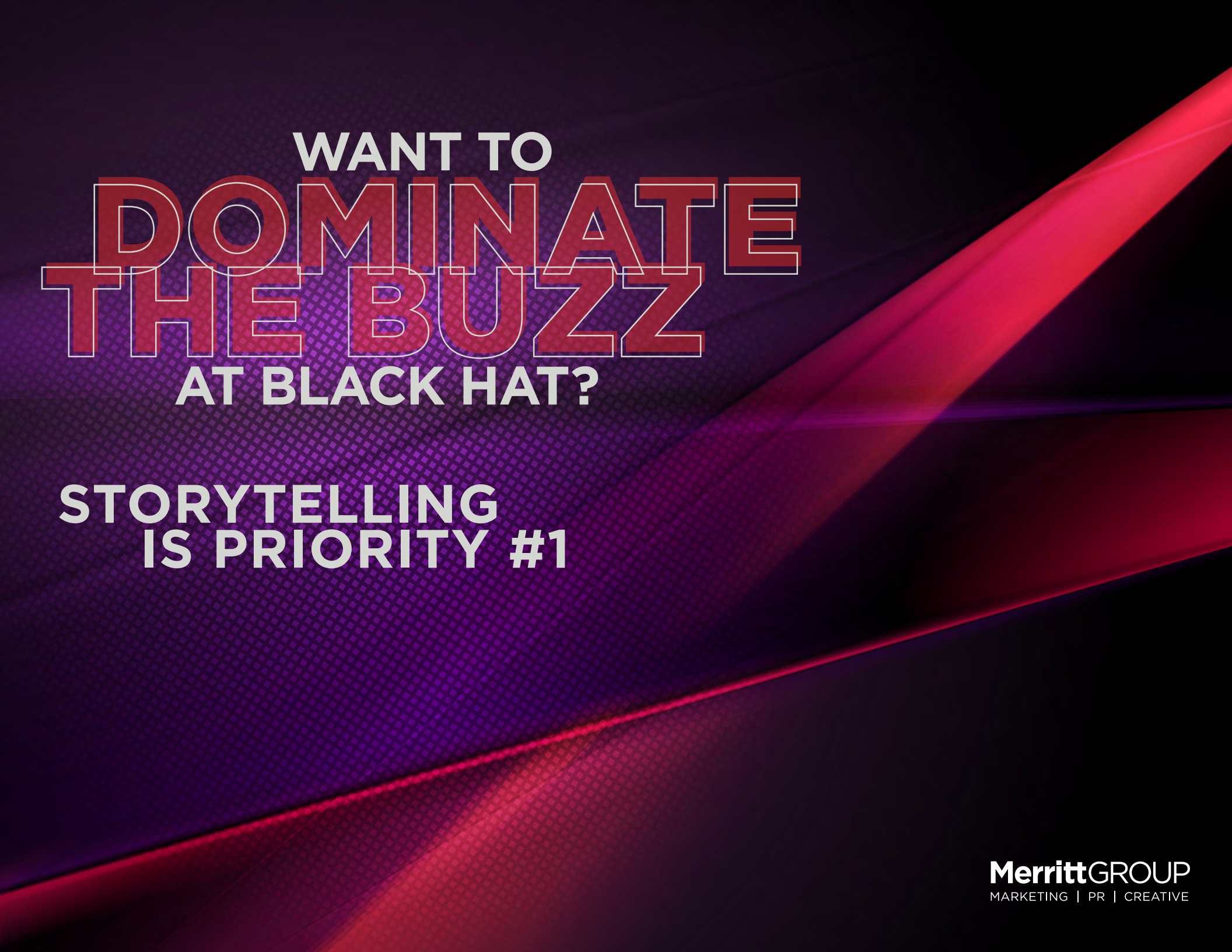

WANT TO
DOMINATE
THE BUZZ
AT BLACK HAT?
STORYTELLING
IS PRIORITY #1
MerrittGROUP
MARKETING | PR | CREATIVE

Anyone who has walked the show floor at Black Hat knows how immense and noisy the cybersecurity industry has become. **Last year alone**, more than 300 vendors exhibited at the show, and nearly 19,000 security professionals journeyed to Las Vegas for a week of learning, networking and well, exhaustion. In comparison, the 2016 show brought in about 15,000 attendees, showcasing the rapid growth across the industry.

