blueprism®

Blue Prism 이 보안 로봇 프로세스 자동화의 표준을 어떻게 정하는가

Introduction

비즈니스 민첩성과 보안 관리 간의 적절한 균형을 유지하는 것은 모든 조직에게 매우 중요합니다. 클라우드 기반이든 인터넷 지원이든 상관없이 회사에 새로운 기술 접점을 도입할 때마다 새로운 보안 위험을 해결해야 합니다.
동시에, 혁신과 경쟁력이 발휘되기 위해서는 RPA(로봇 프로세스 자동화) 기술의 제어가 기업 전체의 비즈니스 리더와 함께 이루어져야 합니다.

이를 자신 있게 완전히 달성하려면 사용하기 쉬우면서도 각 산업에서 요구하는 높은 컴플라이언스 및 보안 표준을 엄격하게 준수하는 자동화 플랫폼이 필요합니다. 일부 부문에서는 실패 비용으로 인해 막대한 벌금이 부과되고 심지어 징역형에 처해질 수 있습니다.

내장된 디지털 작업자의 보안 자격 증명은, 가장 까다로운 엔터프라이즈 환경 내에서도 신뢰하며 작동할 수 있음을 의미합니다.

Blue Prism 의 연결된 RPA 기술은 디지털 작업자를 배치하여 인간과 동일한 방식으로 프로세스 자동화를 수행하도록 설계되었기 때문에 고유합니다.
디지털 워커의 기본 제공 보안 자격 증명은 가장 까다로운 엔터프라이즈 환경에서 작동하도록 신뢰할 수 있음을 의미합니다. 디지털 작업자는 협업 플랫폼을 통해 비즈니스 사용자가 운영하지만 가장 규제가 심한 비즈니스 부문을 포함하여 IT 부서의 전체 거버넌스 및 보안 내에서 여전히 작동합니다.

Blue Prism 의 연결된 RPA 기술은 사용자 인터페이스를 기계 인터페이스로 용도로 변경하여, 시스템 상호 운용성의 30 년 간의 통합 과제를 해결했습니다. 이 혁신을 통해 디지털 워커는 인간과 동일한 IT 시스템 및 메커니즘을 사용하고 액세스할 수 있으므로 기계 API 와 독립적으로 과거, 현재 또는 미래 시스템의 프로세스를 자동화할 수 있습니다.

연결된 RPA 를 사용하면 비즈니스 사용자가 코딩 없이 디지털 작업자를 교육하고 실행하므로 시스템 인프라가 손상되지 않고, 웹 서비스 및 코드 단계를 사용할 수 있지만 거의 필요하지 않습니다.

연결된 RPA 가 보안성, 지속성 및 회복탄력성을 대규모로 제공하려면 자동화를 신중하게 계획하고 모델링 및 설계를 해야 합니다. 이는 비즈니스 사용자가 직관적인 프로세스 순서도를 그리고 설계함으로써 자동화된 프로세스를 생성할 수 있고, 디지털 작업자가 작업을 자동화하는 데 사용할 수 있음을 의미합니다. 작업의 문서화는 실제 작업이 됩니다. 문서를 변경하면 작업이 즉시 변경됩니다. 디지털 작업자가 실행하는 프로세스 모델은 각 자동화 프로세스의 프로세스 순서도에 명시되어 있습니다. 프로세스 순서도는 감사 및 변경 통제 대상입니다. 이 접근 방식은 모든 문서가 연결된 RPA 플랫폼 내에서 안전하게 관리되므로 매우 보안성이 높고 컴플라이언스를 준수합니다.

연결된 RPA 는 또한 비즈니스 사용자가 전체 비즈니스에서 관리하고 재사용하는 중앙 기능 풀에 자동화를 추가하여 협업할 수 있도록 합니다. 디지털 작업자의 결정과 행동도 중앙에서 관제되고 감사되며, 인간이 수행하는 교육 이력도 마찬가지입니다. 프로세스의 중요한 부분인 이는 연결된 RPA 플랫폼 전체의 모든 활동에 대한 포괄적인 감사를 제공합니다.

조직은 최고 수준의 Veracode Verified 인증(회사의 보안 소프트웨어 개발 프로세스를 검증하는 제 3 자 자격 증명)을 입증할 수 있는 RPA 공급업체만 고려해야 합니다.

Blue Prism 은 Verified Level 5 를 달성한 최초의 RPA 공급업체입니다. 이 인증은 Blue Prism 이 진정으로 구축된 엔터프라이즈급 보안 솔루션에 중점을 둘 뿐만 아니라 회사 고유의 제품 개발 방법론의 일부임을 보여줍니다.

안전한 소프트웨어 개발 수명 주기

Blue Prism 의 제품 개발 방법론은 소프트웨어 및 서비스의 설계 및 개발의 모든 단계를 알리는 포괄적인 보안 보증 프로세스를 따릅니다. 이 접근 방식은 취약성과 위협을 예측, 식별 및 완화하는 데 도움이 됩니다. Blue Prism 이 매우 안전하게 유지되도록, 모범 사례를 활용하여 이 접근 방식을 지속적으로 검토합니다.

