FUJITSU

Endpoint Security Assurance for Critical Health Services

As the sophistication of cybersecurity threats develops exponentially, they increasingly threaten the security and integrity of public sector and healthcare systems. A cyber breach could compromise operations when endpoint users unwittingly enable prohibited applications that allow hackers to exploit weaknesses in the system. End-user devices serve as points of access to a network and form points of entry that malicious actors can exploit. To eliminate the risk of this exposure, endpoint security is a key intervention in the fortification and ensure the resilience and availability of healthcare services.

This State government agency works to create a more inclusive society by helping citizens receive more equitable access to care.

They support the community by focusing on housing, child protection, disability, ageing and carers, prevention of family violence, women, veterans, youth, multicultural affairs and LGBTIQ+ equality. The agency's responsibilities include service provision for a large population throughout a widespread urban and regional area.

With a focus on care delivery, systems upgrade had not been a priority for investment, the server fleet and the including the increasing number of system vulnerabilities. With the increase in cybersecurity threats, they needed to protect these critical systems with improved threat detection capabilities and the ability to block cyberattacks.

Challenge

Endpoint security has evolved from archaic antivirus software, to leading-edge cybersecurity technology that reduces the vulnerability to cyberattacks without interfering with the user experience. The agency was faced with increasing cybersecurity threats that potentially exposed endpoints to security breaches. In fact, the cyber threat actors have accelerated their focus on healthcare disruption and compromise to capitalise on the pressures faced by hospitals and governments who are prioritised on fighting the COVID-19 pandemic. Fujitsu was tasked to facilitate collaboration between the system vendor, the system integrator and the agency; to install and configure the CylanceProtect platform so that the urgent challenges could be overcome.

The agency, together with Fujitsu, codesigned a plan to address the following challenges:

Remediate anti-virus and malware protection for ageing Windows 2003/2008 server fleet

Protect the technical environment against malicious software and cyber threats

Minimise any negative performance impact to systems from installing the new platform

Minimise the likelihood of any service disruptions during deployment

Solution

Fujitsu's approach was to trial the CylanceProtect platform on 10 ageing Windows 2003/2008 non-production servers to determine whether the endpoint application would cause any performance issues with the existing applications. Thorough groundwork during the pilot phase 'derisks' the subsequent wider rollout, scanning each host and reviewing the results before enforcing protection. Fujitsu designed an exception configuration to ensure legitimate applications would not be impacted.

To enable the protected servers to be managed from a cloud console, without exposing them to the internet, a CylanceHybrid virtual appliance was installed to broker communications between CylanceProtect and Cylance Venue cloud console. The agency engaged the Application Support Vendor to undertake performance testing before and after implementation and confirmed that no unreasonable performance and functional impacts were observed on the applications. A significant number of applications have been subject to 'global waiver' i.e. the CylanceProtect platform will not block or interfere with them.

As part of the pilot project, Fujitsu was able to remediate the ageing servers for anti-virus compliance and implemented malware protection through the deployment of endpoint security software. Over 150,000 files were scanned across the pilot server fleet and no high-risk files or malware were found. The trial successfully confirmed that the platform would not cause any performance issues with the target applications. The agency was appreciative that the project was completed successfully and within budget.

Outcomes

Following the successful completion of the Pilot project, Fujitsu was able to provide the agency with an affordable plan to deploy the CylanceProtect platform to all the Win2003/2008 outdated server fleet across the enterprise as part of a managed service including:

- Integration of system logging and reporting dashboard tools
- Auto-ticketing integration with the IT Service Management platform
- Development of Business-as-Usual processes for ongoing maintenance and configuration of the CylanceProtect application suite of products
- Remote monitoring of the hybrid environment Cylance Hybrid virtual appliance

Collectively, the proposed, innovative solution delivers a robust and impermeable security posture provides deterrence to cyber-attacks across endpoints, enabling the business to securely concentrate on care services for disadvantaged populations.

> "Fujitsu provides managed services to the agency, so we were engaged to work with a Cybersecurity platform vendor to set-up and configure a rapid and effective endpoint security suite of applications using Artificial Intelligence algorithms to detect, prevent and block threats from infiltrating all endpoints linked to the system."
>
> Fujitsu Team Lead