Despite the overwhelming attendance and chatter surrounding Black Hat, the show is actually just a small fraction of the broader momentum happening in the cybersecurity industry. **According to Cybersecurity Ventures**, the cybersecurity market grew by roughly 35X over the past 13 years, and, **according to MarketWatch**, the market is expected to reach $300 billion by 2024. In comparison, the global AI market is only **expected** to reach about $71 billion by the same year... Let that perspective sink in.

So how can marketers at security vendors break through the noise to get a high level of awareness that will reach their audiences? It's simple: effective storytelling. To uncover what's been driving conversations within the industry since Black Hat 2018, Merritt Group's Security Practice conducted the following research and analysis, highlighting top reporters, publications and shared content. Taking this all into account, we highlight some best practices to stand out in this crowded marketplace along with some input from industry insiders and more.

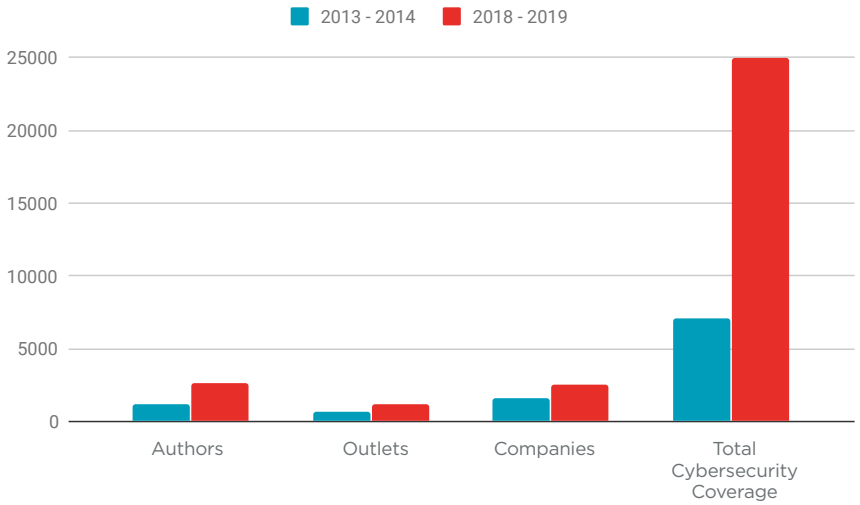
"...the market is expected to reach $300 billion by 2024."

KEY FINDINGS FROM OUR ANALYSIS

- The buzz in the cybersecurity industry has reached deafening levels as the volume of **overall cybersecurity media/blog coverage increased a whopping 352 percent over the past five years** (24,975 placements from May 2018-May 2019 compared to 7,091 placements over the same period 2013-2014).

- Likewise, **the number of media outlets and blogs covering cybersecurity increased by a massive 214 percent** (2633 compared to 1233) during the same time period. Not surprisingly, **the number of reporters/authors writing on the topic jumped 185 percent** (1149 compared to 62) and the volume of companies mentioned in cybersecurity surged by 161 percent (2501 compared to 1557.

- **The top four companies with the most buzz in cybersecurity - determined simply by their volume of press coverage over the past 12 months - only account for 13 percent of total coverage on the topic collectively over the past year.** This means there is significant opportunity for cybersecurity vendors looking to join the cybersecurity conversation. That said, content-focused companies like CrowdStrike regularly churn out unique research and dominate the headlines, so similar vendors looking to break out need to have clear-cut messaging that addresses white space in the market and a dominant content strategy.



