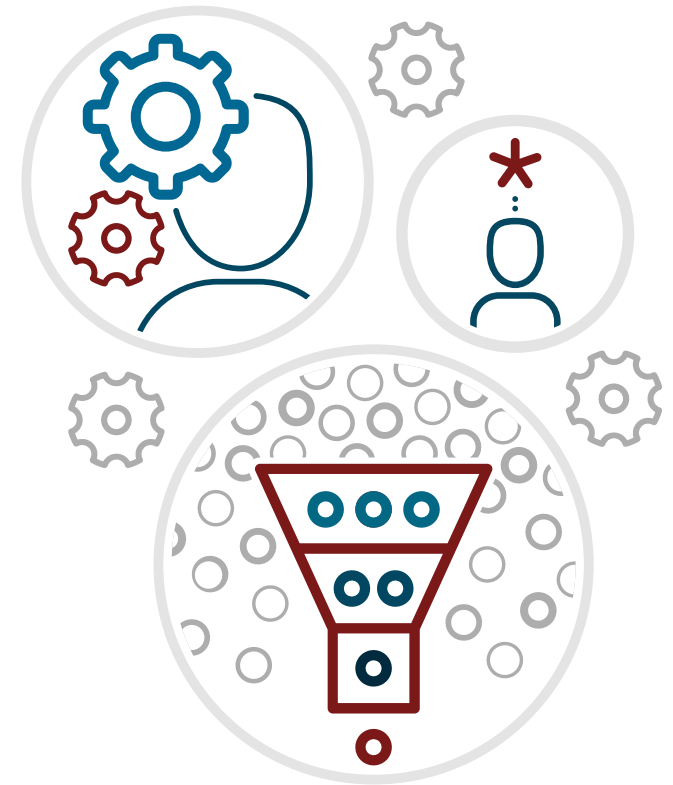




# TechTarget and WhiteHat Security: More Effective ABM Using Advanced Account Insights

As presented by Beth McCullough, former Director,  
Demand Generation at WhiteHat Security  
August 2017



## Who is WhiteHat Security?



Founded  
**2001**



**320+**  
Employees



**150+**  
Security Experts



**800+**  
Active Customers



**50,000+**  
Applications



**92 Million+**  
Attack Vectors Detected

Founded in 2001 and based in Santa Clara, California, WhiteHat Security offers application security for small and enterprise customers. They have over 800 active customers and 320 employees, including 150+ application security engineers who monitor clients' security vulnerabilities, alert clients and recommend how to prioritize them.

WhiteHat's ABM journey has consisted of a hybrid approach, with more of a traditional demand gen model.

## WhiteHat Security: Why should we play the ABM game?

- Learned that we sell to specific accounts better than others
- Have solid demand gen in place, but can only scale to a point
- To better organize our Sales and Marketing gaps
- Shift to digital transformation from a cost perspective



ABM takes time, and it's a commitment.

WhiteHat began the process by considering their business as an end-to-end process, from demand gen through to closed won/closed loss. They compared themselves to peers, conducted benchmarks, reviewed their ideal customer profile and reviewed their top industries, geographies and personas. They also needed to better align Sales and Marketing.



## Spring Training

**Spring 2016 WhiteHat had its ABM team “train up” on what ABM entailed and how we could get in the game.**

WhiteHat decided to add ABM in early 2016. During their “spring training,” their marketing team attended several conferences, which gave their core ABM team an opportunity to do research, identify a framework and figure out the best way to start. They consulted with dozens of martech vendors and conducted intensive data analysis before finally jumping in.

## Early Strikeouts

**Accounts Selected the  
“old way”**

**Start playing before the  
field is ready**

**Creating the lineup takes  
more time than expected**



There were some early “strikeouts.” Initially the field wasn’t ready, and too many accounts per vertical had been selected. They eventually categorized their accounts in three categories:

- A. Top accounts per vertical
- B. Mid-level enterprise and small/mid-sized accounts
- C. Everything else. These accounts were still marked as ABM but didn’t get as much personalization and follow-up.

