Solution: **Security Solutions** Industry: **Media & Entertainment**

Wimbledon 2017

Protecting the oldest brand in tennis with the latest in cognitive security

Balancing tradition with innovation, the Wimbledon brand is built on grass courts, tennis whites and a digital experience that attracts fans with real-time coverage of the world's best tennis tournament. In 2017, cognitive security technology and constant vigilance from IBM helped protect Wimbledon.com and the integrity of the Wimbledon brand.

Share this

Business challenge

The Wimbledon digital experience is crucial to helping grow the value of the Wimbledon brand by attracting a new "digital native" audience—but it also increases risk from cybercrime.

Transformation

Cognitive and other security technologies enabled analysts to quickly and efficiently identify and address the real threats hidden in nearly 200 million events experienced during the tournament.

Results

60x faster

security threat investigations with Watson compared to manual analysis

5x increase

in volume of security incidents analyzed over the course of the tournament

Zero

breaches that impacted the 2017 Wimbledon website and brand

Business challenge story

Building brand value through digital transformation

As spring turns to summer, the eyes of fans around the world turn to Centre Court at the All England Lawn Tennis Club (AELTC), home to the longest-running and most prestigious tournament in tennis, The Championship, Wimbledon. Steeped in tradition, Wimbledon is grass courts, white clothing, strawberries and cream—and great tennis.

Wimbledon today is just as strongly associated with its award-winning digital platform. It brings the action to fans via the web, interactive TV and the Wimbledon mobile app in an immersive experience that blends video, real-time scoring, rich statistics and in-depth

reporting. Driven by cognitive computing and technology innovations from IBM such as Cognitive Highlights and real-time statistical analysis, the digital platform has become an essential component of the Wimbledon brand.

“It is the balance of the traditional with modern innovation that makes Wimbledon quite a unique event,” says Alexandra Willis, Head of Communications, Content and Digital at AELTC.

“We recognize that there is a finite number of people who are able to come to Wimbledon in any given year. But there are millions of people who have shown an interest in and passion for the tournament. The Wimbledon digital experience has become a critical part of how we take Wimbledon beyond the gates and bring the full experience to people around the world who want to engage with us.”

Ultimately, one goal of the AELTC’s investment in its digital transformation is to deepen that engagement with current and young new fans alike. “This is the future of our long-term commercial success,” says Alexandra Willis. “If we build that brand and ensure that fan loyalty we become more attractive to our partners, including our broadcast partners, and increase the value of the Wimbledon brand over time.”

> “Where it might have taken 60 minutes to analyze a security threat, with help from Watson an analyst can do it in just a minute.”
>
> **—Martin Borrett,Chief Technology Officer,IBM Europe**

Transformation story

Harnessing the power of cognitive security

Wimbledon relies on IBM to provide not only the technology infrastructure that differentiates its brand in the world of sports but also the IT security measures that help protect it. While the staff at the AELTC and the fans focused on the courts, the IBM cognitive security operations center (SOC) focused on safeguarding the tournament’s website.

“Although we spend a year in planning for Wimbledon, we really only have two weeks to get it right, when we are the focus of millions of people,” comments Alexandra Willis. “A security breach during those two weeks would be really damaging to the Wimbledon brand. And because Wimbledon is so much a part of the fabric of British identity, a successful attack could be perceived as more than just targeting a tennis event.”

The key word here is “successful.” Martin Borrett, IBM Distinguished Engineer and Chief Technology Officer for IBM Europe, notes: “We saw nearly 200 million security events over the course of the tournament. Wimbledon trusts IBM Security and our cloud to detect and block the real threats.”

The Wimbledon website is protected by multiple security products, at the core of which is IBM® QRadar® SIEM, a security intelligence platform that brings together data from literally thousands of endpoints and devices across the infrastructure, correlates it and helps the security team prioritize and identify the threats they are facing.