- **Nearly all of the 20 most shared articles over the past year fell into two buckets**: 1) politically charged conversations around election and national security and 2) breaches or vulnerabilities that had a significant impact for the everyday individual (i.e. Facebook leak, fake cancer scans created by malware, etc.)

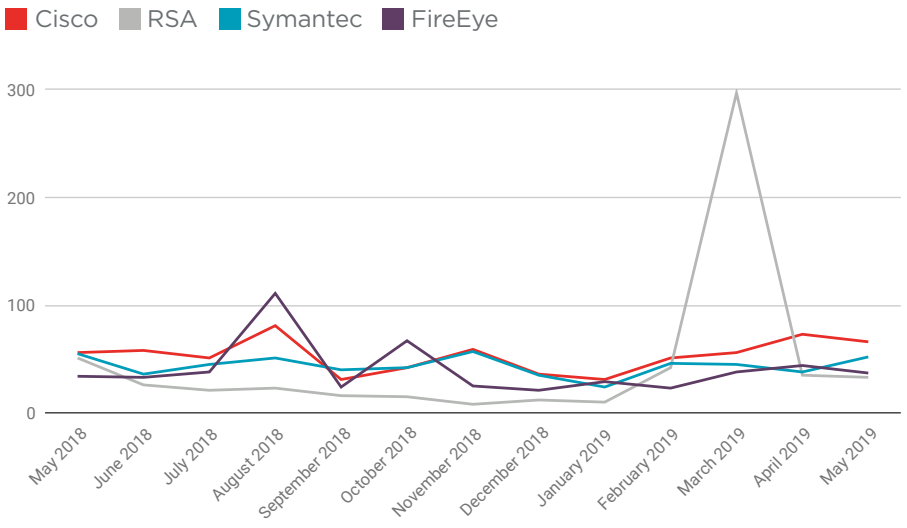
- When it comes to volume of press buzz, the trades of course dominate, as well as media that produce daily cybersecurity newsletters. Given the sheer number of attacks, vulnerabilities, discoveries and the like, many of these stories are brief summaries of who, what, where, when and why, rather than deep dives or investigative reports. **The most shared content come from the business press as these are a more in-depth analysis into the impact and implications of the hack of the day, with emphasis on why it matters.**

FOOTNOTE: This analysis was conducted using **TechNews** *and details U.S. coverage date from May 1, 2018 to May 31, 2019. It does not include analyst reports.*

