CENGN

BDATA INNOVATION HIGHLIGHT

BDATA
Innovating Security

COMPANY OVERVIEW

According to IBM, a cyberattack costs, on average, around $3.6 million to manufacturers and critical infrastructures. Over 50% of the damage is due to disruptions in operation by shutting down high-value machines and equipment. Less than 10% of the damage is directly related to the attack. BDATA created digital fingerprints for IoT, Edge, and Endpoint devices to increase the equipment's transparency and keep the cyberattack from spilling over to the operation side. By using password-less, peer-endorsing, and zero-trust networks, BDATA helps to reduce disruptions in operation and minimize cyberattack damage.

LOCATION: HAMILTON, ON

TECHNOLOGY

Cybersecurity

Owen Wang, Co-Founder / Business Development

BDATA
Innovating Security

owen@bdata.ca

bdata.ca

Rick Penwarden, Sr. Manager, Marketing

CENGN

rick.penwarden@cengn.ca

cengn.ca/projects/

LACK OF CYBERSECURITY ON THE IT SIDE

Manufacturers and critical infrastructures want to have connectivity at the device level. However, due to the lack of cybersecurity on the device side to defend against cyberattacks, most companies fear a cyberattack on the IT side will spill over to the device side, which will end up shutting down operations and stopping production. Such as the case for Colonial pipeline and the City of Stratford, the direct damage cost by the cyberattack is only 10% of the total damage. However, the device-side cybersecurity adoption rate is low because the current user-based cybersecurity software is not scalable when implemented on devices.

USING DIGITAL FINGERPRINTS FOR DEVICES

BDATA is increasing IoT, edge, and endpoint device transparency and security for manufacturing, infrastructures, and energy companies. By using **unique digital fingerprints for devices** generated by BDATA Technology, customers can minimize cyberattack damage to the IT side and keep their production, operation, and infrastructures running. The device's authentication is handled not by username and password but by a peer-endorsing, zero-trust network of devices. Such configuration allows users not to fear about a stolen account and password.

IDENTIFYING RESOURCE REQUIREMENTS AND SCALE TESTING

Using the CENGN Testbed, BDATA successfully deployed its platform on a Kubernetes cluster. BDATA identified that the resource requirements of the platform were over-provisioned and restructured its resource allocation. The platform auto scaled during the load testing and the services did not fail as the load was managed properly. This testing allowed BDATA to validate their ability to support many devices.

"Testing helped us to understand how performance was under a stressed condition. With the product finished testing, we have confidence that it'll gain lots of traction from users and investors."

Owen Wang
Co-Founder,
BDATA