They also launched an outbound email marketing for air cover. They collaborated with Product Marketing to develop specific content that would appeal to the identified personas and with the sales development reps (SDRs) to determine how best to structure the program.

## Determining WhiteHat's Batting Order

**Start small with the first vertical**

**Marketing air cover**

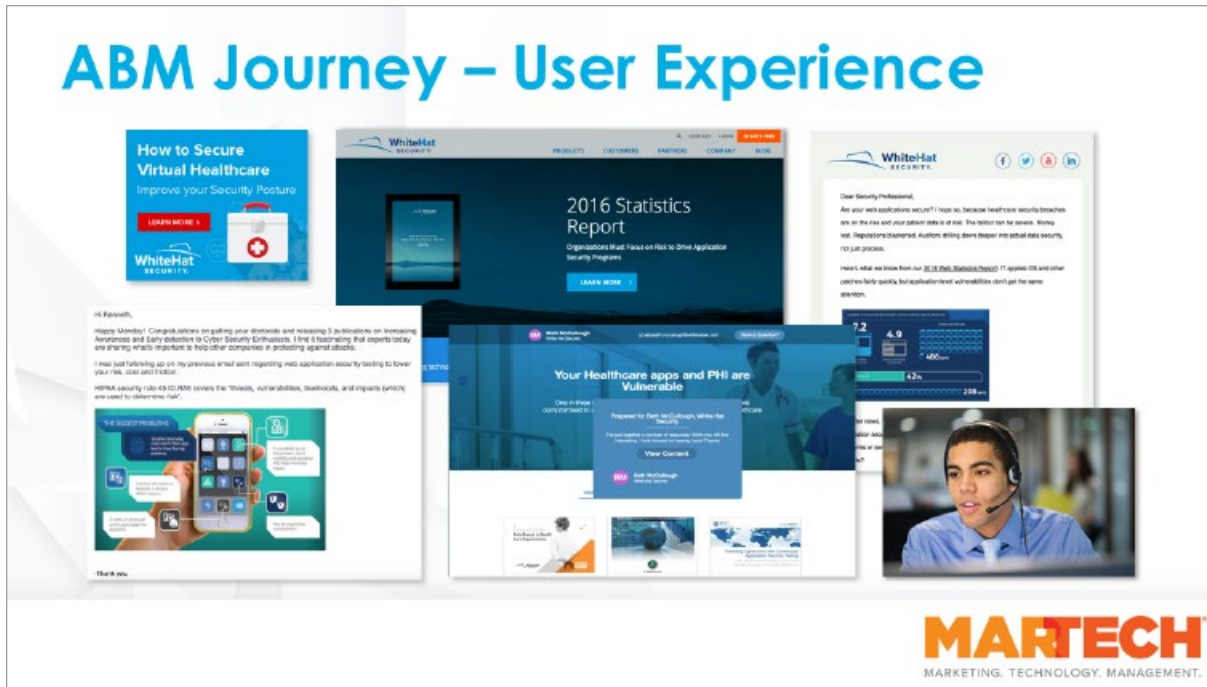
**SDR follow-up**

**Tried different plays to see what might work**



WhiteHat then needed to execute and determine their “batting order.” They started by finding whatever insights they could about different contacts in their verticals. They pulled that data from TechTarget’s Priority Engine™ to see what these accounts were looking at and what insight that gave them. They created custom fields in Salesforce to track the targeted ABM accounts at the account level vs. the lead level. They also worked to set up KPIs with the SDR team around follow-up with these accounts.