인증 및 컴플라이언스

RPA 의 혜택을 가장 많이 받는 기업에는 컴플라이언스 및 데이터 보안 절차에 가장 관심이 많은 기업(예: 보험 회사, 은행, 금융 기관, 정부 기관, 의료 제공자)이 포함됩니다. 그들은 RPA 제공업체가 사이버 보안 및 정보 제어 표준 및 정책을 충족할 것으로 기대합니다. Blue Prism 은 PCI-DSS(Payment Card Industry Data Security Standards), HIPAA(Health Insurance Portability and Accountability Act) 및 SOX(Sarbanes-Oxley Act) 준수 프로세스를 지원하며 필요한 보안 및 거버넌스를 제공하기 위한 제어 기능을 갖추고 있습니다.

Blue Prism 은 Veracode 와 계약하여 정기적인 제품 취약성 분석을 수행합니다. Veracode 는 다음과 같은 업계 모범 사례 보안 방법론을 사용하여 애플리케이션 보안 및 취약성에 대한 공정하고 안정적이며 독립적인 검증을 제공합니다.

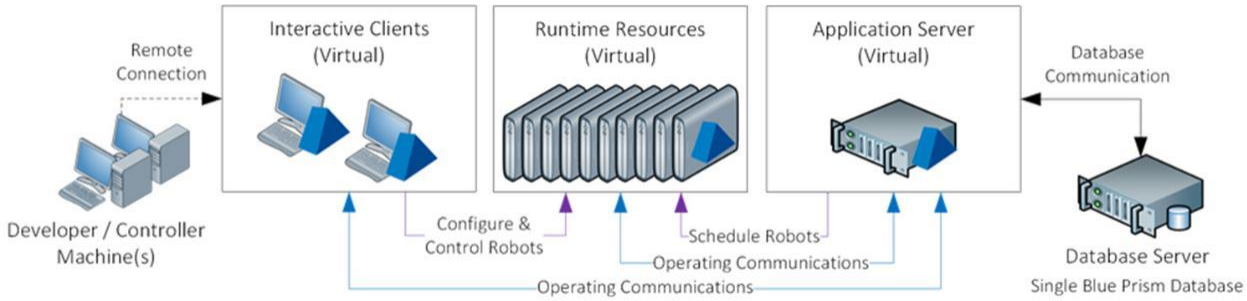
Industry best practice security methodologies:

- PCI DSS
- PCI PA-DSS
- OWASP
- 2011 CWE/SANS Top 25
- SEI CERT C Secure Coding Standard

- PCI DSS: PCI DSS 는 업계 전반에 걸쳐 안전하고 표준화된 솔루션이 사용되도록 보장하고 사기 가능성을 최소화하기 위해 식별 가능한 카드 소유자 데이터의 저장 및 처리에 적용되는 일련의 기술, 관리 및 절차 규칙입니다. Blue Prism 은 고객이 PCI 호환 솔루션의 일부로 Robotic Process Automation 을 구현할 수 있도록 최적화되어 있습니다.
- PCI PA-DSS: PCI PA-DSS(Payment Application Data Security Standard) 요구 사항은 PCI DSS 요구 사항 및 보안 평가 절차에서 파생됩니다.
- OWASP: OWASP(Open Web Application Security Project) Top 10 은 애플리케이션 보안에 대한 편견 없는 실용적인 정보를 제공하는 데 전념하는 비영리 조직이며, 가장 중요한 웹 애플리케이션 보안 결함에 대한 광범위한 합의를 나타냅니다.
- The 2011 CWE (Common Weakness Enumeration)/SANS Top 25 가장 위험한 프로그래밍 오류는 심각한 소프트웨어 취약점으로 이어질 수 있는 가장 심각한 오류 목록입니다. 이 목록의 오류는 자주 발생하며 종종 쉽게 찾아 악용될 수 있습니다. 공격자가 소프트웨어를 가로채거나 데이터를 훔치거나 소프트웨어가 전혀 작동하지 못하게 하므로 위험합니다. CWE/SANS Top 25 는 소프트웨어에 이러한 오류가 포함되어 있지 않다는 증거가 없이는 웹 애플리케이션이 아닌 애플리케이션을 고객에게 제공할 수 없을 정도로 현재 만연하고 심각한 결함 목록입니다.
- CERT Secure Coding: 시큐어 코딩으로 개발하면 기업이, 악용 가능한 취약점을 유발할 가능성이 가장 높은 소프트웨어 결함을 피할 수 있습니다. SEI(Software Engineering Institute) CERT C 코딩 표준(2016 년판)은 오늘날 가장 널리 퍼져 있는 소프트웨어 취약점의 근본 원인을 식별하고, 악용 방법을 보여주고, 잠재적인 결과를 검토하고, 안전한 대안을 제시합니다.
- HIPAA: HIPAA 는 의료 산업에 대한 일련의 미국 연방 입법 요구 사항이며 무엇보다도 PHI(건강 정보 보호)의 관리, 처리, 저장 및 전송에 대한 표준 및 요구 사항을 포함합니다.

아키텍처(Architecture)

Blue Prism 은 사설 클라우드("온프레미스"라고도 함) 또는 공용 클라우드에서 가장 일반적으로 호스팅됩니다. Blue Prism 의 실행은 업무 부서가 주도이지만 플랫폼은 IT 부서에서 배포, 관리 및 관리하는 것이 좋습니다.



The basic components of the Blue Prism architecture

표준 Blue Prism 아키텍처는 4 가지 주요 구성 요소로 구성됩니다.

