Product Security White Paper

The purpose of this document is to detail the security and privacy practices that Baxter applied to Baxter SmartCare Remote Management (SCRM) and SCRM Actionable Insights, which is hosted on the SCRM platform. This paper also covers what you should know about maintaining security of this product and how we can partner with you to ensure security throughout this product's lifecycle.

Baxter is committed to protecting the security of our products and the data privacy of our customers. We strive to maintain and improve the security of our devices throughout the product lifecycle, including:

- Security by Design
- Security risk management
- Secure coding
- Security scanning and testing
- Responsible vulnerability disclosure processes
- Vulnerability and threat monitoring
- Security patch management
- Incident response
- Information sharing

Baxter maintains continued vigilance for cybersecurity threats and vulnerabilities affecting our products and services. We are dedicated to ensuring that our customers receive information related to these threats, vulnerabilities, and actions to maintain the integrity of our products and the protection of patient data. To fulfill these commitments, Baxter maintains a global Product Security program focused on designing security best practices into our products and maintaining secure operations throughout our product's lifecycle.

Effective security management is a shared responsibility. Our product literature and support teams provide recommended network settings and configurations to enable proper and secure connectivity. We advise customers to conduct a hazards analysis pursuant to ISO/IEC 80001 Application of Risk Management for IT-networks Incorporating Medical Devices prior to deployment to identify and remedy any interoperability issues.

If you would like to report a potential product related privacy or security issue (incident, breach, or vulnerability), please contact productsecurity@Baxter.com or visit https://www.Baxter.com/en/responsible-disclosures/

Contents

1 Product Description 4

2 Hardware Specifications 4

3 Operating Systems 5

4 Third-party Software 5

5 Sensitive Data Transmitted 7

6 Sensitive Data Stored 7

7 Network and Data Flow Diagram 8

8 Malware Protection 9

9 Authentication Authorization 9

10 Network Controls 11

11 Encryption 12

12 Audit Logging 12

13 Remote Connectivity 12

14 Service Handling 12

15 End-of-Life and End-of-Support 13

16 Secure Coding Standards 13

17 System Hardening Standards 13

18 Risk Summary 13

19 Third Party Certification 14

20 Disclaimer 14

1 Product Description

SmartCare Remote Management (SCRM) lets you optimize your healthcare operations by remotely connecting Baxter products for servicing and actionable insights. The system is designed to integrate Baxter vital signs monitors, vision screeners, and hospital beds with real-time tracking and control. The diagram below shows the system deployment landscape. SCRM Actionable Insights hosted on the SCRM platform provides insights into device diagnostic data to assist the Baxter Service team and customers to proactively maintain a healthy fleet.

SCRM Actionable insights is accessible through the SCRM portal. SCRM Actionable insights processes the data offloaded by SCRM to the Lakehouse.

The Lakehouse is a software platform that collects, stores, and processes data in compliance with data privacy and security regulations in the target markets. The Lakehouse provides the infrastructure, data, and governance to support the development of future business intelligence and machine learning applications that turn information into insights to improve outcomes.

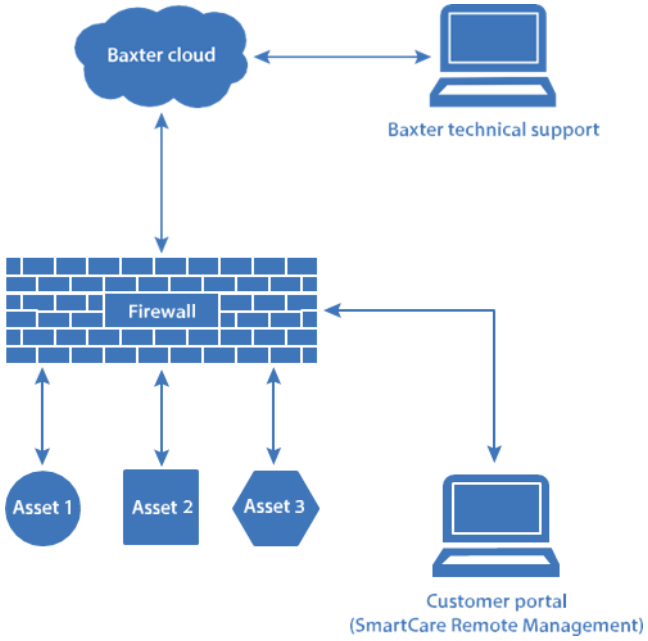


Figure 1 SCRM Landscape.