## ABM Journey – User Experience



The collage illustrates the user experience for WhiteHat Security's ABM campaign. It includes:

- An email titled "Happy Monday! Check out our getting your devices and receiving 3 notifications on increasing Awareness and Early Detection in Cyber Security Operations. Find 8 fascinating real opportunities and sharing what's important to help other companies in protecting against attacks."
- A landing page titled "How to Secure Virtual Healthcare" with the subtext "Improve your Security Posture" and a "LEARN MORE" button.
- A report titled "2016 Statistics Report" with the subtext "Organizations Must Focus on Risk to Drive Application Security Programs" and a "LEARN MORE" button.
- A social media post titled "Your Healthcare apps and PHI are Vulnerable" with the subtext "One in Five Outpatient Sites" and a "View Content" button.
- A social media post titled "Dear Security Professionals, Are your web applications secure? I hope so, because healthcare security breaches are on the rise and your patient data is at risk. The risk can be severe. Money isn't the only concern. Auditors bring down doors faster than actual data security, too. Let's discuss."
- A social media post titled "Here's what we know from our 2016 Data Breach Report: IT spends 10% and other departments barely qualify, but regulatory fines and penalties can get the same amount."
- A social media post titled "Hi Randall, I may just be following up on my previous email sent regarding into application security testing to lower your risk, cost and friction. HIPAA security rule 45 CFR 164.312 covers the "technical, non-technical, hardware, and all impacts (policy) are used to determine risk."
- A social media post titled "The 5 most vulnerable..." with a list of vulnerabilities.
- A social media post titled "Thank you..."
- A social media post titled "Presented by Dan, Jay, Colleen, White Hat Security" with a "View Content" button.
- A social media post titled "One in Five Outpatient Sites" with a "View Content" button.
- A social media post titled "Your Healthcare apps and PHI are Vulnerable" with a "View Content" button.
- A social media post titled "Dear Security Professionals, Are your web applications secure? I hope so, because healthcare security breaches are on the rise and your patient data is at risk. The risk can be severe. Money isn't the only concern. Auditors bring down doors faster than actual data security, too. Let's discuss."
- A social media post titled "Here's what we know from our 2016 Data Breach Report: IT spends 10% and other departments barely qualify, but regulatory fines and penalties can get the same amount."
- A social media post titled "Happy Monday! Check out our getting your devices and receiving 3 notifications on increasing Awareness and Early Detection in Cyber Security Operations. Find 8 fascinating real opportunities and sharing what's important to help other companies in protecting against attacks."
- A social media post titled "I may just be following up on my previous email sent regarding into application security testing to lower your risk, cost and friction."
- A social media post titled "HIPAA security rule 45 CFR 164.312 covers the 'technical, non-technical, hardware, and all impacts (policy) are used to determine risk.'"
- A social media post titled "The 5 most vulnerable..."
- A social media post titled "Thank you..."
- A social media post titled "Presented by Dan, Jay, Colleen, White Hat Security"
- A social media post titled "One in Five Outpatient Sites"
- A social media post titled "Your Healthcare apps and PHI are Vulnerable"
- A social media post titled "Dear Security Professionals, Are your web applications secure? I hope so, because healthcare security breaches are on the rise and your patient data is at risk. The risk can be severe. Money isn't the only concern. Auditors bring down doors faster than actual data security, too. Let's discuss."
- A social media post titled "Here's what we know from our 2016 Data Breach Report: IT spends 10% and other departments barely qualify, but regulatory fines and penalties can get the same amount."

**MARTECH**  
MARKETING. TECHNOLOGY. MANAGEMENT.

They started by focusing on the healthcare vertical. Marketing touches included an online ad as “air cover” to build awareness of WhiteHat. The ads linked to a personalized website with statistics targeting that audience.

Users who were already in their existing database as a contact saw outbound emails explaining the importance of why someone in healthcare should be concerned with web application security. SDRs reached out with targeted and more personalized emails—which drove contacts to a content board with specific healthcare vertical content—and follow-up calls. With ABM, there are multiple buyers at an account, so the SDRs looked for all the possible members of that buying team.