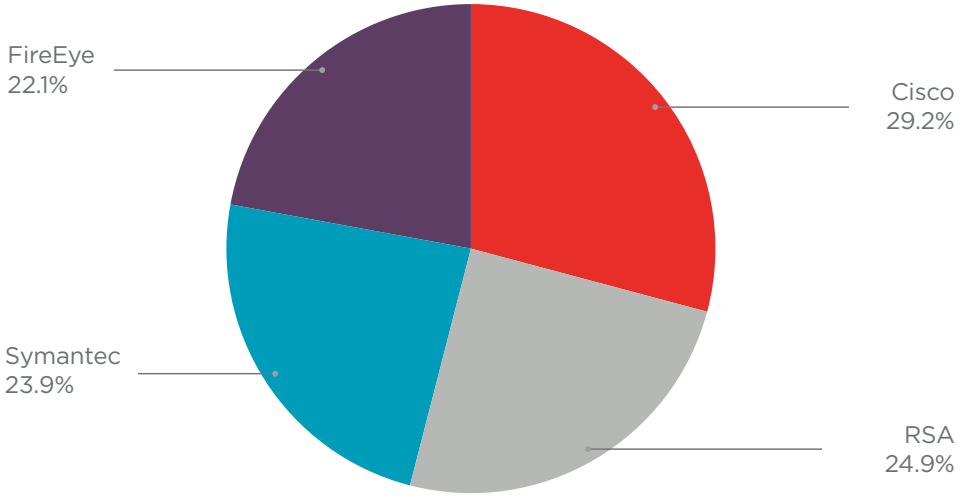
TOP CYBERSECURITY VENDORS

CISCO
RSA
SYMANTEC
FIREEYE

MONTHLY MEDIA COVERAGE:
TOP FOUR CYBERSECURITY COMPANIES



MEDIA COVERAGE SHARE OF VOICE:
TOP FOUR CYBERSECURITY COMPANIES



TOP CYBERSECURITY VENDORS

- Cisco tends to get a lot of attention for the compelling and mainstream nature of the initiatives they undertake. For instance, they made the headlines around their call for governments and citizens around the world to establish privacy as a fundamental human right in the digital economy, their partnership with USGA to conduct the world's first large-scale trial of Wi-Fi 6 services at the US Open and their efforts to connect astronauts and other space pioneers via webex to the official Apollo 50th Anniversary Gala at the Kennedy Space Center Visitor Complex in Florida.

- Cisco Talos Security Intelligence and Research Group findings also drive coverage for the company, with the "VPNFilter" botnet discovery in May 2018 generating a flurry of articles at the time reported and a year after in top tier and security trade publications like *Krebs on Security, Washington Post, Ars Technica CyberScoop, ZDNet, Wired, Daily Beast, Slate*, and many more. Talos regularly reports on newly discovered vulnerabilities and their Talos Intelligence site is cited by security and mainstream business publications alike.

- In June 2018, Cisco also issued a "Small and Mighty" Cybersecurity Special Report exploring threats and security best practices for small and mid-market businesses which was cited by publications like *SecurityWeek, Dark Reading* and more.

- The company was also cited numerous times surrounding the Huawei controversy since Cisco accused Huawei of intellectual property theft back in 2003. Their association with Huawei generated quite a bit of coverage over the past year.

- In May 2019 of this year, Cisco made the headlines in a negative manner after the company issued firmware releases to address a vulnerability to patch a firmware bug, with key security publications like *ThreatPost, CyberScoop, InfoSecurity* and more.

- Cisco is a press release juggernaut, generating and releasing 7-9 announcements per month on average. News is generally corporate in nature, pertaining to earnings, personnel and partnership announcements, product news, CSR initiatives, acquisitions and events. For instance, over the past year, Cisco announced a partnership with Telenor Group to collaborate on cloud, security and Open vRAN for 5G and with the Government of Colombia to develop a cybersecurity workforce for local communities and businesses.

- Given its suite of solutions, the company is very vocal on issues such as cloud security, IoT and the challenges and possibilities of 5G. They've also been at the forefront of data privacy discussions, urging the U.S. government to develop a US federal privacy law that assures customers their data is protected.

RSA

TOP CYBERSECURITY VENDORS

- For context, RSA's placement in this group is largely due to their involvement in the RSA Conference held each year in San Francisco and their other conferences. Each year, the company sees a spike in coverage in the months ahead and weeks following the main event, as the thousands of vendors who flock to Moscone promote their solutions and reporters share key takeaways from the sessions.
- More generally speaking, RSA is pushing a larger message around "business driven security" and this theme carries through the website, blog and media coverage.
- The company does not put out a lot of news and does not engage in a lot of proactive PR. In the past year, they have issued only 7 press releases which have mainly been around analyst reports, events, executive hires and product updates.
- That said, in February 2019, RSA partnered with YouGov Plc on a 6,000 respondent survey exploring ethical data use and data privacy. The research garnered coverage in *Forbes* and a range of security trades. They also issued another survey in April examining the social media platforms that cybercriminals use. The 2019 Current State of Cybercrime report from RSA Security, was covered by publications such as *CNET* and *Forbes*.
- RSA operates 3 separate blogs and pushes a fair amount of content. The blogs focus on cybersecurity fundamentals, executive point of views (POVs) and threat intelligence updates from RSA's research team.
- One successful campaign was around their Cyber SOC set up and they were able to secure a feature on *Reuters TV*, examining open network traffic from show attendees, in addition to a spike in coverage in March due to the RSA conference. The company's CEO did a fair amount of interviews on his keynote and the future of digital risks and was featured on *SiliconANGLE's* "TheCube" video.
- Additional coverage resulted from announced updates to the Netwitness and Archer offerings, as well as a push around holiday fraud and predictions that netted a few feature stories earlier in the year.

