Fortune 500 Beverage Manufacturer Secures Data on Unmanaged Devices

An agentless Forcepoint ONE enabled employees and contractors to access corporate data from unmanaged devices and prevented leavers from walking away with sensitive information.

Low user adoption of its mobile device management solution led the Fortune 500 beverage manufacturer to look at other ways to secure its corporate data on unmanaged devices. Using an agentless Forcepoint ONE, it was able to continue its BYOD policy, maintain tight control over its data, and even wipe sensitive information from the mobile devices of employees leaving the company. The firm reached its full deployment goal just three weeks after implementing the solution.

CUSTOMER PROFILE:
The multinational beverage manufacturer is a household name with over 90 brands on tap. Headquartered in the United States, the Fortune 500 firm operates on a global scale.

INDUSTRY:
Beverage

HQ COUNTRY:
United States

PRODUCTS:
› Forcepoint ONE

Balancing User Productivity with Security Concerns

Greater user productivity is a driving force behind this Fortune 500 beverage manufacturer's Bring Your Own Device (BYOD) policy. But with tens of thousands of employees spread across the world, maintaining visibility into data access and enforcing usage policies was challenging.

The company initially turned to Mobile Device Management (MDM) solutions to mitigate the risks of allowing sensitive information to be accessed from unmanaged devices. However, the IT team was quickly met with privacy concerns from employees about installing the software on their personal mobile phones and devices.

Adding to the hurdle was the complexity of installing and configuring MDM agents on thousands of devices with many different operating systems and hardware types. It was a time intensive operation that didn't yield the results the business was looking for.

After the company saw fewer than 10 users install the MDM, the organization's CIO tasked his team to find a solution to bridge the gap between user experience and security.

Going Agentless with Forcepoint ONE

The CIO had three key factors in mind when evaluating how to protect the business' data on employees' personal devices. The solution needed to:

→ Be easy to deploy.
→ Eliminate workforce privacy concerns.
→ Work across its on-premises Exchange server to Office 365 in the cloud.

The Forcepoint ONE Cloud Access Security Broker (CASB) checked all the boxes. The agentless solution enabled the company to extend data security to unmanaged devices without needing to rely on users to download software or install certificates.

"When you make security as simple as setting up the apps on their phone the same as they normally would, then you take away that barrier to mass adoption," the CIO said.

The agentless Forcepoint ONE also greatly reduced the amount of work for IT Helpdesk during deployment. Since devices were configured to communicate with the proxy, the solution would automatically sync with the beverage manufacturer's Active Directory – making user management seamless and straightforward.

Protecting the Business and Enabling the Workforce

A frictionless user experience that is unique to the Forcepoint ONE agentless CASB led to the firm's deployment goals being reached just three weeks after the project started.

The respect paid to employee privacy and the absence of any impact on device performance were encouraging factors that drove the solution's high adoption rate. It was a stark difference to the resource-heavy mobile device management solutions used in the past.

One of the key functionalities introduced by the Forcepoint ONE has become more valuable over time as the Great Resignation, as some term it, leads to higher turnover in companies across the world.

When employees leave the beverage manufacturer and are removed from Active Directory, the platform automatically wipes corporate data from the device – without impacting the personal data on it. Furthermore, the company can now implement policies that prevent sensitive information from being downloaded even if employees have accessed it on their own device.

The agentless platform helped the IT team strike the perfect balance between improving its security posture while catering to the user experience to elevate adoption.

Challenges

- Balance user productivity and privacy with the need to secure unmanaged devices interacting with data.
- Prevent employees leaving the company from walking away with sensitive information.
- Improve adoption of BYOD security policy.

Approach

- Deploy Forcepoint ONE agentless CASB.

Results

- Reached user adoption goals within three weeks of Forcepoint ONE deployment.
- Maintain BYOD policy with frictionless security.
- Introduced ability to wipe leavers' mobile devices of corporate data while preserving personal data.