.

Driving attendance has been the major roadblock for most.

Only a fraction of respondents reported that they had been seeing an attendance rate of more than 75% which is about the same show rate as SDR generated SQL meetings.

Most of the companies that have signed up with us to manage their events claim that the driving factors in their decision are the ability to attract their target audience, producing the event in such a way as to compensate for the absent human interactions associated with in-person events, and managing the mid-event drop-off.

When it comes to the types of events utilized by companies with good attendance rates, the clients enjoying 75% or better attendance rates most often are participating in largescale, multi-vendor virtual tradeshow.

Others who are experiencing success claim their focus has been on small-scale, single-vendor virtual events and webinars that resonate better with today's audiences.

VIRTUAL EVENTS: 3

The bottom line is that the more companies focus on marketing an event to their own audiences, the more registrants they are able to reach, and using co-promotion, our clients are seeing strong turnout for all classes of virtual events.

Not surprisingly, a lack of consistent messaging gets in the way of effectively marketing virtual events.

In addition to challenging timeframes, promotional tactics and reach, high-attendance organizations are finding it difficult to match the messaging with the increased scale, content and volume of registrants common to large-scale events.

The path to success here is to establish a clear set of sharable messaging and branding guidelines well in advance of any pre-event promotion.

Close attention to email and digital ad content is critical to attracting today's event participants who are inundated with invitations.

Differentiation and excitement are keys.

Current event registrants have very different calendars than they did pre-COVID-19.

Gartner | COVID-19's Impact on Security Spend

Like Other Segments Of IT, Security Will Be Impacted In The Near-Term With Most Sectors Rebounding In A Couple Of Years.

- The negative impact of COVID-19 on both supply chain and demand trends has led Gartner to reduce its security forecast for 2020 from 9% to 4% growth
- Some security spending will be supported by the need for remote access:
 - Recommends that any device that is needed for remote access should be configured with an endpoint protection platform (EPP)
 - Cloud-based Secure Web Gateway (SWG) services protect mobile laptops when devices are off the corporate network
 - Interest in Cloud Access Security Brokers (CASBs) will remain intense in a post-COVID-19 world
 - Adoption of multifactor authentication (MFA) will continue



Segment	Impact Of Security Segments		Near-Term	Long-Term	Select Representative Vendors
	2020	2021-2023			
Network Security (Firewalls)	↓	↓	2020 growth affected; demand for VPNs will provide some offset	Demand for remote access will highlight benefits of SDP	CISCO, DREAMWIRE, JUNIPER, PaloAlto
Endpoint Protection Platforms (EPP)	↔	↑	Organizations will seek to connect more remote employees	Integration of EDR will remain significant	Carbon Black, Trend Micro, McAfee, Microsoft
Secure Email Gateway (SEG)	↓	↔	Migration of email to a cloud-based service will continue	Email continues to be the preferred channel for attacks	CISCO, Mimecast, Proofpoint, Symantec
Secure Web Gateway (SWG)	↔	↑	Cloud-based SWGs are beneficiary of the work from home trend	Cloud-based SWGs are at the core of many SASE platforms	BOSS, McAfee, Manta Security, Cloudflare
Security Information & Event Management (SIEM)	↓	↔	Demand strong, however, SIEM projects will be put on hold	SIEM could be impacted by Competitive dynamics of XDR	IBM, Loggly, PAGER, Splunk
Access Management (AM)	↔	↑	Cloud computing has shifted from perimeter to identity context-based	Convergence of AM / IGA / PAM for mid market & expansion of IaaS	Audco, IBM, Okta, Ping
Identity Governance & Administration (IGA)	↓	↑	Complexity and investments could hold up IGA in near-term	IGA-as-a-service has accelerated and expected to become dominant	ORACLE, SAILPOINT, CYBERARK, IBM
Privileged Access Management (PAM)	↔	↑	Demand has been strong due to the increasing number of cyberattacks	Ability to control plane from network to endpoint to identity	PERIOD8, CyberArk, IBM
Data Security	↓	↑	Encryption solutions promise strong ROI with minimal cost; DLP impacted	Encryption embracing cloud / mobile deployment will emerge strong	McAfee, Fidelis, Forcepoint, Thales
Cloud Security	↔	↑	Will see decent adoption to satiate remote workers; see some slowing	Emergence of SASE drives demand; Cloud default starting point for projects	CISCO, McAfee, Netskope, PaloAlto
Application Security Testing (AST)	↓	↑	Additional spending will be delayed for short-term / mid-term	Reliance on online transactions, will prompt buyers to return to the market	OWASP, IBM, PAGER, Synopsys
Web Application Firewall (WAF)	↔	↑	On-Premise slowdown; Increased demand of Cloud WAF for remote users	More organizations expected to look for a cloud-first approach to WAF	Alibaba, Akamai, Imperva
Vulnerability Assessment (VA)	↓	↑	Foundational security process mandated by majority of end-user orgs	Continued migration of VA to the cloud-delivered solutions	NOPSEC, Qualys, RAPID7, Tenable
Integrated Risk Management Solutions (IRMS)	↓	↑	Spending negatively impacted by overall weakness in business environment	Orgs will increasingly take more integrated approach to risk / compliance	BlackBerry, Merckxam, RSA, ServiceNow
Security Services	↓	↑	Services will be weaker on net new deals in the near term	Growth resumes as some orgs replace people that were impacted during crisis	AT&T, IBM, Secureworks, Verizon