2 Hardware Specifications

Baxter SmartCare Remote Management is a cloud-based platform hosted on Cumulocity. Cumulocity IoT Cloud is a Software as a Service (SaaS) remote platform that does not require any hardware.

3 Operating Systems

The Cumulocity platform supports the following operating system:

- Rocky Linux 8 (Edge)
- Red Hat Linux Enterprise 8 (Cloud)

Baxter SmartCare Remote Management agents currently support the following operating systems:

- Windows 10 (64-bit)
- Windows Server 2016 (64-bit)
- Windows Server 2019 (64-bit)

4 Third-party Software

Vendor and Name	Version	Description
Keycloak	15.0.1	Keycloak is an OTS open-source Identity and Access Management solution. Its purpose is to link applications (i.e., SCRM, Cumulocity) with identity providers (i.e., Microsoft Azure AD, Google, etc.), providing SSO for the application.
Python Software Foundation Pymssql	2.3.1	A simple database interface for Python that builds on top of FreeTDS to provide a Python DB-API (PEP-249) interface to Microsoft SQL Server.
Microsoft MSAL	1.31.0	The MSAL library for .NET is part of the Microsoft identity platform for developers (formerly named Azure AD) v2.0. It enables you to acquire security tokens to call protected APIs. It uses industry standard OAuth2, and OpenID Connect. The library also supports Azure AD B2C.
Python Software Foundation Requests	2.32.0	Requests is an elegant and simple HTTP library for Python, built for human beings.
HashiCorp Terraform	1.9.7	Terraform codifies cloud APIs into declarative configuration files.
Databricks Databricks CLI	v0.228.1	The Databricks command-line interface (also known as the Databricks CLI) provides a tool to automate the Databricks platform from your terminal, command prompt, or automation scripts.
Databricks runtime: Operating System Ubuntu	22.04.3 LTS	Ubuntu is the world's favorite Linux operating system.

Azul Systems Java	Zulu 8.72.0.17-CA-linux64	Zulu OpenJDK is the Commercial Open Java Development Kit Developed by Azul Systems.
EPFL Scala	2.12.15	A programming language that scales with you: from small scripts to large multiplatform applications.
Python Software Foundation Python	3.10.12	Python is a programming language that lets you work more quickly and integrate your systems more effectively.
CRAN R	4.3.1	R is a free software environment for statistical computing and graphics. It compiles and runs on a wide variety of UNIX platforms, Windows and MacOS.
Linux Foundation Delta Lake	3.0.0	Delta Lake is the universal storage format that unifies analytics and AI on all your data

Network Ports and Services

Port	Protocol	Service Name	Description of Service	Encrypted	Open/Closed
443	TCP/HTTP(s)	Cumulocity IoT platform	Baxter SmartCare Remote Management setting at the top of Cumulocity IoT platform	Yes TLS 1.2 and TLS 1.3	Open
8883	MQTT	Cumulocity IoT platform	Baxter SmartCare Remote Management setting at the top of Cumulocity IoT platform	Yes TLS 1.2	Open
7711	UDP	NRS port	NRS communication facilitate network unicasting over SmartCare Remote Management platform	No	Open
22	TCP(SFTP)	RV700 Fleet Management	RV700 Fleet Management communicates with SmartCare Remote Management	Yes TLS 1.2	Open
283 & 7721	TCP	Welch Allyn Service Monitor	Allow Welch Allyn Service Monitor communicates to a device (CSM, CVSM)	No	Open

Other Cumulocity Platform Ports					
5683, 5684, 5783, 5784	UDP	Cumulocity Platform Service Ports	Facilitate remote connectivity to Cumulocity	Yes DTLS	Open
80, 443, 1883, 8883, 9447, 31010, 8774	TCP	Cumulocity Platform Service Ports	Facilitate remote connectivity to Cumulocity	Yes TLS 1.2/1.3	Open

5 Sensitive Data Transmitted

Baxter SmartCare Remote Management does not transmit PHI.