- Blue Prism Runtime Resource: 일반적으로 '디지털 워커'라고 하며 자동화된 프로세스의 실행을 담당하는, 일반적인 표준 최종 사용자 데스크톱의 가상화된 인스턴스입니다. 이러한 구성 요소에는 일반적으로 향상된 물리적 보안 및 원격 접근 통제가 필요합니다.
- Blue Prism Interactive Client: 환경 전반에 걸쳐 Blue Prism 프로세스의 설정, 개발, 구성, 스케줄링 및 모니터링을 용이하게 하는 최종 사용자 데스크탑 프로그램(물리적 또는 가상)입니다. 일반적으로 다른 Blue Prism 구성 요소와 함께 데이터 센터에서 가상화되지만 이 프로그램은 최종 사용자의 데스크톱에 직접 배포할 수도 있습니다.
- Blue Prism Application Server: Blue Prism 서버 서비스는 Blue Prism 구성 요소와 데이터베이스 간의 모든 연결을 마샬링합니다. 일반적으로 가상 Windows Server 로 프로비저닝되는 이 구성 요소에 의해 활성화되는 주요 기능에는 보안 자격 증명 관리, 데이터베이스 연결 마샬링, 데이터 암호화 및 예약된 프로세스 실행이 포함됩니다.
- Microsoft SQL Server 데이터베이스는 프로세스 정의, 로그, 감사 및 사용자 정보를 보관하는 중앙 저장소로 사용됩니다. Blue Prism 구성 요소의 연결은 Blue Prism 응용 프로그램 서버를 통해서만 가능합니다.

암호화(Encryption)

DATA AT REST

저장 중인 데이터란 물리적으로 존재하는 임의의 디지털 형식의 비활성 데이터를 나타냅니다. Blue Prism 은 인정된 암호화 표준만 사용하며, FIPS(연방 정보 처리 표준) 호환 옵션을 포함합니다.

최종 사용자는 알고리즘을 선택하고 암호화 키를 생성하며 키 저장 위치를 지정할 수 있습니다. Blue Prism 제품에는 암호화 키 순환을 용이하게 하는 도구가 있습니다.

사용자 구성 가능한 암호화 키 관리:

다음 정보는 사용자 구성 가능한 암호화에 사용되는 암호화 키가 생성되는 방법과 저장 위치에 대해 설명합니다.

- Blue Prism Application Server (recommended): 암호화 키는 Application Server 에 저장되며 키는 환경 내의 각 Application Server 에 수동으로 배포되어야 합니다. 이것은 키가 암호화된 데이터와 별도로 저장되도록 하기 때문에 가장 일반적으로 선택되는 시나리오입니다. Application Server 를 통해 연결하는 클라이언트를 지원합니다.

- Database: 암호화 키는 Blue Prism 데이터베이스에 저장됩니다. 이는 배포된 Application Server 가 없는 시나리오에 적합합니다. 데이터베이스에 직접 연결하는 클라이언트와 애플리케이션 서버를 통해 연결하는 클라이언트를 지원합니다.

Blue Prism 데이터베이스의 일부 정보는 테이블의 행 내에 암호화된 데이터로 저장됩니다. 이렇게 하면 데이터베이스가 손상된 경우에도 데이터가 노출되기 위해 암호를 해독해야 합니다. 기본적으로 이 정보는 AES 암호화를 사용하여 대칭적으로 암호화됩니다. 또한 기본 Microsoft 암호화 메커니즘을 통해 데이터베이스 암호화를 제공할 수 있습니다. 그렇지만 Transparent Data Encryption(TDE)는 최종 사용자가 구현해야 합니다.

DATA IN USE

사용 중인 데이터는 일반적으로 컴퓨터 랜덤 액세스 메모리, CPU 캐시 또는 CPU 레지스터에 있는 비영구적 디지털 상태에 저장된 활성 데이터를 나타냅니다.

Blue Prism 은 .Net 프레임워크에 내장된 Microsoft 의 Secure String 기능을 사용합니다. 보안 문자열은 더 이상 필요하지 않을 때 컴퓨터 메모리에서 삭제하는 것과 같이 기밀로 유지되어야 하는 텍스트를 나타냅니다. Blue Prism Safe String 은 .NET Framework 에 내장된 Secure String 을 둘러싼 래퍼입니다. 암호와 같은 민감한 정보가 메모리에서 처리될 때 손상될 수 없는 안전한 컨테이너에 보관되도록 합니다. 공격자가 그 당시 애플리케이션의 메모리 스냅샷을 검사할 수 있었더라도 민감한 정보는 노출되지 않을 것입니다.

DATA IN MOTION

이동 중인 데이터는 네트워크를 통과하거나 컴퓨터 메모리에 일시적으로 상주하여 읽거나 업데이트되는 데이터를 나타냅니다. Blue Prism 은 각 런타임 리소스에 적절한 인증서를 수동으로 배포하고 장치의 시작 매개변수를 업데이트하여 인증서 기반 암호화를 적용할 것을 권장합니다.

TCP connections:

Blue Prism 은 .NET Framework 버전 4.7 을 기반으로 합니다. .NET Framework 4.7 이상 버전은 기본적으로 호스트 운영 체제 구성으로 설정되어 최상의 보안 프로토콜과 버전을 자동으로 선택합니다. 이것은 TCP, WCF 및 HTTP 기반 통신에 적용됩니다. 사용 가능한 프로토콜 및 암호는 최종 사용자가 관리하거나 Microsoft 보안 업데이트를 통해 자동으로 처리됩니다. Blue Prism 6.1 ~ 버전 6.5 TLS1.2 는 TCP 및 HTTP 프로토콜에 적용되었습니다. 이것은 버전 6.6 이상에서 위의 것을 사용하도록 변경되었습니다.