For Wimbledon 2017, IBM Security added Watson™ for Cyber Security, bringing a new set of cognitive capabilities that allow the security team to manage threats faster and far more effectively. IBM QRadar Advisor with Watson addresses a key issue facing security operations today: the volume of security incidents and available threat data far exceeds the capacity of even the most skilled security professional.

With QRadar Advisor with Watson, an analyst is provided with a description of the threat and a recommended set of actions based on Watson’s analysis of the threat. Watson’s great skill isn’t the ability to comb through huge amounts of information (though it does that too), it’s the ability to contextualize that information by combining structured data such as specific security events with unstructured data like white papers, research reports and blog posts.

“Where it might have taken 60 minutes to analyze a security threat, with help from Watson an analyst can do it in just a minute. That 60x increase in speed translates into being able to tackle a fivefold volume of incidents and alerts,” Martin Borrett explains.

“So it helps the team bridge gaps in expertise and resources to deal with the ever increasing volume of threats we see year over year. Tackling those and understanding which are the real threats that could be harmful and which are the false positives that can be safely ignored is a huge challenge.”

Assistance from Watson helps position the team to address the evolving threat landscape. Attacks have become more sophisticated as hackers collaborate across geographies and use increasingly advanced infrastructure and techniques. For example, Martin Borrett notes, “This year we noticed a ‘low and slow’ coordinated attack. It began with a kind of distributed denial of service attack that actually wasn’t an attempt to disrupt the website. It was a distraction and a cover up of the real threat. That’s something we’ve not seen before.”

> “Thankfully we haven’t had a major challenge in the security area over [our 25-plus-year partnership], which is fundamental proof that IBM is offering us a good service.”
>
> **—Alexandra Willis,Head of Communications, Content and Digital,AELTC**

Results story

Protecting the Wimbledon brand

“Our ambition has always been that the experience of Wimbledon embodies this idea of tennis in an English garden. So it’s a beautiful experience, like a swan floating across a lake,” says Alexandra Willis. “But what you don’t see is all the activity that’s going on underneath—in our case, the teams that IBM provides us with that the public doesn’t ever know about.”

With IBM focused on operating and protecting Wimbledon’s digital properties, the Wimbledon team is free to focus on the courts, not the cloud—putting on the world-class tennis experience that stands behind the Wimbledon brand. Behind the scenes, cognitive security, IBM technology and the security specialists who monitor and manage the daily deluge of events, incidents and attacks combine to keep the personal data of Wimbledon fans out of the hands of hackers.

Alexandra Willis comments: “The most important thing in working with any partner is having trust. Wimbledon and IBM have been partners for more than 25 years, and we have built up a considerable amount of trust.

"Thankfully we haven't had a major challenge in the security area over those 25-plus years, which is fundamental proof that IBM is offering us a good service—particularly in the context of today's day and age when hacks and security breaches are common. We read about them in the paper often, so it's even more important to know that that trust is there and that resilience is there if ever a problem should arise."

> "Although we spend a year in planning for Wimbledon, we really only have two weeks to get it right. A security breach during those two weeks would be really damaging to the Wimbledon brand."
>
> **—Alexandra Willis,Head of Communications, Content and Digital,AELTC**

About Wimbledon 2017

Known to millions of fans simply as "Wimbledon," The Championships is the oldest of tennis' four Grand Slams, and one of the world's highest-profile sporting events. Organized by the All England Lawn Tennis Club (AELTC), Wimbledon has been a global sporting and cultural institution since 1877.

Solution components

- GTS ITS Security Services: Managed Security Services (Cloud)

Take the next step

For more information about IBM's 28-year partnership as Official Technology Supplier to the AELTC, please visit: ibm.com/Wimbledon

For more information on IBM Security solutions and services, visit: **ibm.com**/security. Follow us on Twitter at @IBMSecurity or visit our blog.

View more client stories or learn more about IBM Security

Print

Security Blog

systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that systems and products are immune from the malicious or illegal conduct of any party.