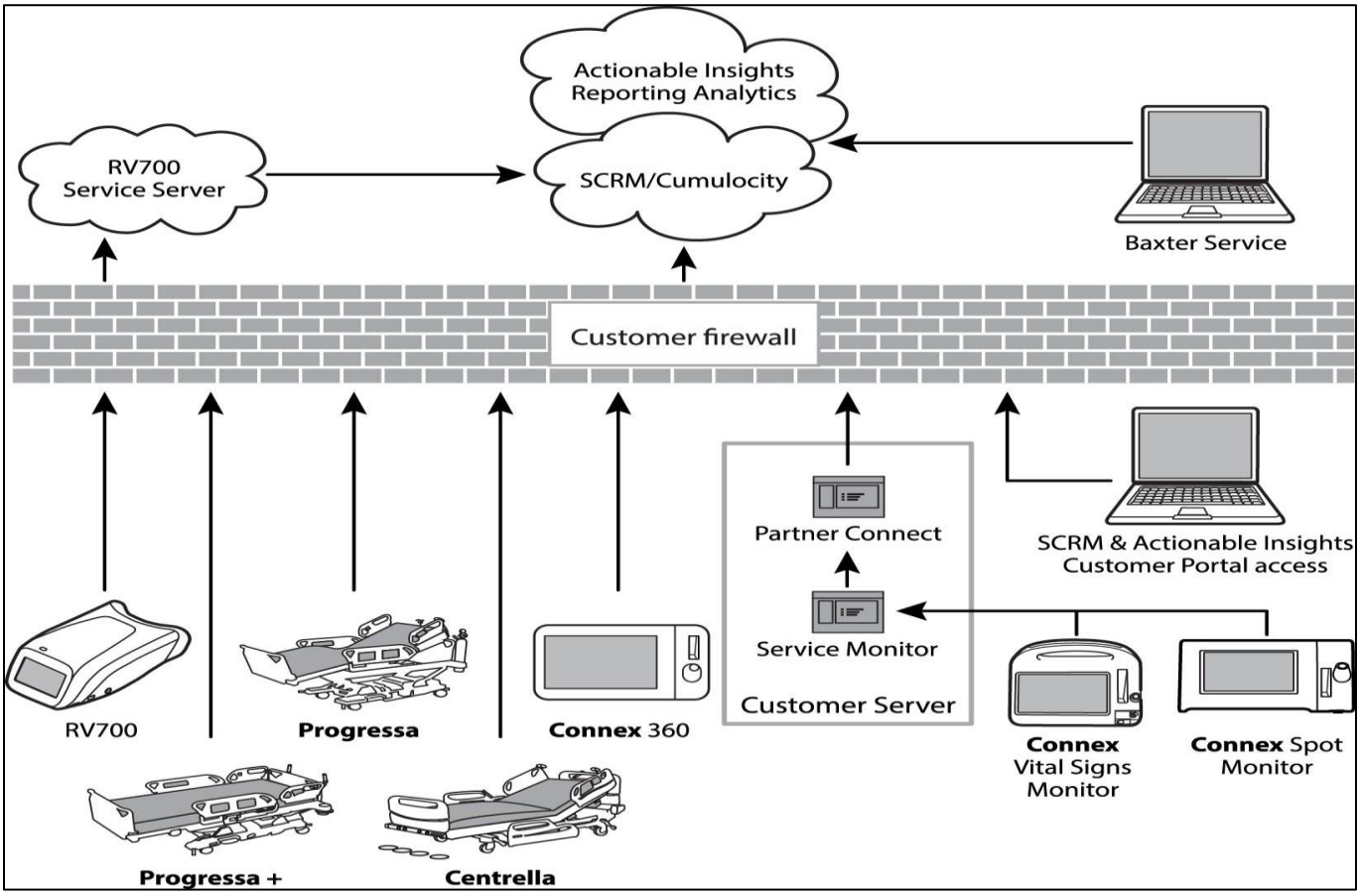
Baxter SmartCare Remote Management does transmit PII such as IP address and location information.

6 Sensitive Data Stored

Baxter SmartCare Remote Management does not store PHI.