WCF Connections:

Blue Prism 에서 사용되는 WCF 연결에는 다음과 같은 사용자 선택 가능한 암호화 방법이 있습니다.

- 메시지 암호화 및 Windows 인증
- 전송 암호화 및 Windows 인증
- 전송 암호화
- 없음(디버그 전용)

메시지 수준 암호화에 사용되는 WCF 구성은 프로그래밍 방식으로 생성되며 변경할 수 없는 AES256 의 .NET 표준 암호화 체계를 사용합니다. Blue Prism 구성 요소가 Active Directory 네트워크 인프라 내에 배포되고 적절한 도메인 신뢰로 구성되면 구성 요소 간 통신에 대해 기본적으로 통신 메시지 보안이 활성화됩니다. 메시지 보안을 활성화하여 연결을 보호하는 방법에 대한 추가 정보는 보안 네트워크 연결 데이터 시트에 나와 있습니다.

써드파티 암호화 기능

Blue Prism 에서 사용하는 암호화 기능은 다음 제 3 사 제품에서 제공합니다.

- **Microsoft Windows Operating System**
- **Microsoft .Net Framework**
- **Microsoft Windows Communication Foundation (WCF)**
- **Microsoft SQL Server**

Database connections: 이것은 Application Server 와 데이터베이스 간의 읽기/쓰기 연결입니다. 인증서 기반 암호화는 자체 서명된 인증서를 자동 생성하거나 기존의 확인 가능한 인증서를 활용할 수 있는 SQL Server 기능을 활용하여 지원됩니다.

난독화(OBFUSCATION)

암호화 외에도 Blue Prism 은 난독화 알고리즘을 사용합니다. 난독화는 덜 명확하고 이해하기 어렵게 만들어 민감한 정보 공개의 위험을 줄이는 데 도움이 되며 다른 기존 기술이나 제어를 보완하는 데 자주 사용됩니다.

- 암호 난독화: 주로 자격 증명(Blue Prism 자격 증명 관리자) 정보를 난독화하는 데 사용됩니다.
- 단순 난독화: 경계를 넘어 직렬화/역직렬화되는 정보를 난독화하는 데 주로 사용됩니다.

- 소스 코드 난독화: Blue Prism 소스 코드는 업계 최고의 난독화 도구를 사용하여 대부분 난독화됩니다. 소스 코드 난독화는 작업의 복잡성과 수행에 필요한 시간을 증가시켜 성공적인 리버스 엔지니어링 및 악의적인 패치의 위험을 크게 줄입니다.

FIPS 140-2 COMPLIANCE

버전 6.6 에서는 FIPS 호환 알고리즘을 적용하는 장치에서 Blue Prism 을 사용할 수 있습니다. 이를 구현하기 위해 Blue Prism 이 FIPS 를 준수하도록 몇 가지 변경이 이루어졌습니다. Blue Prism 응용 프로그램 서버, 대화형 클라이언트 및 런타임 리소스는 이제 암호화, 해싱 및 서명에 FIPS 호환 알고리즘을 사용하는 그룹 정책이 활성화되어 있는지 확인합니다. 활성화된 경우 대화형 클라이언트의 암호화 구성표 및 작업 대기열 시스템 설정에서 비 FIPS 호환 암호화 구성표를 선택할 수 없습니다. 또한 애플리케이션 서버에 대한 암호화 체계를 구성할 때 선택할 수 없으며 FIPS 규격이 아닌 옵션을 사용하는 AutomateC 명령을 실행할 수 없습니다.

인증 관리(Authentication)

ACTIVE DIRECTORY INTEGRATION

.Net System.Security 및 SystemDirectoryServices 네임스페이스를 사용하는 Blue Prism 은 Active Directory(AD) 도메인 서비스를 활용하여 다양한 엔터프라이즈급 기능을 제공합니다. Active Directory 는 기업 배포에 권장되는 접근 방식인 기존 보안 정책에 따라 Blue Prism 플랫폼에 대한 사용자 액세스를 관리하고 제어하는 데 사용됩니다. 또한 Active Directory 를 사용하여 구성 요소 간 메시지 보안을 제공할 수 있습니다.

Blue Prism 플랫폼은 다음과 같은 엔터프라이즈급 기능을 활성화하기 위해 Active Directory 네트워크 인프라 내에 배포되어야 합니다.

- Blue Prism Platform(Active Directory Domain Services 에서 제공)을 위한 SSO(Single Sign-On).
- SSO 를 위해 Blue Prism 을 Active Directory 와 통합하면 Active Directory 의 기능을 활용하여 플랫폼에 대한 사용자 액세스를 검증할 수 있습니다. 이 접근 방식은 로그온 프로세스를 단순화할 뿐만 아니라 사용자 액세스 제어를 기존 네트워크 보안 정책과 일치시킵니다. 이를 위해서는 사용자의 AD 계정, Blue Prism 서버 및 사용자가 액세스할 모든 Blue Prism 장치(예: 대화형 클라이언트 및 런타임 리소스)가 공통 Active Directory 포리스트 내에 있어야 합니다.
- 런타임 리소스 도메인 계정 인증. Blue Prism 런타임 리소스가 도메인 계정을 사용하여 인증하도록 구성된 경우 SSO 방법을 활용하여 프로세스 자동화의 일부로 사용되는 비즈니스 애플리케이션 및 시스템을 인증할 수 있습니다.