TOP CYBERSECURITY VENDORS

- Company announcements have been a large coverage driver for them over the past year with announcements including 3 acquisitions (Appthority, Javelin and Luminate Security) and Symantec being a contender for Thomas Bravo's search to acquire a new organization. In a more negative breadth, there was a good amount of coverage surrounding hits taken by the company, such as, 3 C-level executives leaving amidst big changes from the CEO, the CEO unexpectedly leaving the organization just 6-months after this and a lawsuit against Symantec filed by NSS Labs.
- Less surprising, another major news driver has been their original research with topics surrounding several key verticals and topics, such as financial attacks being on the rise in 2018, an increase in ICS attacks and various reports on differing aspects of healthcare security. Additionally, Symantec produced numerous reports that uncovered bad actors and attacks as well as detailed pervious major attacks - included in these were the Whitefly attack on SingHealth, attacks by Gallmaker against diplomatic and military actors, the SamSam ransomware and WannaCry to name a few. They have also had a vetted focus on nation-state attackers with coverage surrounding China cyber espionage attacks on both the telecoms market and their theft of NSA tools and North Korea's attacks on our ATMs.
- Extensive amounts of coverage surrounded their new products to address trending threats. Over the past year this has included, an AI-powered cyber platform, cloud protection services, end-point services and a GDPR compliance tool. In addition to initial announcements surrounding this news, they have been major players in many trend pieces and breaking news surrounding each of these topics.
- Symantec has been a major voice surrounding the U.S. election security since the midterms last year became a point of conversation, launching a service to guard campaign websites against hackers for free, discussing the DNC breach, and all threats associated with the 2020 elections.
- Additional coverage of note surrounded Symantec joining the Department of Defense's cyber threat sharing program, the spike in supply chain attacks, the skills gap and women in cyber, IoT, and cyber being a C-suite issue not something just for IT to worry about, as well as inclusion on several "companies to watch" or "top products" lists.

FIREEYE™

TOP CYBERSECURITY VENDORS

- Major coverage drivers were a number of high profile research reports, their investigations team's work in a number of high-profile breaches and their acquisition of Verodin.
- The Verodin acquisition was covered very positively by a wide range of top tier business and tech/security trade press. The size of the acquisition was somewhat substantial ($250M) but followers saw Verodin filling a key need for FireEye in their toolset. Given their financial performance, FireEye also garners a lot of corporate coverage in the financial press like *CNBC*.
- Not surprisingly, they drove a large amount of their coverage based on the work of their research team's reports on the following. While the company's release of these reports spawned a spike in coverage, they continue to be referenced in related coverage which creates a "long tail" effect in the company's thought leadership coverage. This coverage mainly appears in the trades but also bubbles up to top tier publications such as *The Washington Post, Wired* and more.

    - Triton ICS Malware
    - A new Iranian hacker group tied to fraudulent Facebook accounts. Facebook later removed these accounts, which drove a lot of top tier coverage.
    - DNS hijacking from a Middle East group
    - A hacker group in Russia targeting the European elections
    - Fake social media accounts that were setup for candidates in the 2018 U.S. midterm elections.
    - New APT targeting telecom and travel companies
    - APT groups in China and Vietnam.
    -Ryuk ransomware

- Their investigative unit, Mandiant, is covered whenever they are involved in the aftermath of a major breach. Among others, the Caribou payment breach was one that stood out during this time period.
- The company has a heavy focus on the channel with channel-focused news announced during the quarter as well as the CEO doing a big Q&A feature with *CRN*.
- Securing validation for their technology strategy is a focus with awards/listings by SC Awards, CRN's 10 Hottest Threat Intelligence Platforms, CRN's Channel Madness Championship and more.
- *Cyberscoop*, *Dark Reading*, *SC Magazine*, *CRN* and *POLITICO* covered the company the most during this time period (10+ times each) however, the company gets regular attention from the top tiers who covered the company at least 4 times during this time including *Wired*, *The Washington Post*, *Fortune* and more.