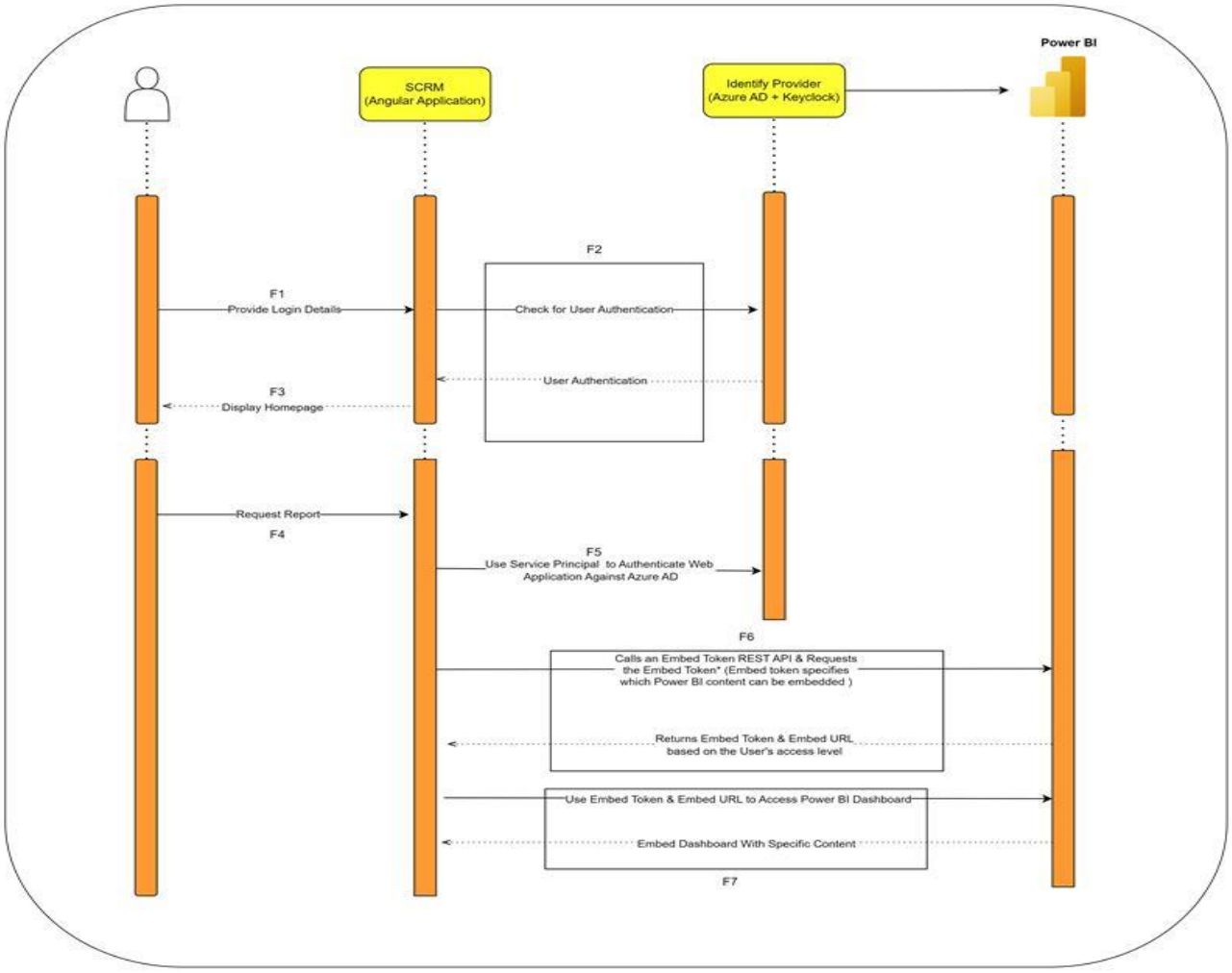
Baxter SmartCare Remote Management does store PII such as IP address and location information.

7 Network and Data Flow Diagram



The following table describes RAMAI data flow and other attributes of the flow.