LOGIN AGENT

로그인 에이전트 기능을 사용하면 런타임 리소스에서 사용자 세션을 원격으로 초기화하고 닫을 수 있습니다. 이렇게 하면 런타임 리소스가 필요하지 않을 때 "로그아웃" 상태가 될 수 있으므로 의도하지 않은 상호 작용이 방지됩니다. 로그인 에이전트는 보안 Credentials Manager 에서 로그인 자격 증명을 가져옵니다.

MULTIFACTOR AUTHENTICATION

MFA(다단계 인증)는 인증 메커니즘에 둘 이상의 증거(또는 요소)를 성공적으로 제시한 후 액세스 권한을 부여합니다.

- 사용자만 아는 것
- 사용자만 가진 것
- 사용자만 그런 것

디지털 워커:

MFA 의 요구 사항은 인간의 취약성을 피하는 것입니다. 그러나 디지털 워커는 본질적으로 인간보다 더 안전합니다. 예를 들어 디지털 워커는:

- 클라이언트 자체 방화벽 내의 안전한 환경에서 작업합니다.
- 인터넷 연결을 통해 전 세계의 시스템과 네트워크에 접속하지 않습니다.
- 비밀번호를 적어두거나 사람처럼 공개하지 않습니다.
- 피싱, 숄더 서핑 또는 폭력적인 위협에 취약하지 않습니다.
- 비밀번호를 자주 변경하고 길고 복잡한 비밀번호를 쉽게 처리하도록 구축할 수 있습니다.

Interactive clients:

Blue Prism 은 현재 제품 내에서 MFA 에 대한 기본 지원을 제공하지 않습니다(즉, 최소 두 가지 인증 형식을 사용하여 제품에 로그인). 이는 SSO 가 Blue Prism 내에서 구성된 경우 운영 체제에 위임되고 사용자가 소프트웨어에 로그인할 때 수행할 수 있습니다.

Third-party applications:

대상 응용 프로그램의 MFA 요구 사항은 대상 응용 프로그램의 기능과 지원 여부에 따라 전적으로 결정됩니다. 필요한 경우 물리적 토큰은 적절하지 않지만 사용할 수 있는 몇 가지 대안이 있습니다.

- Software tokens: 많은 토큰 기반 인증 체계는 API 또는 "소프트웨어 토큰" 옵션과 함께 제공되며 물리적 토큰 대신 이를 사용할 수 있습니다. 소프트 토큰 옵션의 몇 가지 예에는 가상 모바일을 통한 SMS, OTP 등이 있습니다. 동일한 소프트웨어 및 보안 서버이지만 하드웨어 토큰은

디지털 작업자가 있는 가상 머신에 있는 소프트웨어를 통해 에뮬레이트됩니다. Blue Prism Digital Exchange(DX): https://digitalexchange.blueprism.com 에서 사용할 수 있는 MFA 에 대한 몇 가지 옵션이 있습니다.

- Smart cards: 일부 조직에서는 스마트 카드를 비롯한 다른 형태의 2 단계 인증을 사용합니다. Blue Prism 은 하드웨어 스마트 카드 장치로 인증 프로세스를 자동화한 광범위한 경험을 보유하고 있습니다.

그러나 Blue Prism 은 이러한 상황에서 MFA 에 대한 모든 요구 사항을 검토하여 디지털 작업자에 대한 필요성을 고려할 것을 권장합니다.

권한 관리(Authorization)

Blue Prism 구현의 일부로 사용자 계정이 필요한 몇 가지 상호 작용이 있습니다. 이러한 예는 다음과 같습니다.

- 네트워크 또는 작업 그룹에 대해 인증하기 위해 런타임 리소스에서 사용하는 상호 작용
- 대상 애플리케이션에 액세스하고 자동화하는 데 사용되는 런타임 리소스
- Blue Prism 컨트롤러 및 개발자가 프로세스 및 관련 대기열, 일정 및 설정을 구성, 개발, 릴리스 및 배포하는 데 사용하는 상호 작용

다음과 같은 경우에도 보안을 고려해야 합니다.

- 다양한 Blue Prism 구성 요소(예: 애플리케이션 서버 또는 런타임 리소스)에 대한 액세스(원격 액세스 포함)

  Blue Prism 환경 내에서 각 사용자의 행동에 부여된 논리적 접근 권한

사용자 계정: 런타임 리소스 네트워크 인증(RUNTIME RESOURCE NETWORK AUTHENTICATION)

런타임 리소스가 도메인 또는 작업 그룹에 대해 인증될 때 사용자 계정이 사용되는 경우 고려 사항은 다음과 같습니다.

- 응용 프로그램 서버 또는 런타임 리소스와 같은 다양한 Blue Prism 구성 요소에 대한 접근(원격 액세스 포함)
- 각 사용자의 작업에 부여된 논리적 접근 권한으로 Blue Prism 환경 내에서 사용 가능

사용자 계정: 대상 애플리케이션(TARGET APPLICATIONS)

Blue Prism 런타임 리소스는 각 사업부 또는 자동화된 타사 응용 프로그램에 대한 적절한 액세스 권한이 있어야 합니다. 적절한 권한이 있는 사용자 계정은 주어진 애플리케이션에 동시 연결을 가질 각 런타임 자원에 대해 사용 가능하도록 하는 것이 좋습니다. Blue Prism 런타임 리소스가 공유 자격 증명을 사용하도록 지원도 제공됩니다.