Gartner's assessment on sector impact during the pandemic and into the future has some segments declining slightly or remaining even in 2020.

Firewalls, SEGs, SIEMs and the like are predictably not leading market segment growth.

While Endpoint, SWGs, IAM, PAM, Cloud and WAF are holding ground.

The prediction for 2021 and beyond is that every category segment other than Firewalls, SEG and SIEM will grow revenue and increase market value.

Of the 49 companies covered in this report, 49 of them are our customers.



Source: Gartner Invest Series COVID-19's Impact on Security Spend.

[Return To Table Of Contents](#)

COMMUNITY.

Ultimately, the success of our Cybersecurity brands depends on a community of prosumers who see value and want to tell others.

Communities depend on consistency of values, information, education, interests and appetite for action.

While every CISO is focused on solutions to their organizational security challenges, underneath that energy, they all embrace the larger goal of making the Internet and our digital world a safer place, leaving cyberspace better than it was before they got here.

Vendors who achieve a level of partnership with that belief system will find greater receptivity among the CISO community.

As many of our advisory board members have said, vendors who admit that their product or service is not a good fit for a prospect and go on to recommend a different solution earn significant trust and advocacy points among that tribe.

By being good digital citizens and sharing with the community, you may be contributing to the greater good of protecting the world from the next big cyberattack and your reward will likely be priceless word-of-mouth marketing.

SUMMARY.

As Forrester noted in its recent 2021 predictions, business buyers have become more like independent consumers, and “2021 will be a pivotal year as buyers’ demand for a compelling experience increases and B2B marketers strive to get ahead of that demand.”

Cybersecurity buyers are closing more transactions online and dealing less with salespeople, yet at the same time, they want more engagement in their customer experiences, with more relevant content and connection with peers.

We have seen that many of our traditional approaches to Cybersecurity marketing during this pandemic have been challenged.

Persona development has now taken on new characteristics to reflect the increase in market noise and the shifts in business goal alignments.

Market and regulatory changes have accelerated the move toward highly contextual first-party data for more precision marketing insights.

The expansion of the competitive landscape has highlighted the need to adapt our messaging to a more authentic and targeted audience seeking parsimonious and direct communications.

Our content has been challenged.

We have seen market pushback on long-winded technical assessments as our targets have less time and smaller appetites for consumption.

We have less visibility into content relevance and receptivity with fewer resources to help us with analysis.

SUMMARY.

Conventional thrown-over-the-wall leadgen campaigns have increasingly failed to perform and we have continued to address cost efficacy with conventional cpl approaches.

Virtual events have proven hugely popular, yet many companies have unsuccessfully tried to produce and manage these independently and have endured the consequences.

We have begun to appreciate the complexity and depth of well-executed virtual events and the benefits that accrue.

The growth of digitally savvy millennial enterprise decision-makers means that content plans in 2021 will have to be more on point and more personalized than ever, speaking to a particular use case and audience, and delivered in the right format and at the right moment.

Community matters.

Besides being more skeptical about product claims, this generation also comprises purpose-based buyers who will choose brands that reflect their values and expect their employers to do the same.

The Cybersecurity technology community trusts one source of information over anything else: their peers.

Sophisticated marketers must go all the way down to their client's end-user customers in order to build brand champions.

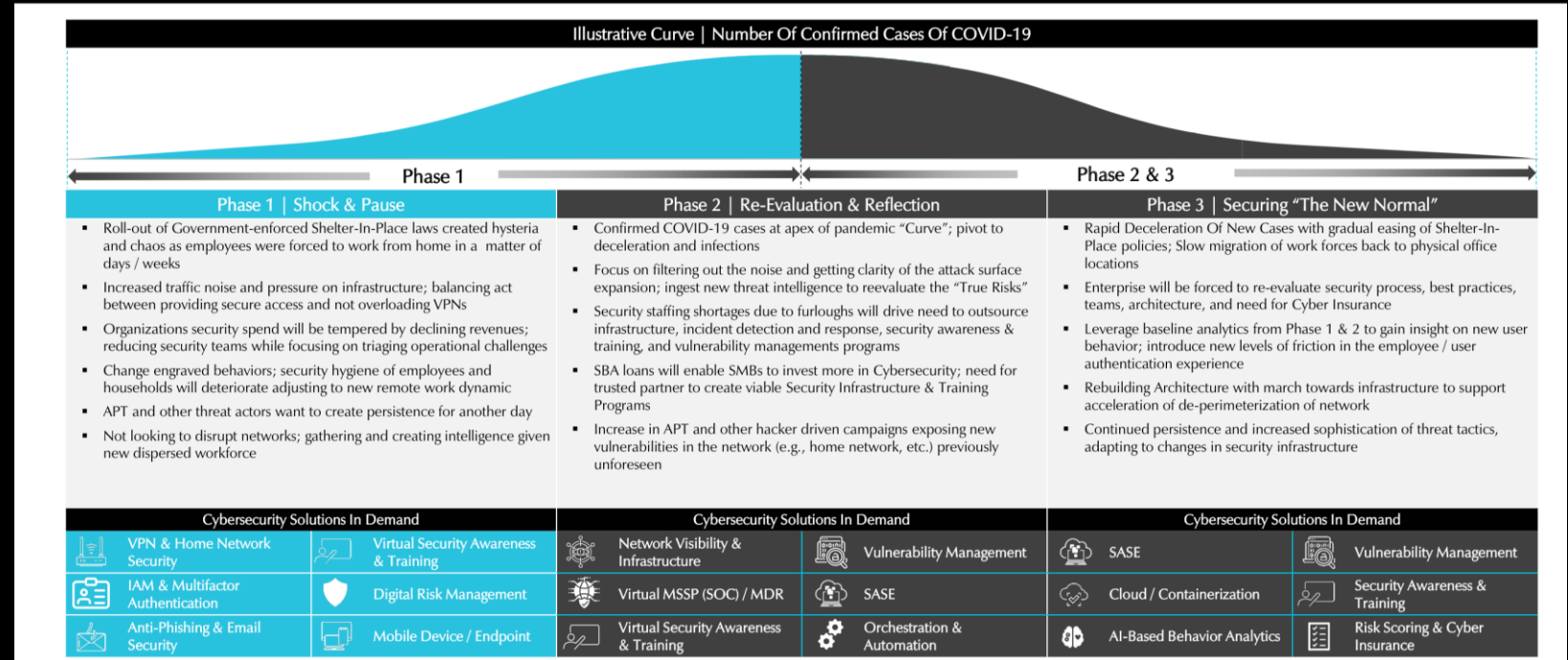
Mapping the impact of COVID-19 across the threat landscape in multiple stages, we can see the transition from early infrastructure pressure to attack surface expansion to rebuilding architecture toward permanent boundariless networks.

Marketers who are able to map the messaging and content for their product and service offerings to evolving changes in demand will be able to succeed against rapidly shifting contours.

How we communicate with our target audience will be critical to segment share growth over the next 24 months.

Webcast Highlights | The Evolution Of Cybersecurity During The Pandemic

Cybersecurity Is Mission Critical; Securing Business Continuity And Connectivity Going Forward.



[Return To Table Of Contents](#)

CONCLUSION.

Marketers who can ...

1. adapt to the true influencer persona in addition to the CISO,
2. empower first-party data in their campaigns, personalizing outreach and messaging,
3. labor over their messaging to assure authenticity and resonance with their target audience,
4. adopt analytics and advanced technologies to optimize and continuously improve content,

5. accelerate their pipeline and model their leadgen strategies around total ROI,

6. partner with Cybersecurity media firms with trusted member networks to manage events, and

7. appeal to the community interests of the target audience through noble-purpose selling,

... will be in the best position to capture and retain market-leadership in 2021.

All of the claims and results presented in this research report are available upon request – all charts are from the Momentum 1st Half Cybersecurity Market Review Report.

ABOUT CYBERTHEORY.

CyberTheory is a full-service cybersecurity marketing advisory firm, providing advertising, marketing, content, digital strategy, messaging, positioning, event management and media publishing.

We deliver innovative demand generation programs with extremely high conversion rates.

In addition to our resident CISO team and Customer Advisory Board, our extensive knowledge model allows us personalized targeting of each and every Cybersecurity buyer persona.

With strategic insights from global education services, media providers, intelligence analysts, journalists and executive leaders, we're always aligned with the latest industry direction and future trends.



MARKETING CONNECTED TO REVENUE

(212) 518-1579 • info@cybertheory.io
530 7th Avenue, New York, NY 10018 • www.cybertheory.io

