

Fever-Tree Harnesses OneLogin Desktop and MFA to Ensure Only Authenticated Users Access Essential Apps and Information



Founded in 2004, Fever-Tree is the world's leading supplier of premium carbonated mixers for alcoholic spirits by retail sales value, with distribution to over 70 countries internationally. Based in the UK, the brand now sells a range of 14 differentiated flavors to hotels, restaurants, bars, cafes, and supermarkets as well as off-licenses for retail purchase throughout the UK, USA, Spain, and Belgium. The first mover and innovator of the premium mixer category, Fever-Tree was voted the number-one best-selling and number-one trending tonic water four years running by the world's best bars in Drinks International's Annual Brand Report.

Gained visibility into
app and network access



Quickly and easily onboard
and offboard users



Improved security posture



CHALLENGES

Since completing its acquisition of Global Drinks Partnership, Fever-Tree counts 245 employees, the majority of whom are in the UK, US and Germany. These employees fulfill roles in sales, marketing, innovation, supply chain, quality, finance, HR, and legal.

From the start, the company has operated a distributed model, with many people working from their home offices. Since COVID-19 struck, all employees are working remotely. At the same time, the company runs a non-domain network in the United States, meaning Macs run on the company's Windows infrastructure. Combined, these factors meant that Fever-Tree did not have visibility into who or when someone was authenticating into the company's network.

Even when the company migrated to Office 365, anyone with the correct password could log in and access the network. In fact, Fever-Tree dealt with various attempts at third parties trying to gain network access in 2019.

When someone successfully breached the network and installed ransomware, it stopped business. "We were involved in lots of marketing for tennis, golf, and cricket tournaments that we sponsor and the network hack disrupted our ability to operate as usual," explains Mayur Mistry, Head of IT at Fever-Tree.

With extensive experience in the finance world, Mayur knew Fever-Tree needed to enhance its security measures. His vision was to secure laptops by complementing the anti-virus, next-generation firewall and clever email filtering Fever-Tree already used. "As a global brand, we need top-notch security to ensure no one can access and share our information with a competitor. I proposed to the board of directors that we shore up our users and laptops by adding a layer of security on top of our two main applications – Office 365 and Egnyte," continues Mayur.

SOLUTIONS

A trusted peer recommended that Mayur check out OneLogin so he compared OneLogin Multi-Factor Authentication (MFA) against Duo Security, Mimecast and Okta.

In previous companies, Mayur had used two-factor authentication, including Duo Security. However, he felt Duo Security was not the best option for Fever-Tree. "Many of our employees are on laptops and we want to enable them to be as mobile as possible from an MFA perspective," he explains.



INDUSTRY

Retail



USERS

245 users



INTEGRATIONS

Office 365 and Egnyte

"OneLogin fits well into our vision of a mature security estate and is the gateway to ensure that our security landscape is as secure as possible."

Mayur Mistry

IT Operations Manager



In addition, Mayur discovered another shortcoming with the other solutions. “Where Duo and others fall away is that no certificate is installed on machines – you simply put in your user name and the software authenticates via the SSO provider. OneLogin confirms the user’s account and the machine before enabling access.”

Plus, Mayur was impressed with the ease of integrating OneLogin into Fever-Tree’s environment. He also appreciates that it’s versatile and easy to use. As he says, the GUI interface makes it easy to use, and eliminates the need for Mayur to scroll through lots of information to switch something on or off. “I’m the only person in IT for Fever-Tree and I don’t want to struggle to do the basics. OneLogin makes it easy to do my job, enabling me to do many key things with the click of a button,” he continues.

RESULTS

With OneLogin Desktop installed on everyone’s machines, Mayur has been able to enforce security policies and make all machines compliant with how Fever-Tree runs its infrastructure. When out of the office, employees must access the company’s network via OneLogin MFA to access Office 365 and Egnyte.

“The setup before was cowboy-esque style IT – anyone could log in from any device and we couldn’t police it. Now we can make sure employees only use their company laptops to access the network,” explains Mayur.

As Mayur explains, when people are working remotely, it’s impossible for the company to determine if they are logging in from home or even if someone else in the household is logging in using their machine. “Two-factor authentication ensures trust between our employees and the Fever-Tree network. As such, OneLogin MFA enables a proactive approach to security and protecting both employees and the company,” he continues.

Plus, Fever-Tree has the visibility needed to ensure employee laptops are secure and that employees are using their devices as intended. “With OneLogin, we can see how all the pieces join together in our IT infrastructure and build a story about what each employee is doing, using OneLogin as the cornerstone of our reporting. This helps managers and the board see how essential IT is to the business,” concludes Mayur.

While onboarding is currently enabled through the connection to Active Directory, Fever-Tree plans to use Bamboo HR as its source of truth going forward so the company can fully automate the onboarding and offboarding process.

When a user is added to Egnyte, for instance, they receive an email that helps configure their system for access. Mayur also relies on OneLogin for streamlined deprovisioning. “I can easily deactivate a user and remove their license via the OneLogin dashboard, which is much simpler than logging into Active Directory. I can even log into the OneLogin dashboard on my mobile phone, which makes it possible for me to quickly handle the deactivation process from anywhere at any time,” he explains.

In the future, Mayur plans to integrate OneLogin with more web services and systems, including Salesforce, Jira, and the VPN associated with the company’s network firewall. “The beauty of OneLogin is its flexibility to integrate with various software. Our plan is to be fully cloud-based in the future, and an important part of our security will be protecting all cloud-based products by ensuring they are MFA authenticated via OneLogin,” concludes Mayur.



Ensured compliance with company’s security policies



Reduced risk of security breach



Streamlined IT administration