TOP 20 REPORTERS & PUBLICATIONS

REPORTERS
Ben Canner, Solutions Review
Info Security Editors, Info Security
Ed Buzz, Information Security Buzz
David Marshall, Vmblog
Jane Edwards, GovConWire, Executive Biz, ExecutiveGov
Tim Starks, Politico Morning Cybersecurity
Joseph Marks, The Washington Post
Michael Vizard, DevOps.com, IT Unmasked, Container Journal, Security Boulevard, SmartMSP, The Channel Happy Hour, Futuriom
Edward Gately, Channel Parners, Channel Futures
Sean Lyngaas, CyberScoop
Doug Olenick, SC Magazine
Derek B. Johnson, Federal Computer Week, Government Computer News
Loren Bline, Intelligence Community News
Michael Novinson, CRN
Jessica Davis, Health IT Security
Fred Donovan, Health IT Security and Health IT Infrastructure
Marianne Kobalsuk McGee, HealthInfoSecurity.com
Brenda Marie Rivers, GovConWire, Executive Biz, ExecutiveGov
Nichols Martin, GovConWire, Executive Biz, ExecutiveGov
Joe Panettieri, ChannelE2E

PUBLICATIONS
Solutions Review
Info Security
ExecutiveBiz
SC Magazine
CyberScoop
NextGov
ExecutiveGov
TechRepublic
Federal Computer Week
Information Security Week
Vmblog
FederalNewsRadio.com
Security Boulevard
CRN
Dark Reading
CNET News
Investor's Business Daily
HealthcareInfoSecurity.com
Politico Morning Cybersecurity
GovConWire

FOOTNOTE: This analysis was conducted using ***TechNews*** *and details U.S. coverage date from May 1, 2018 to May 31, 2019. It does not include analyst reports.*

TOP 20 ARTICLES

With the whirlwind year we've had, it's no surprise that election security dominated the cyber headlines over the past 12 months. In fact, **a *PBS* article** from August of 2018, reporting that an 11-year old boy was able to change election results on a replica Florida state website, received roughly 1.1M total engagements, according to Buzzsumo analytics. But alongside these stories was a constant stream of breach-of-the-day headlines that, aside from a few stand outs, tend to blend together. Among those was the seemingly endless stream of news surrounding privacy concerns and vulnerabilities with social media giant, Facebook. One ***New York Times* article** in particular from September of 2018, which detailed the breach that exposed the personal information of nearly 50 million Facebook users, received over 144K total engagements. Additionally, major business focused outlets, such as *NBC*, *CNBC* and *The Washington Post*, and security trade publications, including *ZDNet*, demonstrated high levels of engagement for stories relating to the Trump administration's cybersecurity strategy and various breaches; including WhatsApp, Marriott, and the Google Plus bug.

