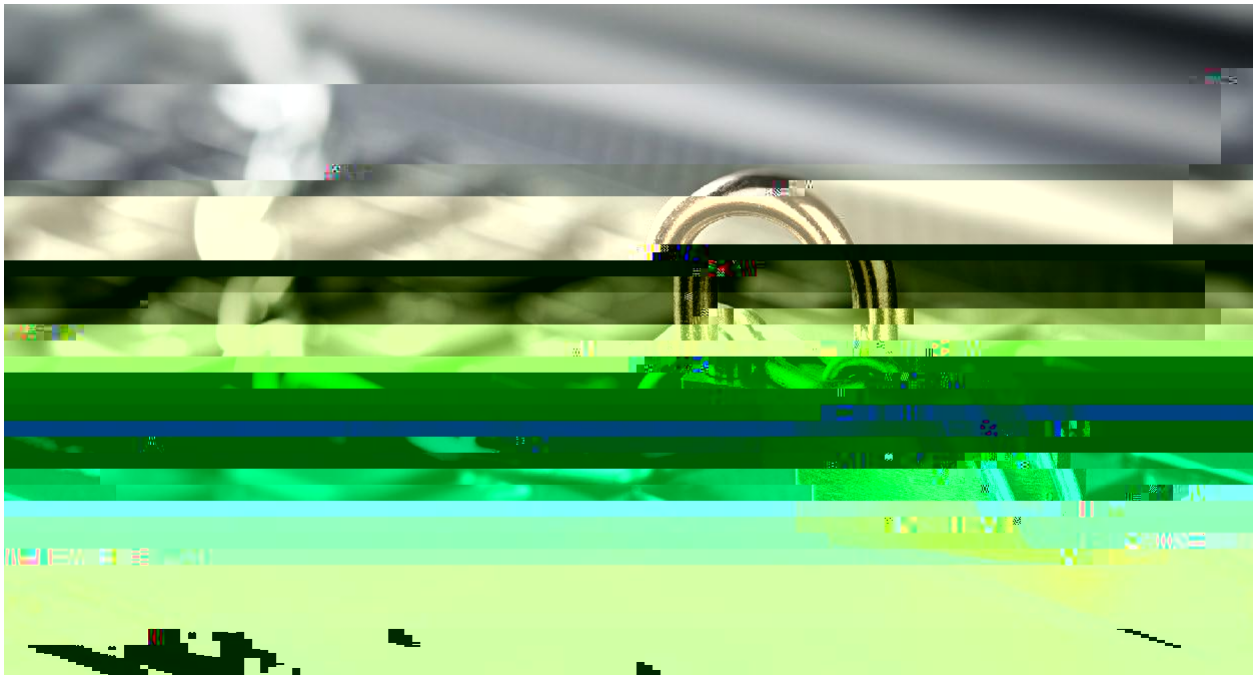
[redacted]

March 2023

Thomson Reuters is a leading provider of business information services. Our products include highly specialized information-enabled software and tools for legal, tax, accounting, and compliance professionals combined with the world's most global news service – Reuters. For more information on Thomson Reuters, visit tr.com and for the latest world news, reuters.com.

We maintain our reputation for providing reliable and trustworthy information through a variety of means, including a comprehensive information security management framework supported by a wide range of security policies, standards, and practices.

This document explains Thomson Reuters' approach to information security and risk management.



White Paper

Patch Management

Thomson Reuters' patch management standard follows industry best practices and product security principles which adhere to specific requirements wherein patches are communicated, rated, and deployed in an effective manner. The standard requires that technology teams deploy security patches based on their importance, and within specific time frames. We also employ forced patching protocols to mitigate unknown threats. Where required, additional Endpoint Protection security controls may be implemented to provide mitigation against known threats.

Endpoint Protection

Thomson Reuters takes the threat from malware to its networks and its customers very seriously and uses a variety of methods to prevent, detect and eradicate malware.

Our comprehensive endpoint protection strategy features antivirus scanners to protect against uploading and downloading malicious content. We deploy a combination of endpoint and antivirus solutions to prevent and detect both server and workstation environments to identify and prevent malicious code from reaching Thomson Reuters. The virus signature files are updated automatically, and our system administrators can also manually upgrade antivirus software as soon as important updates are available. Any update made to the virus software is validated and tested before being applied.

Cyber Intelligence

Thomson Reuters utilizes a range of commercial and open-source intelligence sources to enable our teams to continuously monitor, analyze, and mitigate potential cyber threats to the company. This intelligence includes indicators of compromise, attacker tactics and techniques, and changing motivations and targeting across threat groups. As new threat details are identified, we work to ensure our network and endpoint detection and prevention technologies are updated to better defend against these evolving threats.

The company also participates in strategic threat sharing forums and partnerships, which provide increased visibility into the latest threat trends observed across industries to which Thomson Reuters is aligned.

Thomson Reuters has an established resilience strategy to ensure our continued ability to serve our customers, and to protect our people and assets. Our Business Continuity Plan (BCP) prepares us to respond and recover from disruptive incidents including but not limited to natural disaster, pandemics, transit shutdowns. The BCP itself is company confidential and

Our Business Continuity Plan prepares us to respond and recover from disruptive incidents such as natural disaster, pandemics, transit shutdowns.