ID	Data Flow	Sensitive	Authenticated	Encrypted	Protocol
F1	User login Credentials	Y	Y	Y	HTTPS
F2	Authentication	Y	Y	Y	HTTPS
F3	Homepage display	N	Y	N	HTTPS
F4	Report Request	N	Y	Y	HTTPS
F5	Service Authentication	Y	N	Y	App registration key
F6	Embedding report process	Y	Y	Y	HTTPS/Rest API
F7	Using Embed details to get specific content for report	Y	Y	Y	HTTPS



RAM-AI Network Flow Diagram

8 Malware Protection

Microsoft Azure cloud-hosted application is ISO 27001:2013 Compliant (Information Security Management Systems) and SOC 2 type compliant (Data Security). Within the cloud infrastructure, all servers are equipped with the protection tool "Trend Micro Deep Security" that provides antivirus protection, network intrusion detection and prevention, and integrity monitoring.

9 Authentication Authorization

Mutual TLS (mTLS) with Baxter-issued certificates is the authentication method used by Connex360. Communication with Cumulocity is done by HTTPS and Basic access authentication. Cumulocity platform provides Single-Sign-On capability. The feature can be enabled or disabled. The users whose accounts are created through the Cumulocity Portal are called local users. The SSO user accounts are created automatically upon successful user

authentication by the external Identity service. SCRM is linked to the identity services through an identity broker, Keycloak.

SCRM uses a Keycloak v15.0.1 docker image hosted in Azure as an App Service. Identity services will be provided by Baxter Azure AD for internal Baxter users, and Microsoft Azure AD for SCRM customers. Customers must use Microsoft Azure AD as their identity provider to utilize SSO for SCRM.

10 Network Controls

Network Configuration

Application/Service	Domain name, IP address, port	Protocol	Connection
SmartCare Remote Management	https://smartcareremotemanagement.hillrom.com 52.224.38.138 Port: 443 MQTT Port: 8883	TCP (HTTPS)	External
RetinaVue 700 Fleet Management Server	Production Service: https://service.retinavue.net Port:22	TCP (SFTP)	External
DCP	NRS port: 7711	UDP	Internal
Actionable Insights (PowerBI) Backend APIs	*.analysis.windows.net Port: 443	TCP	External
Actionable Insights (PowerBI) Backend APIs	*.pbidedicated.windows.net Ports: 443, 1443	TCP	External
Actionable Insights (PowerBI) Content Delivery Network (CDN)	content.powerapps.com Port: 443	TCP	External
Actionable Insights (PowerBI) Portal	*.powerbi.com Port: 443	TCP	External
Actionable Insights (PowerBI) Power Query Online	*.powerquery.microsoft.com Port: 443	TCP	External
Actionable Insights (PowerBI) Manage gateways, connections, and data policies (preview)	gatewayadminportal.azure.com Port: 443	TCP	External
Actionable Insights (PowerBI) Service telemetry	dc.services.visualstudio.com Port: 443	TCP	External
File outbound types	*.log, *.zip, *.txt, *.csv	Not applicable	External
File inbound types	*.tar.gz, *.tar, *.zip, *.pim, *.xml, *.txt, *.pdf, *.wuupdate, *.bas, *.json, *.csv	Not applicable	External

Browser Information:

- Microsoft Edge: version 89 and higher
- Google Chrome: version 86 and higher
- Apple Safari: iOS 14 and higher

11 Encryption

Data is encrypted at rest and when traveling over network connections, including internal network with Transport Layer Security (TLS 1.2). Encryption keys are stored in Cumulocity Keystores and trust stores.

Communication with Cumulocity is done by HTTPS and Basic access authentication. All passwords of agent and child device credentials are stored encrypted locally on filesystem or in platform.

The cipher suites used for communication are managed by the Cumulocity platform. Baxter monitors the platform to ensure that only state-of-the-art cipher suites are supported and that declared weak cipher suites are deprecated in accordance with industry best practices.

12 Audit Logging

Audit logging is managed by the Cumulocity Audit API resource. The audit API resource returns URIs and URI templates to collections of audit records, so that they can be retrieved by criteria such as "all records from a particular user", or "all records from a particular application".

