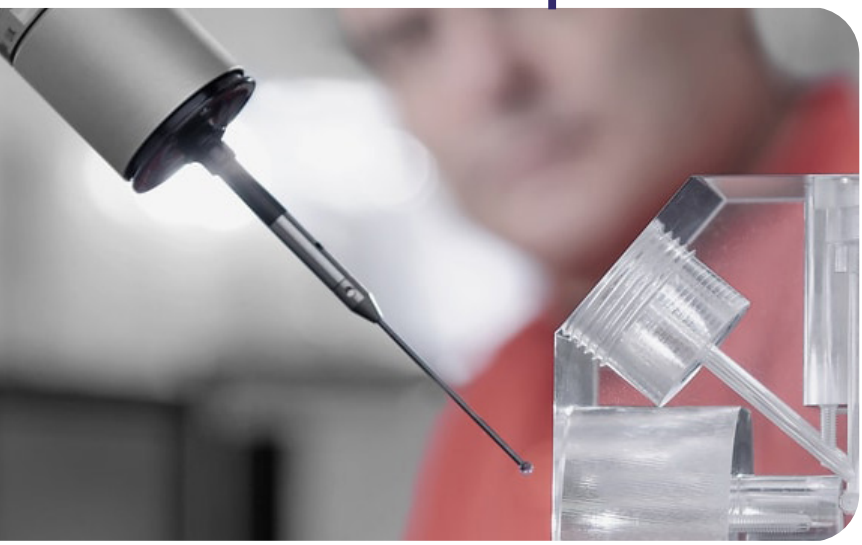
Ontinue

CUSTOMER STORY

Ontinue Provides 24/7 Protection for the Swiss BBC Group



On a daily basis, the average Swiss individual encounters products and services from Behr Bircher Cellpack BBC AG twice. While officially established by Giorgio Behr in 2003, the company's origins trace back to the early 1990s. Under the ongoing guidance of the Behr family, the company has systematically broadened its divisions and ventured into new business domains. Evolving over time, it has transformed into the medium-sized BBC Group, organized into six distinct sub-areas.

Presently, the corporate group operates in pivotal markets, including energy distribution, plastics processing, medical technology, packaging, as well as safety and comfort sectors. This extensive portfolio positions the BBC Group, despite its medium size, with a sophisticated geographical and organizational structure. The company extends its presence across numerous countries in North and South America, Europe, and Asia. The intricate network of locations, however, amplifies the susceptibility to cyber threats, surpassing that of comparable organizations of similar size.

"We keep hearing from our partners, suppliers and customers that the number of cyberattacks is increasing," explains Thomas Stadler, CIO of BBC Group. "We can also see that the threat situation is worsening, although fortunately our security measures have been sufficient so far. But it's only a matter of time before they aren't going to be enough."

Large corporations typically implement the most robust security measures and maintain around-the-clock security systems, making it challenging for cybercriminals to breach their defenses. Consequently, hackers tend to redirect their attention towards what they perceive as more vulnerable targets. Unfortunately, this has resulted in small and medium-sized companies, like the BBC Group, becoming ideal targets due to their comparatively limited resources and security infrastructure.

BBC GROUP

Motivation

- 24/7 security coverage
- Faster response time to attacks
- More awareness of cybersecurity in the company
- Better use of existing security infrastructure

Solution

- Close collaboration with external SOC via Microsoft Teams
- Creation of the position of security engineer to collaborate with the MXDR service provider
- Threat intelligence through Ontinue ION

Outcomes

- 24/7 SOC coverage
- Partial automation of important security processes
- Reducing MTTR and dangerous phishing attacks
- More value creation from existing data

About BBC Group

The Behr Bircher Cellpack (BBC) Group is active in vital markets such as energy distribution, plastics processing, medical technology, and packaging through BBC Cellpack. Additionally, in the sectors of security and comfort through BBC Bircher. Their extensive international footprint in both manufacturing and sales positions them as a highly competent and exceptionally competitive partner.

"You have to protect yourself, otherwise you are the weakest link in the chain," emphasizes Alex Oehler, Head of IT Infrastructure & Systems Management at BBC Group. "One hundred percent security is impossible, but it must be the ultimate goal of a medium-sized company to increase the effort required for hackers to carry out a successful cyberattack to such a level that it is no longer worthwhile."

This includes a security infrastructure that is as watertight as possible, an aspect Behr Bircher Cellpack BBC AG has addressed on the software side through Microsoft Sentinel and Microsoft 365 Security. However, a persistent challenge has been effectively managing the continuous stream of and threats intelligence – These are crucial elements in the ongoing battle against cyber attacks and are best ensured through a Security Operations Center (SOC).

Use synergies sensibly

Limited staffing and constrained budgets make it nearly impossible for most medium-sized companies to establish an in-house Security Operations Center (SOC). Consequently, the BBC Group has opted for outsourcing and entrusted Ontinue's MXDR (Managed Extended Detection and Response) service ION. The decision to choose Ontinue as a SOC service provider stems from the successful collaboration with the Open Systems team, the origin of Ontinue, during the implementation of their software-defined network (SD-WAN). Microsoft, whose security platform the BBC Group employs, further endorsed this decision with a recommendation during the evaluation phase.At the same time, the group of companies created the position of a security engineer internally, i.e. the insider who is so important for external SOC teams and who works with the service provider's security experts. This interface between BBC Group's internal IT department and Ontinue's SOC is of immense importance because external service providers never have as deep an insight into the systems as in-house experts.

The practical implementation of all these measures only took about two months. The BBC Group and Ontinue were able to meet this short period of time because Microsoft's security software was already solidly configured. So it was only necessary to raise the new security layer to the functional foundation.

Better MTTR through streamlined collaboration

In practical terms, Ontinue ION enhances and streamlines communication by consolidating the ticketing system and email alerts into a clear and organized Microsoft Teams channel. This ensures that warnings don't get lost in the clutter of internal IT experts' overflowing inboxes. Coupled with round-the-clock monitoring of the IT infrastructure, the BBC Group has successfully reduced its response time to cyberattacks, leading to a substantial decrease in the Mean Time to Respond (MTTR).

Through its threat intelligence capabilities, Ontinue helped the group uncover vulnerabilities. Like most companies, BBC Group has recognized that individual user misconduct represents a persistent and significant risk that needs to be addressed. This knowledge led to awareness campaigns and semi-automated security processes that quickly reduced the number of dangerous phishing attacks by 50%. For example, if a user today clicks on a suspicious link that triggers a warning, a member of the security team simply has to enter the name into the system. The user is automatically locked out and receives a security key with which they can set a new password for their account and log in again.

In the future, the BBC Group would like to invest even more in security and plans to expand the good cooperation with Ontinue. The threat areas of Intelligence and vulnerability management will especially play a major role in this. The aim is to successively identify and close security gaps. "It is a fact that security is usually inconvenient for users," says Thomas Stadler, "but this does not change the business need for adequate security and with Ontinue we have a security partner at our side who helps me sleep well at night leaves."

> **"The topic of security is often uncomfortable for users, but unfortunately necessary for business. Thanks to Ontinue, I sleep better at night because their experts protect us around the clock."**

Thomas Stadler
CIO
BBC Group

Ontinue

About Ontinue ION: Nonstop SecOps

Ontinue offers nonstop SecOps through an AI-powered managed extended detection and response (MXDR) service. Ontinue ION MXDR combines powerful proprietary AI with the industry's first collaboration with Microsoft Teams to continuously build a deep understanding of our customers' environments, informing how we prevent, detect, and respond to threats.
Continuous protection. AI-powered Nonstop SecOps. That's Ontinue.