Protect valuable employee data with best-in-class ransomware defense

Enterprises are increasingly concerned about the growing threat of cyberattacks, which target employees’ personal identifiable information, customer data, financial data, and other critical business information. The impacts can be crippling, including downtime from the complete shutdown of data centers, supply chain and business operations, lost reputation with customers and partners, and significant financial ramifications. With Ransomware Containment as part of their cybersecurity and business continuity protocols, organizations can have peace of mind that their critical, sensitive information assets are protected.

Business Challenges

- Growing threat of cyberattacks, especially ransomware
- Increase in security risks and vulnerabilities associated with remote work and digital workplace, such as user errors in clicking on an email link with malware, accessing websites with malicious content, or using an infected USB driver
- Growing threat of cyberattacks, especially ransomware
- 200% increase in downtime year over year as a result of security breaches

Business Results

- Minimal impact on IT infrastructure and network performance
- Can prevent potential system lock down and avoid significant data recovery and repair costs
- Confidence in ability to manage potential breaches with focus on business continuity
- Countering the impact of additional security threats associated with more staff working from home
Growing cyber security concerns

The growing concerns of cyber threats in enterprises have recently been attributed to increases in remote work and digital transformation initiatives. Online threats grew six-times in 2020 with the average increase in ransom payments amounting to $780,000 or more for a large enterprise.¹, ²

Most enterprises have invested in multiple layers of perimeter and endpoint security to protect their infrastructure and assets from a potential security breach. However, cyber criminals are continuously innovating new and unknown methods to defeat traditional prevention-based security solutions, often spending weeks to months working undetected inside a network before delivering a payload, encrypting up to 10,000 files per minute.³

The increase in remote work has elevated security risks with employees not leveraging VPN, accessing company data from personal devices, or using infected USB and other removable media to manage files. With being one click away from a possible ransomware breach, employee HR records, customer data, and critical business reports and data are stolen, and devices and files are encrypted. The impact could be devastating to the enterprise from damaging reputation with customers, large financial ramifications from losing an estimated $8,500 per hour due to ransomware-induced downtime, legal costs and paid ransom, and interrupted business operations.¹

When employees are away from the office, they tend to be less mindful of security best practices. Despite robust security systems, enterprises recognize that there is a heightened risk with more employees working from home.

Implementing a ‘Last Line of Defense’

To help defend against ransomware, the enterprises that have implemented Ricoh’s Ransomware Containment solution as a last line of defense get an instant alert, and the solution responds by shutting down the endpoint under attack, including laptops. The solution is an agentless application that is installed on a virtual server in the central IT system instead of every endpoint and has minimal impact on IT infrastructure and performance. It monitors, in real-time, data across the entire enterprise. It is intended to spot a ransomware attack – usually via a laptop or desktop – anywhere across the entire network even when it has managed to by-pass existing security systems. The solution then locks down the location, isolates files impacted by malware encryption, and stops the ransomware from spreading across the entire network.

As a result, the enterprise can have confidence in its ability to manage a potential breach with a focus on business continuity. Operations are running smoothly, systems and applications are not locked down, and only a small number of files need to be repaired and recovered. Stopping the ransomware attack would also allow the enterprise to preserve its reputation with customers and partners without financial ramifications such as legal fees, settlement costs, a ransom payout, or other long-term financial liabilities.

¹ 2021 Ransomware Statistics, Data, & Trends, PurpleSec
² Cyber-Attacks Up 37% Over Past Month as #COVID19 Bites, InfoSecurity Magazine
³ Ransomware containment: protecting against ransomware attack, Ricoh USA, Inc