CASE STUDY

Business

- Bültel International Fashion Group
- Website: www.bueltel.com
- Sector: Fashion
- Headquarters: Salzbergen, Germany
- Employees: 2,000+

Challenge

As a globally active company with worldwide subsidiaries, the Bültel International Fashion Group must ensure that increasingly strict compliance and data protection requirements are met. In an era in which the Cloud and Software as a Service are becoming increasingly important, it is crucial that IT remains in control of the data. To this end, Bültel relies on real-time audits with the Symantec CloudSOC Cloud Access Security Broker (CASB).

Solution

- Symantec CloudSOC Audit

Services

- Analysis of the cloud landscape across all worldwide subsidiaries
- Identification of Cloud and SaaS services used
- Assessment of business readiness of applications used
- Removal of potentially harmful apps through robust alternatives
- Raising of awareness about data protection

Cloud and SaaS always under control

How fashion company Bültel retains control of its cloud environment with Symantec CloudSOC

Founded in 1964, the Bültel International Fashion Group has grown continuously over the past five decades, during which time it has steadily expanded its portfolio and global presence. In addition to its headquarters in Salzbergen, Lower Saxony, Bültel now has subsidiaries, factory outlets and retail stores in many European countries, as well as its own procurement and production capacities in Hong Kong, Vietnam and the Philippines. Furthermore, almost 1,000 points of sale are managed by B2B market customers.

In order to ensure smooth, functional communication processes across the entire group, Bültel relies upon an efficient enterprise IT infrastructure. The network, which is managed in Salzbergen, therefore enables high availability and is protected with a wide range of state-of-the-art IT security systems, many of which are developed by Symantec.

As the IT landscape has developed historically and very dynamically, the IT team undertook a comprehensive assessment of the application landscape in 2018. The primary objective was to obtain a comprehensive overview of cloud applications used in the company with and without the knowledge of the IT team. On the basis of this analysis, it was then necessary to check whether business-critical or legally regulated data were flow off these channels and if so, to permanently prevent this.

“In view of our company’s security and compliance, it is essential for us to keep track of our critical data,” explains Carsten Hirche, Group CIO at Bültel. “However, this seamless transparency is increasingly difficult to achieve in globalized, highly complex IT environments. We therefore decided to analyze our application landscape in detail using Symantec and PingUs Solutions. The aim is to identify data that could leave the Bültel ecosystem.”

Testing Symantec CloudSOC

Bültel asked its long-time systems integrator and Symantec partner PingUs Solutions to plan, prepare and conduct a detailed cloud assessment. Caroline Kiel, Managing Director at PingUs Solutions reports: “We recommended starting the project with an individually configured Symantec CloudSOC Audit test installation. This efficient cloud access security broker evaluates log files of corporate firewalls, proxies and gateways, and uses this analysis to provide a detailed overview of the applications used by employees. This list usually triggers a ‘eureka’ moment, providing the project team with a solid basis for further protective measures.”

The demo unit at Bültel began to collect application data within the company in January 2018. The system was preconfigured to collect all data anonymously, ensuring reliable protection of employee data. The data provided by the CASB during this first test run was indicative for the project team in more ways than one.

> “In view of our company’s security and compliance, it is essential for us to keep track of our critical data,”
>
> —Carsten Hirche, Group CIO at Bültel

First insight: The cloud is everywhere

The PingUs Solutions and Symantec cloud audit quickly revealed that employees across all continents and subsidiaries used a wide range of cloud apps – not just webmail tools, but also a number of file-sharing applications such as WeTransfer, Google Drive and Dropbox.

Second insight: High bandwidth usage

Analysis of application bandwidth usage revealed that Bültel’s cloud applications consume a significant portion of the available network bandwidth and that, sooner or later, this will affect the performance of the entire infrastructure. Measures must therefore be undertaken to solve this problem.

Third insight: Cloud apps are a threat to compliance

The project team then analyzed the data stored in the apps. “Upon closer inspection, it became clear that our information does not belong in an unprotected cloud environment,” explains Dennis Müglitz, IT project manager at Bültel. “For example, some of our employees had uploaded technical drawings, patterns or new collections to file sharing apps to give suppliers and customers access to them. In order to improve security and compliance, but without interrupting the process, IT must provide our employees with safe, sensible alternatives.”