이러한 사용자 계정에 대한 자격 증명은 프로세스 정의와 관계없이 중앙 집중식 자격 증명 관리 저장소에 안전하게 저장됩니다. 환경 내에서 무단 사용을 방지하기 위해 특정 자격 증명에 대한 액세스는 특정 런타임 리소스, 프로세스 및 사용자로 제한됩니다. Blue Prism 프로세스는 이러한 응용 프로그램 암호를 주기적으로 변경하도록 구성할 수 있으므로 사용자가 자격 증명을 알 수 없습니다.

사용자 계정: BLUE PRISM USERS (CONTROLLERS / DEVELOPERS)

기본적으로 Blue Prism 의 기본 인증은 Blue Prism 애플리케이션에 대한 사용자 액세스를 관리하고 각 사용자에게 적절한 제어 및 권한을 할당하는 데 사용됩니다. 또는 Blue Prism 을 Active Directory 도메인 서비스와 통합하여 사용자 액세스 및 제어를 제어 및 구성할 수 있습니다.

선택한 인증 유형에 관계없이 사용자 액세스는 역할 기반이며 각 환경에 대해 독립적으로 구성되어 특정 사용자가 환경에 따라 다른 액세스 권한을 가질 수 있도록 하고 단일 사용자가 모든 환경에서 전체 액세스 권한을 갖지 못하도록 제한합니다.

구성해야 하는 논리적 액세스 권한은 프로젝트 시작의 일부이며 Blue Prism 은 맞춤형 보안 역할과 즉시 사용 가능한 보안 역할의 혼합 사용을 지원하여 각 사용자에게 각 환경에서 적절한 액세스 권한을 할당합니다.

이 정의의 일부로서 자주 검토되는 역할의 예는 다음과 같습니다.

- 프로세스 생성, 읽기, 편집, 삭제
- 비즈니스 객체 생성, 읽기, 편집, 삭제
- 프로세스 또는 비즈니스 객체 비교, 내보내기, 가져오기
- 릴리스 패키지 정의, 릴리스 생성
- 일정 생성, 편집, 삭제
- 대기열/세션에 대한 전체 또는 읽기 전용 액세스
- 시스템 설정, 사용자, 자격 증명 등을 정의하기 위한 액세스

다양한 환경에서 적절한 수준의 제어 및 거버넌스를 제공하기 위해 구현될 논리적 액세스 제한을 설정해야 합니다. 여기에는 다음이 포함될 수 있습니다.

- 프로덕션 환경에서 발생하는 모든 개발 방지
- 다양한 환경 간에 프로세스(및 관련 항목)를 마이그레이션할 수 있는 사용자 제한
- 설정, 구성 및 사용자 액세스를 담당할 사용자 식별
- 다양한 유형의 감사 및 로그에 액세스할 수 있는 사용자 식별

다중 팀(MULTI-TEAMS)

MTE(다중 팀 환경) 기능을 통해 조직은 기존 역할 기반 액세스 제어를 확장하여 Blue Prism 내에서 점점 더 복잡해지는 보안 구성을 모델링할 수 있습니다.

더 세분화된 구성을 가능하게 합니다. 이러한 기능을 통해 조직은 비즈니스 객체 및 런타임 리소스와 같은 Blue Prism 자산을 주어진 Blue Prism 환경 내에서 여러 팀과 공유할 수 있습니다. MTE 기능을 사용하면 자산 유형 및 자산의 계층 구조별로 권한을 할당할 수 있습니다. 예를 들어, 팀의 구성원인 사용자는 일부 비즈니스 개체에 대한 전체 액세스 권한을 가질 수 있지만 다른 객체를 보거나 실행할 수 있는 권한만 가질 수 있습니다.

자격 증명 관리(Credentials Management)

CREDENTIAL MANAGER

자격 증명 관리 기능은 런타임 리소스가 대상 응용 프로그램에 액세스하는 데 필요한 로그인 세부 정보를 위한 보안 저장소를 제공합니다. 자격 증명은 Blue Prism 데이터베이스에 저장되며 클라이언트가 정의한 암호화 체계를 사용하여 암호화됩니다. 암호화 키는 Blue Prism Application Server 시스템에 별도로 저장되며 검증된 클라이언트에 자격 증명을 제공하는 데 사용됩니다.

사이버아크에 연결하기(CONNECTING TO CYBERARK)

Blue Prism CyberArk 통합을 사용하면 기존 기능을 사용하여 Blue Prism 환경 내에서 컨텍스트에 대한 제어를 유지하면서 CyberArk 자격 증명 저장소에서 자격 증명을 검색할 수 있습니다. 통합은 Blue Prism Digital Exchange(DX): https://digitalexchange.blueprism.com/dx/search?keyword=cyberark 에서 사용할 수 있습니다. 대체 통합도 DX 에서 사용할 수 있습니다.

Network Connectivity

진화하는 네트워크 인프라와의 호환성을 보장하기 위해 Blue Prism 은 모든 연결에 대해 IPv4 또는 IPv6 네트워크 프로토콜을 사용하는 환경과 두 프로토콜의 조합을 활용하는 하이브리드 접근 방식을 사용하는 환경에 배포할 수 있습니다. 이를 통해 모든 Blue Prism 구성 요소(런타임, 클라이언트, 애플리케이션 서버)가 선호되거나 가장 적합한 방법을 사용하여 연결할 수 있습니다.

Blue Prism 플랫폼에는 데이터베이스 및 런타임 리소스에 대한 연결과 같은 여러 통신 채널이 있습니다. 모두 기본적으로 암호화되거나 인증서를 통해 암호화가 적용될 수 있습니다. 구성 요소 간 통신에 대한 자세한 내용은 참조 아키텍처 가이드에 대해 Blue Prism 에 문의하십시오.

Default Ports

While all ports used by each component are configurable, the default ports are detailed below.

Component	Default Port Information
Application Server	• Listens for TCP traffic on 8199 (configurable)
Interactive Client	• Retrieve information from the server via WCF
Runtime Resources	• Listens for TCP traffic on 8181 (configurable) • Retrieves information from the server via WCF

Where there are multiple Application Servers co-hosted on a single operating system, it is common for each to use an independent, dedicated port. This may be common where there are multiple Blue Prism environments.

Where there are a multiple Runtime Resources configured on a single Runtime Resource, each will be configured to listen on an independent, dedicated port.

로깅 및 모니터링(Logging and Monitoring)

로깅 및 감사(LOGGING AND AUDIT)

Session logging

Blue Prism 프로세스에는 런타임 리소스가 프로세스 실행의 일부로 따르는 여러 단계가 포함되어 있습니다. 이러한 단계는 계산, 결정, 사용자 인터페이스 요소에서 데이터 읽기, 하위 프로세스 또는 작업 실행을 비롯한 다양한 작업을 나타낼 수 있습니다. 세션은 Blue Prism 에서 비즈니스 프로세스 실행의 일부로 런타임 리소스가 뒤따르는 모든 적절한 단계를 기록하는 데 사용됩니다. 프로세스 설계의 일부로 각 단계의 로깅의 양을 설정합니다.

작업 대기열 (Work queues)

작업 대기열은 프로세스에 대한 저장 및 워크플로 기능을 제공합니다. 각 작업 항목은 데이터, 상태 및 기록과 같은 개별 레코드를 나타냅니다. 작업 항목에는 보류, 지연, 잠김, 완료 및 종료를 비롯한 여러 상태가 있습니다. 작업 항목이 프로세스에 의해 종료되면 자동으로 재시도될 수 있습니다. 각 대기열은 설정된 자동 재시도 횟수로 구성할 수 있습니다.

감사 로그 (Audit logs)

Blue Prism 의 감사 추적은 중앙에 저장되고 변조되지 않으므로 아무도 변경하거나 위조할 수 없습니다. 비준수 또는 감사의 경우 이 기능은 반박할 수 없는 부인 방지를 제공합니다.

감사 로그는 다음 작업을 기록하는 데 사용됩니다.

- 로그인/로그아웃
- 환경 전체 설정 변경
- 비즈니스 객체, 프로세스 및 대기열 생성/업데이트/삭제

프로세스 및 객체에 대한 변경 사항을 기록할 때 모든 변경 사항 세부 정보가 캡처되어 비교 또는 롤백이 가능합니다.

스케줄 로그 (Schedule logs)

로그는 각 일정에 대해 생성되고 해당 일정 내의 모든 작업 및 세션에 대한 시간과 결과를 기록합니다.

모니터링 및 경고(MONITORING AND ALERTING)

플랫폼 모니터링 (Platform monitoring)

Blue Prism 인프라는 여러 구성 요소로 구성되며 각 구성 요소는 모니터링 및 폴링을 통해 가용성과 응답성을 확인할 수 있습니다. Blue Prism 구성 요소를 모니터링할 때 표준 타사 도구 및 기술을 사용하여 다음을 평가할 수 있습니다.

- 할당된 하드웨어의 상태(예: 디스크 공간, CPU 사용률, 네트워크 연결)
- 특정 Windows 서비스의 가용성(예: 서비스 시작, 적절한 포트에서 응답)
- Windows 이벤트 뷰어 항목

경고 (Alerting)

예외에서 프로세스 완료에 이르기까지 관련 당사자에게 알리도록 구성할 수 있는 몇 가지 경고 유형이 있습니다. 경고 유형은 다음과 같습니다.

- 프로세스 경고: Blue Prism 환경 내에서 선택된 프로세스에 대해 특정 작업이 발생할 때 지정된 사용자에게 알리고 사용자별로 구성됩니다. 사용자는 모니터링할 프로세스, 알리고 싶은 작업 및 알림 방법을 선택할 수 있습니다.
- 일정 알림: Blue Prism 환경 내에서 선택한 일정에 대해 특정 작업이 발생하면 지정된 사용자에게 알리고 사용자별로 구성됩니다. 사용자는 모니터링할 일정과 알림 방법을 선택할 수 있습니다. 또한 일정에 따라 알림이 필요한지 또는 더 자세한 일정-작업 수준에서 알림이 필요한지 선택할 수 있습니다.
- 사용자 지정 알림: 추가 또는 특정 알림이 필요한 경우 모든 프로세스에 사용자 지정 알림 알림을 설계할 수 있습니다.