## Reading the Right Signals

**Who knows us?**

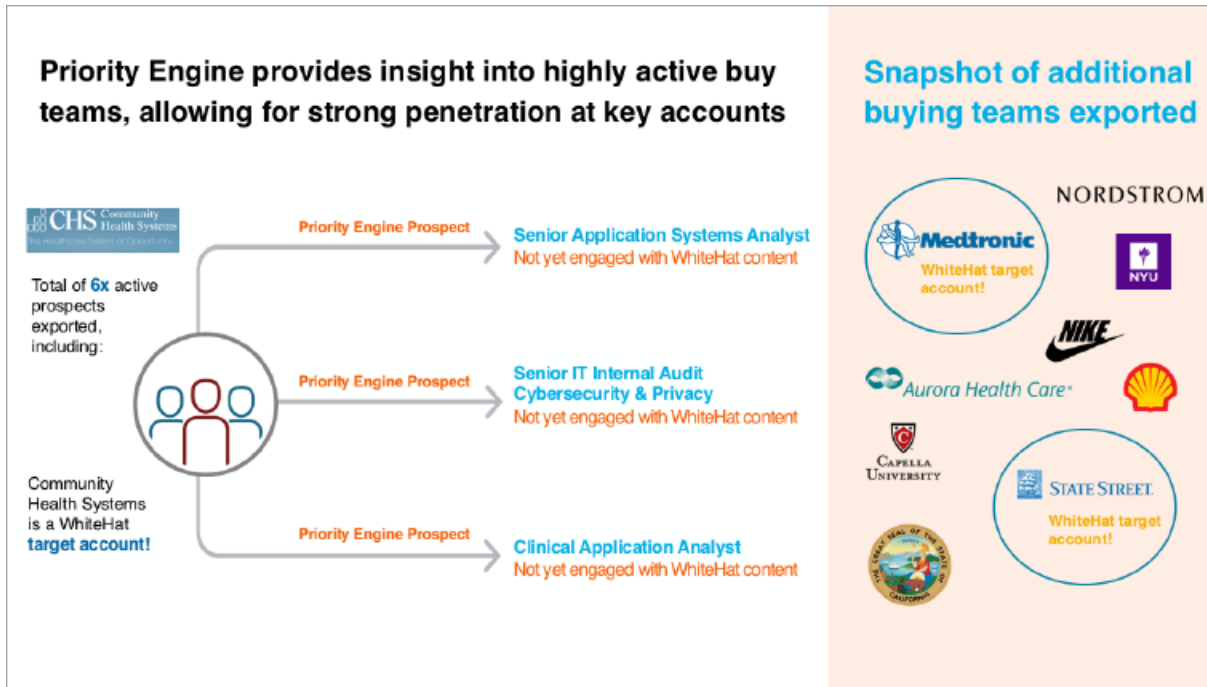
**Who doesn't, but should?**

**What do we know about this account?**

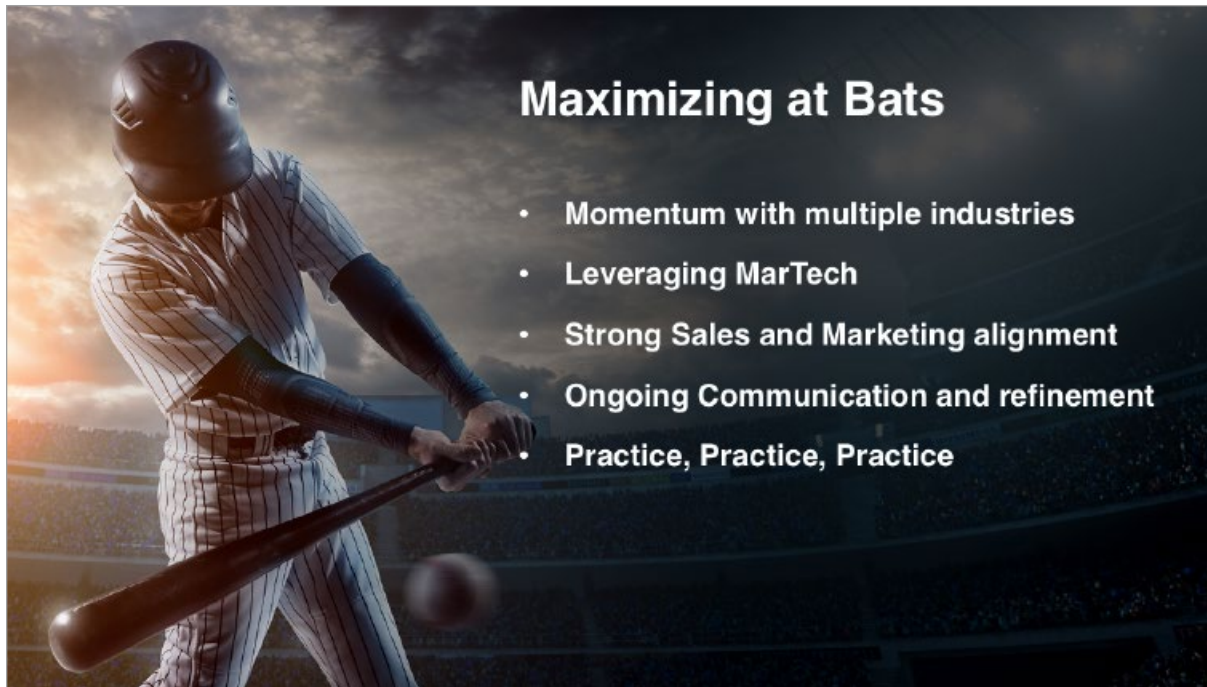


WhiteHat identified the active contacts already in their database. With Priority Engine, they could see who was searching on application security and who might not know of WhiteHat. They gave TechTarget their list of accounts for ABM and saw who had been searching on application security, which competitors they were looking at, which topics they were researching and who in that buying team had been doing the searching. WhiteHat could then give those account details to the SDRs to follow up. With Engagio, they were able to tie marketing and sales together to identify marketing activities and learn where a contact had taken action.





When TechTarget started to see greater engagement on their sites, they sent that feedback to WhiteHat. In this example, WhiteHat could see which accounts had been searching on a healthcare topic, which helped them with follow-up.



WhiteHat started with the healthcare vertical at the end of Q3 2016, added a second vertical in early 2017 and has plans to begin a third.

Key takeaways from their ABM program:

- ABM has helped them build momentum among multiple industries, with solid pipeline growth.
- Once they started leveraging MarTech in Q1 2017, WhiteHat gained further insight into what accounts to target and how to follow up. This insight is among the biggest differentiators between ABM vs. the traditional sales path.