To obtain an overview of the risk potential of the identified cloud applications, the project team subsequently analyzed these apps in detail to determine whether they are actually suitable for use in a professional business environment. “Cloud apps are not all the same,” explains Carline Kiel from PingUs Solutions. “Applications such as Office 365 are designed for businesses and support secure operation with a range of certified security features. However, many other apps are not protected at all, or only to a very limited extent – some even contain malicious codes that create, for example, a backdoor access to the company. Therefore, every audit involves an investigation of the risk potential of the apps being used.”

What may sound time-consuming is actually quite simple using Symantec CloudSOC: The Symantec CASB has access to detailed real-time information on more than 21,000 applications via a dedicated app feed. This facilitated assessment of the business readiness of cloud applications for the project team. Dennis Müglitz explains: “The CASB supplied us with an in-depth risk assessment for each identified cloud application and, for insecure apps, also recommended alternatives with higher security standards. This has really helped us set the course for secure cloud use.”

> “The CASB supplied us with an in-depth risk assessment for each identified cloud application and, for insecure apps, also recommended alternatives with higher security standards. This has really helped us set the course for secure cloud use.”
>
> —Dennis Müglitz, IT project manager at Bültel

Risk minimization measures

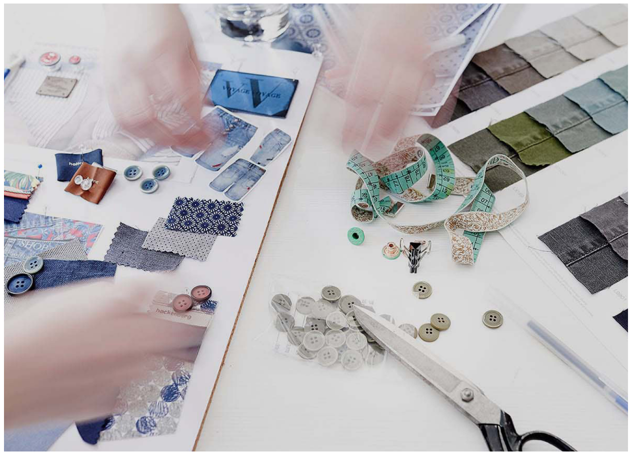
Following the audit, Bültel defined a binding action plan along with experts from PingUs Solutions, in order to curb the use of unwanted applications and to reliably exclude the critical loss of sensitive or regulated data. Key aspects of this are:

Removing inadequately protected applications: Most of the cloud applications were public cloud file-sharing applications. In view of increasingly stringent data protection requirements and the business-critical content that is frequently shared by employees, these tools will now be replaced with secure authentication by a centrally managed file-sharing platform.

Sensitizing employees: In order to raise awareness of the issues arising in public cloud applications among employees, Bültel used the audit as an opportunity to train employees in all its worldwide subsidiaries in data protection, data security and compliance, and established new communication channels in order to sensitize to these topics.

Consistent monitoring of the cloud landscape: The Symantec CloudSOC CASB enables Bültel’s IT team to easily keep track of the cloud landscape and cloud usage by means of clear dashboards and automatically generated reports. This also allows the team to detect and, if necessary, prevent sharing and uploading of critical files much sooner.

Integration of CASB, Secure Web Gateway and Endpoint Protection: To obtain an extensive overview of the cloud environment, the Bültel team seamlessly integrated the CASB with existing firewalls and Symantec Endpoint Protection. Bültel is already planning additional measures to capture all data traffic in the head office and at endpoints; not only for analysis, but also to stop unwanted applications early. By integrating the Symantec Secure Web Gateway in 2019, Bültel will be able to extend existing security policies to the cloud to enable strict authentication for sensitive cloud apps, and to prevent regulated files being sent via webmail.



Conclusion: ‘No cloud’ is not a solution either

Some months after the CASB implementation, Carsten Hirche, CIO of the Bültel Group draws a positive conclusion from the project: “The cloud opens up a whole new world of collaboration for us as a globally active company. However, the benefits in productivity and flexibility should not be at the cost of security and compliance. The Symantec CASB has proven to be an extremely valuable tool in this ‘minefield’, helping us to keep track of our critical data at all times – and to intervene much quicker in an emergency.”

To learn more about Symantec CloudSOC Cloud Access Security Broker (CASB), please visit https://www.symantec.com/products/cloud-application-security-cloudsoc

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world’s leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec’s Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world’s largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com