APIs

Web API 기능은 게시된 HTTP API 를 제공하는 시스템 및 서비스와의 기본 상호 작용을 구성하기 위한 인터페이스를 제공합니다. 이들 중 가장 일반적인 것은 RESTful 웹 서비스입니다. 웹 API 서비스 기능을 사용하면 Blue Prism 프로세스가 이러한 서비스와 상호 작용하고 자동화된 비즈니스 프로세스 내에서 이러한 외부 시스템에서 제공하는 데이터 또는 서비스를 제공하거나 사용할 수 있습니다. Web API 기능이 기본적으로 제공하는 기능을 통해 Blue Prism 은 가장 일반적인 서비스를 자동화할 수 있으며, 이러한 기능은 맞춤형 또는 복잡한 데이터 구조 및 인증 메커니즘을 수용하기 위해 코드 단계를 사용하여 확장될 수 있습니다.

Controls

로봇 운영 모델 (THE ROBOTIC OPERATING MODEL)

Blue Prism ROM(로봇 운영 모델)은 사용자가 RPA 배포를 효과적으로 관리하고 성공적으로 확장할 수 있도록 설계된 프레임워크입니다. ROM 에는 논리적 액세스 모델 및 프로세스 거버넌스를 비롯한 제어에 대한 조언과 지침이 포함되어 있습니다. https://blueprism.com/rom/에서 자세히 알아보십시오.

논리적 접근 모델 (LOGICAL ACCESS MODELS)

Blue Prism 은 처음부터 각 조직이 자체 LAM(논리적 접근 모델)을 만들고 구현할 것을 권장합니다. 이것은 Blue Prism 배포의 일부로 포함되어야 합니다. 제품 내에 정의된 기본 사용자 역할은 조직의 자체 LAM 에서 정의한 사용자 역할로 대체되어야 합니다. 이 작업은 각 Blue Prism 환경, 즉 개발, UAT 및 프로덕션에 대해 수행되어야 합니다.

런타임 리소스 및 시스템 관리자 사용자 역할은 변경할 수 없습니다. LAM 을 만들거나 업데이트하는 프로세스에는 RPA 책임자, RPA 거버넌스 이사회 및 IT 팀을 비롯한 모든 이해 관계자가 참여해야 합니다. 업무 분담도 조직 내에서 고려해야 합니다. LAM 템플릿 및 가이드는 ROM 의 일부로 제공됩니다.

변화 관리 (CHANGE MANAGEMENT)

디지털 인력을 배포하고 유지 관리할 때 조직은 기존 변경 제어 프로세스를 따르는 것이 좋습니다. ROM 은 프로세스가 정의, 설계, 구축, 검토, 테스트 및 출시되는 방법을 설명하는 제공 모범 사례에 대한 지침을 제공합니다.

추가 고려 사항

침투 테스트 (PENETRATION TESTING)

블루 프리즘은 "모범 사례" 환경에서 수행되는 타사 침투 테스트를 거칩니다. 이러한 테스트의 주관적인 특성과 각 클라이언트 환경의 고유한 변수로 인해 보고된 결과는 지침으로만 사용해야 합니다. 테스트 방법 및 결과에 대한 자세한 내용은 최신 Blue Prim Veracode 애플리케이션 보안 보고서에서 확인할 수 있습니다.

결론

Blue Prism 은 항상 보안을, 연결된 RPA 기술의 핵심 구성 요소로 삼았으며, 이는 최초의 Veracode Verified Level 5 RPA 공급업체로 입증되었습니다. 가장 완벽한 엔터프라이즈급 보안을 제공하는 Blue Prism 의 중앙 집중식 데이터 센터 호스팅 방식은, IT 가 관리하는 비즈니스 운영 플랫폼이 가장 안정적이고 안전함을 보장합니다. 암호화를 통해 쉽게 배포할 수 있는 추가 암호화 옵션으로 데이터를 보호할 수 있습니다. 유연하고 강력한 인증 및 권한 부여 기능을 통해 조직은 표준 운영 절차에 맞는 디지털 인력을 배치할 수 있습니다. 광범위한 로깅 및 경고 옵션은 디지털 워커와 Blue Prism 사용자 모두에게 완벽한 가시성과 감사 추적을 보장합니다.

이러한 모든 강력한 기능은 접근 관리 모델 및 전달 방법론을 포함하는 업계 최고의 ROM 의 강력한 거버넌스 및 제어 기능에 의해 뒷받침됩니다. 궁극적으로, 연결된 RPA 는 인간과 디지털 작업자가 실제 디지털 혁신을 안전하게 제공할 수 있는 가장 안전한 협업 플랫폼을 제공합니다.

blueprism®

블루프리즘 소개

RPA(로보틱 프로세스 자동화)의 선구자인 Blue Prism 은 Fortune 500 대 기업 및 공공 부문에서 신뢰받는, 안전한 지능형 자동화 솔루션입니다. 오늘날 Blue Prism 의 연결된 RPA 는 접근 가능한 고급 인식 기술 및 전문가 커뮤니티를 갖춘 운영 리더와 함께 21 세기 인력의 역량을 강화하는 동시에 인간과 디지털 워커 간의 격차를 해소합니다.

1,000 개 이상의 주요 기업에서 사용하는 온프레미스, 클라우드 또는 하이브리드 클라우드 환경의 통합 솔루션으로, 연결된 RPA 를 활용하여 직원들이 수십억 시간의 작업을 다시 비즈니스에 반환하면서 수십억 건의 트랜잭션을 자동화할 수 있도록 지원합니다.

www.blueprism.com 을 방문하십시오.