Audited information:

- Alarm modifications
- Operation modifications
- Two-factor authentication login attempts
- Smart rule modifications
- Complex Event Processing (CEP) module modifications
- User and group permissions modifications
- SSO and OAuth Internal logout and login attempts

13 Remote Connectivity

Remote connectivity to Cumulocity is done through TCP or UDP, depending on the application protocol being used. TCP has TLS 1.2/1.3 support, while UDP has DTLS. Open ports for each:

- UDP: 5683, 5684, 5783, 5784
- TCP: 80, 443, 1883, 8883, 9447, 31010, 8774

14 Service Handling

Baxter IT assists with the creation of user groups that can create and support customer accounts. There is no PHI involved in any maintenance of SCRM.

15 End-of-Life and End-of-Support

Baxter will support and maintain the remote platform by consistently providing newer versions with required features as per Business need until it is no longer supported by Baxter. At this point, there is no defined end-of-life support time length.

16 Secure Coding Standards

Cumulocity aligns with the framework and controls matrix of the CSA Security, Trust & Assurance Registry (STAR) program. The STAR program is a provider assurance program of self-assessment, third-party audit, and continuous monitoring. These assessments are available to customers upon request. All products go through an automated source code security static analysis on a regular basis. The source or the binary security scanning is automated using industry-standard state-of-the-art tools. Cumulocity IoT uses OWASP Top 10 and the OpenSAMM security framework.

Baxter SmartCare Remote Management development follows a "**C coding standard**". This is a standard developed to minimized bugs in firmware by focusing on practical rules that keep bugs out, while also improving the maintainability and portability of embedded software.

17 System Hardening Standards

Remote platform hardening is performed according to CIS Benchmarks Level 1 profile. The Level 1 profile is considered a base recommendation that can be implemented reasonably promptly and is designed not to have an extensive performance impact. The intent of the Level 1 profile benchmark is to lower the attack surface to Cumulocity while keeping machines usable and not hindering Cumulocity business functionality. Beside these, the Baxter security team conducts regular security vulnerability scanning, a Static Application Security Testing (SAST), and penetration testing before any major release. Other system hardening standards are listed in the below table:

Name of Standard
IEC 80001-2-2
ISO IEC 27001
ISO IEC-62305

18 Risk Summary

A security risk assessment was completed on the remote platform. Risks were assessed based on threat, impact, and vulnerability. Vulnerability scanning was completed by Baxter FLC security team; no critical, high, or medium findings were identified. In addition, penetration testing was completed by Cumulocity, and no critical, high, medium findings were identified on the cloud platform. The Cumulocity current penetration testing report is available for review and can be provided upon request.

19 Third Party Certification

Cumulocity aligns with the framework and controls matrix of the CSA Security, Trust & Assurance Registry (STAR) program, a provider assurance program of self-assessment, third-party audit and continuous monitoring. The Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) program is the industry's leading trust mark for cloud security.

The CSA Open Certification Framework (OCF) is a program for flexible, incremental, and multi-layered CSP certifications according to the CSA's industry leading security guidance. The OCF/STAR program comprises a global cloud computing assurance framework with a scope of capabilities, flexibility of execution, and completeness of vision that far exceeds the risk and compliance objectives of other security audit and certification programs.

For all cloud hosted products, the Cumulocity security team performs security penetration testing based on OWASP Top 10 for each cloud release. Whenever there is a new release, Cumulocity performs security penetration testing on the cloud hosted product.

In addition, the Cloud Security, Compliance, and Certifications teams engage with an external security testing company to perform regular penetration testing for standard Cloud services. Baxter also performs internal penetration testing on the application whenever a new software version is released, as required by our Product Security SOP. The frequency varies based on our yearly project roadmap.

Physical access to the data center or hosting facility is controlled and monitored by Cumulocity. Microsoft is responsible for all physical access controls to SaaS for Cumulocity Cloud Services. Microsoft takes a layered approach to physical security, to reduce the risk of unauthorized users gaining physical access to data and the datacenter resources. Datacenters managed by Microsoft have extensive layers of protection: access approval at the facility's perimeter, at the building's perimeter, inside the building, and on the datacenter floor.

20 Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and Baxter, or Baxter subsidiaries or affiliates (collectively, "Baxter"). Baxter does not make any promises or guarantees to customer that any of the methods or suggestions described in this Product Security White Paper will restore customer's systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper.