A critical national cyber security event and the effectiveness of compensating technical controls provided by Roche managed firewalls

On 14 May 2021 the Health Service Executive (HSE) of Ireland suffered a ransomware cyber attack which resulted in a nationwide disruption of its health and social care services:

"Initial reports indicated a human-operated 'Conti' ransomware attack that had severely disabled a number of systems and necessitated the shutdown of the majority of other HSE systems. There are serious impacts to health operations.....as hospitals implement their business continuity plans."

National Cyber Security Centre (NCSC) Ireland[1]

The Threat to Roche Diagnostics Systems

Roche Diagnostics, manufacturer of a wide range of network connected clinical diagnostics systems, supports HSE diagnostics operations across a large number of installations across the Republic of Ireland. These form part of the Irish healthcare ecosystem receiving test requests from HSE systems and returning diagnostics test results. In connecting to such customer networks, the Roche Diagnostics systems are subject to the same cyber security threats as occurred in 14 May 2021.

The Solution: Rigorous Roche Diagnostics Security Controls

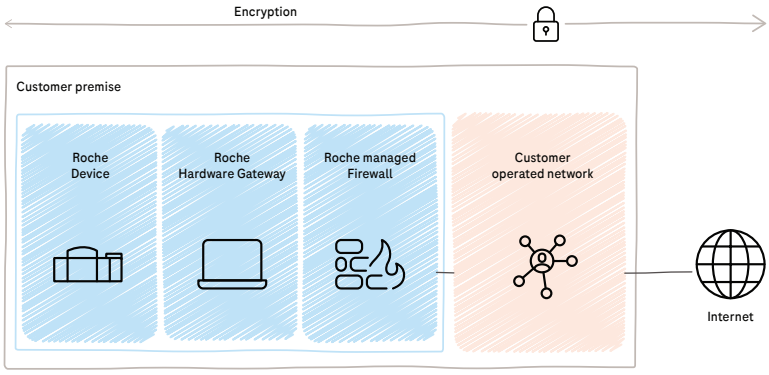
Roche's approach is to ensure that the performance of the solution delivers constant reliable results within tolerance. To assure that performance, extensive validation tests are undertaken against standard configurations including all components; hardware, clinical assays and software. The trustworthy validated performance of Roche instruments underpins the operation of laboratories to quality and license to operate requirements such as ISO 15189:2012. Changes to any component in the validated solution, risk the trustworthy performance of the solution.

In recognition of the difference in cycle times between;

1) **Corporate IT controls** such as OEM security (Patch Tuesday), Antivirus, AntiMalware updates and,

2) **The clinical validation cycle** of diagnostics solutions

It is Roche policy to implement compensating controls in the form of a Roche managed firewall between your network and the diagnostics system. These firewalls deny all traffic which is not directly related to the operation of the diagnostics instrument and its interaction with supporting systems on your network (e.g.: Laboratory Information System - LIS). Across the Republic of Ireland we have more than 100 diagnostics instruments and modules protected behind Roche managed firewalls.



The Roche managed firewall is located within the customer laboratory network to protect Roche devices from cyber-security threats. It is a stateful firewall manufactured by the leading firewall company - Fortinet, with a custom configuration for Roche medical devices.

The outcome: All firewall-protected Roche instruments were safe

Roche is pleased to report that no instruments connected to the HSE network but protected behind Roche managed firewalls were infected by the 'Conti' ransomware attack in May 2021. This affords high levels of assurance around the effectiveness of this approach protecting the operation of customer diagnostics operations during a period when the NCSC reports ransomware as the most serious and tangible cyber security threat globally.

"Roche devices in University Hospital Galway that were located behind the Roche supplied Fortigate Firewalls showed no signs of compromise and were not impacted by the Cyber Attack last year."

Martin Murphy

Technology Manager Galway University Hospitals, Ireland

[1]National Cyber Security Centre (NCSC), Ransomware Attack on Health Sector - UPDATE 2021-05-16, https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf. Last Accessed 11 Aug. 2022.

navify