TITLE	PUBLICATION
An 11-year-old changed election results on a replica Florida state website in under 10 minutes	PBS
Donald Trump Saves Aircraft Carrier, Ignoring Navy Advice	Time
Facebook Security Breach Exposes Accounts of 50 Million Users	The New York Times
Jared Kushner's Using WhatsApp for White House Business is 'Far More Egregious' Than Hillary Clinton's Emails, Cybersecurity Expert Says	Newsweek
Inmates hack prison tablets, transfer nearly $225k into own accounts	AJC
A mysterious grey-hat is patching people's outdated MikroTik routers	ZDNet
Hillary Clinton Accepts Role Teaching About Cybersecurity	Western Journal
Trump admin has no central strategy for election security, and no one's in charge	NBC News
Hospital viruses: Fake cancerous nodes in CT scans, created by malware, trick radiologists	The Washington Post
Google did not disclose security bug because it feared regulation, says report	CNBC
The hacking threat to the midterms is huge. And technology won't protect us.	Vox
Microsoft says it has found a Russian operation targeting U.S. political institutions	The Washington Post
Facebook hack exposed 50 million users' info — and accounts on other sites	CNN
China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare	The Washington Post
Porn-Watching Employee Infected Government Network with Russian Malware, IG Says	NextGov
Russian Hackers Apepar to Shift Focus to U.S. Power Grid	The New York Times
New Russian Hacking Targeted Republican Groups, Microsoft Says	The News York Times
Facebook discovered 'security issue' affecting 50 million accounts	CNBC
Someone is trying to take entire countries offline and cybersecurity experts says 'it's a matter of time because it's really easy'	Business Insider
Minister in Charge of Japan's Cybersecurity Says He Has Never Used a Computer	The New York Times

FOOTNOTE: This analysis was conducted using BuzzSumo.

INSIDER INSIGHTS
FROM TOP SECURITY PRESS

When breaking news happens, it's frustrating that so many vendors send us comments without having direct knowledge of the news event. So the sources that are most credible are those who have direct knowledge of a particular threat/exploit/issue...We aren't as interested in "visionaries" as we are in sources who have hands-on, practical experience with a particular threat, issue, or best practice."

- Tim Wilson, *Dark Reading*

Breaking news is awesome and very much the priority if it's a story CyberScoop is breaking. If it's big news that's already out there we often need to crank something out just to get it on the site, while trying to differentiate coverage, and then think about how to make a more nuanced story happen. **Longform stuff is the ideal, and it's typically the organic result of conversations with interesting researchers, but the challenge is finding time."**

- Jeff Stone, *CyberScoop*

7 TIPS FOR STORYTELLING SUCCESS

In a highly crowded marketplace with incredibly dynamic media cycles, it is a daunting task to break through the noise that is the cybersecurity industry. Here's the good news: the top five companies covering cybersecurity only account for a portion of total coverage on the topic, meaning there is ample opportunity to become a part of the conversation. That said, unique story development is critical and companies looking to join the fray need to have clear-cut messaging and a compelling narrative to have a shot to gain a share of voice.

Enter: Merritt Group's Recipe for Storytelling Success. Our tried and true approach to storytelling is key given today's media landscape and includes seven critical considerations:

1. Establish a Clear Purpose & Goal: Tell stories that matter to the market/society to compel your audience to engage from the first word/image on.
2. Foster Human, Emotional Connections: Establish a protagonist and intimately understand the needs and motivations of the target buyer.
3. Find the Friction & Surprise: Explain who the "good" and "bad" guys are, the challenges that need to overcome, what's holding them back and how success can be achieved.
4. Have an Opinion & Unique POV: Be bold and put a stake in the ground around a topic, and then back it up with facts and other validation points.
5. Use Data-Driven Storytelling: Leverage custom-data sources to pull unique insights that can validate your story and provide a visual voyage.
6. Paint a Picture: Show and tell by using visual storytelling to engage with your audience. Provide a visual voyage and engage audiences with digital content you can touch, pinch, scroll and zoom.
7. Gain the Trust of Your Audience: Nobody wants to feel "messaged" to. The brand voice must be authentic and not overpromise.

Merritt Group understands your marketing, content and PR challenges. More importantly, we have the deep cybersecurity expertise to develop a clear, cohesive story that can elevate your brand and delivers the high-impact awareness you need that feeds the top of your sales funnel. Learn more about how we've created compelling stories and amped up awareness for security vendors **here** and contact us for a complimentary awareness audit to learn more.

MerrittGROUP

MARKETING | PR | CREATIVE