- Sales and Marketing alignment is critical. WhiteHat's Demand Gen team worked closely with the SDR team.
- Ongoing communication and refinement are key to a successful ABM program. It's important for Marketing and Sales to circle back with each other. Frequent stakeholder meetings are important as the program evolves.
- ABM takes practice. There's no single way to do ABM that brings in a homerun every time; it's different for every business. Look at what's working and what's not and continue to build on your success.

# About TechTarget

TechTarget (Nasdaq: TTGT) is the global leader in purchase intent-driven marketing and sales services that deliver business impact for enterprise technology companies. By creating abundant, high-quality editorial content across more than 140 highly targeted technology-specific websites, TechTarget attracts and nurtures communities of technology buyers researching their companies' information technology needs. By understanding these buyers' content consumption behaviors, TechTarget creates the purchase intent insights that fuel efficient and effective marketing and sales activities for clients around the world.

TechTarget has offices in Beijing, Boston, London, Munich, Paris, San Francisco, Singapore and Sydney. For more information, visit [techtarget.com](http://techtarget.com) and follow us on Twitter [@TechTarget](https://twitter.com/TechTarget).



 275 Grove Street, Newton, MA 02466

 888.274.4111

 [InstantABM@techtarget.com](mailto:InstantABM@techtarget.com)

 [www.techtarget.com](http://www.techtarget.com)