Eliminating Risks from BFSI Operations with Endpoint Security Solutions

Summary: The BFSI sector in India has adopted a range of technologies to serve its customers efficiently. The digitalisation of key operations in the sector was also realised to improve business reach and revenues. However, it has been observed that the adoption of efficient cybersecurity practices has not kept pace with the rate of deploying digital platforms for business. The growing use of wireless devices for professional work is a particular concern as these machines use different data connectivity options to access the business network. They may also have applications that can snoop on protected data.

Over the past decade, the banking and financial services sector, including the fintech and insurance companies (BFSI), has aggressively transformed itself and adopted digital technology to suit the changing expectations of consumers.

Moving from paper records to net banking and mobile applications, and offering online methods to pay bills and insurance premiums, these companies aim to make financial transactions quick and easy for their customers. Although this digital transformation has improved the brand image of such organisations, it has also raised concerns on how securely they manage the savings and investments of millions of people.

The BFSI sector has become a prime target for hackers who use devious ways to pilfer bank account and credit/debit details, user credentials, tax records and insurance data. The information stolen from the cyberspace and employees’ machines can be misused to fund high-value transactions, file fraudulent tax returns, commit insurance fraud and invest in cryptocurrency.

While the use of wireless devices by the BFSI workforce and the storage of data in the cloud give them more flexibility to manage their files, it also makes them more vulnerable to cyber threats.

During the recent outbreak of coronavirus that impelled many employees to work from home using their personal computers or wireless devices, the cases of cybersecurity attacks showed a marked spike.¹

While most businesses in this financial segment install advanced software systems and cybersecurity tools on their employees’ devices to safeguard customer data and applications, their siloed nature and the need for frequent updating render them weak.

To counter this weakness, BFSI companies need integrated security solutions that can seamlessly safeguard their digital devices and the exchange of information over the cloud network they work on.

Enhancing device security from end to end

The DoBig Endpoint Security solution offered by Tata Tele Business Services (TTBS) fortifies BFSI organisations with a strong line of defence against any online threat that can sabotage their operations.

Endpoint security is a methodology of securing a business network that is accessed via wireless devices such as laptops, tablets and smartphones. Each device connecting to the network from remote locations gets a secure endpoint that keeps it resilient against cyber threats.
Is it different from antivirus?

Although the objective of an endpoint security solution is similar to that of antivirus software, there is a considerable difference in how deeply they work. Whereas antivirus systems protect individual devices on which they get installed, endpoint security solution secures a device and every aspect of the network that it is connected to.

Beyond the safety provided by basic antivirus packages, endpoint security comes with abilities for network access control, application whitelisting, managed threat detection and response and indicators of compromise (IOC) security.

How does endpoint security work?

While the TTBS endpoint security system is a Software as a Service (SaaS) tool, to begin using the service endpoint security system, a client or executable software needs to be installed on each device. User can simply click on a link provided to them and download the software.

This method of deployment makes our security solution superior to traditional endpoint security systems that require an organisation to install a master server first in its office. This server, in turn, enables all laptops (clients) to draw security updates from it. The server also needs a continuous supply of Internet connectivity – if there is an outage for a few minutes, the endpoints do not get updated.

The TTBS endpoint security system, on the other hand, is cloud-based and needs no server or hardware in the workplace. It helps to save on power consumption and eliminates the issues of hardware obsolescence and space constraints in the server room.

With our endpoint security, the organisation’s system administrators get a centralised console that allows them to manage security for all devices remotely. As an example, they can block the USB port of a laptop or restrict access to undesirable sites.

The system safeguards endpoints for application control and blocks the use of apps that could harm the user's device or are not authorised to be used on a device meant for BFSI work operations. It also provides end-to-end encryption, thereby preventing data loss from the device.

Once endpoint security is installed, it can rapidly detect malware and other risks. Unlike run-of-the-mill antivirus systems, it can also detect and eliminate advanced threats like polymorphic phishing attacks, file-less malware and zero-day bugs.

With seamless monitoring, our endpoint security solution provides better visibility and multiple response options to protect the devices used for BFSI work and financial transactions.

Features of TTBS endpoint security solution

TTBS’s endpoint security solution is powered by Trend Micro – a brand that leads in enterprise data security and cybersecurity solutions for offices, data centres, cloud platforms, networks and endpoints.

It supports a variety of devices used by the BFSI industry staff. These include Windows-based PCs and laptops, iOS devices and Android smartphones.
The key features of DoBig Endpoint Security include:

- Antivirus
- Anti-Spyware
- Anti-Ransomware
- Application Control
- Component Updates
- Data Loss Prevention
- Device Control
- Firewall
- HTTPS Web Protection
- Predictive Machine Learning
- Role-Based Administration
- Unauthorised Change Prevention Service
- URL Filtering
- Web Reputation
- Full Disk Encryption

Additionally, the endpoint security solution brings an analytics dashboard to scan all security reports, user group reports and the different notifications or alerts on security.

It also has an easy-to-use admin portal for policy and exception management. The portal offers a unified view of the health status of all devices.

As a scalable and cloud-hosted solution, DoBig Endpoint Security allows for real-time discovery of threats and instant patch management. The multi-tenant architecture of TTBS products and services affords value-for-money pricing, and the business gets a single bill covering all the devices using endpoint security. An around-the-clock contact centre is available for account managers and users.

If your organisation has a BYOD policy or some of the employees work from home using different devices, it is essential to stay protected against the looming threats in the cyberspace. This is even more critical for organisations in an industry that handles others’ money and must always be compliant with government regulations and pertinent monetary policies.

To know more about DoBig Endpoint Security for BFSI companies, please call Tata Tele Business Services at 1800-266-1800.

Source