Dell Threat Defense

설치 및 관리자 가이드

Cylance 기반

v17.11.06

2017 년 11 월 6 일

차례

개요

Cylance 기반 Dell Threat Defense 는 장치에 영향을 미치기 전에 맬웨어를 감지 및 차단합니다. Cylance 는 수학적 접근 방식을 통해 사후 방식의 서명, 신뢰 기반 시스템 또는 샌드박스가 아닌 기계 학습을 사용하여 맬웨어를 식별합니다. 이러한 접근 방식으로 새로운 맬웨어나 바이러스, 또는 봇을 비롯해 향후 나타날 수 있는 변종까지 무력화합니다. Threat Defense 는 잠재적 파일 실행을 분석하여 운영 체제의 맬웨어를 찾아냅니다.

본 가이드에서는 Threat Defense 콘솔의 사용법, Threat Defense 에이전트 설치, 그리고 콘솔과 에이전트의 구성 방법에 대해서 설명합니다.

작동 원리

Threat Defense 는 작은 용량의 에이전트가 각 호스트마다 설치되어 클라우드 기반 콘솔과 통신합니다. 에이전트는 테스트를 통과한 수학적 모델을 사용해 호스트에 존재하는 맬웨어를 감지 및 차단할 뿐만 아니라 지속적인 클라우드 연속성이나 서명 업데이트가 필요하지 않고, 개방되거나 격리된 네트워크 모두에서 실행 가능합니다. 위협 환경이 끊임없이 진화를 거듭한다고 하지만 Threat Defense 역시 마찬가지입니다. 엄청난 양의 실제 데이터 세트에 대한 지속적인 트레이닝으로 Threat Defense 는 항상 공격자보다 한 발 앞서 나갈 것입니다.

- **위협**: 위협 요소를 장치에 다운로드하거나, 혹은 익스플로잇 시도가 있는 경우
- **위협 감지**: Threat Defense 에이전트의 위협 식별 방법
    - **프로세스 스캔**: 장치에서 실행 중인 프로세스를 스캔합니다.
    - **실행 제어**: 실행할 때만 프로세스를 분석합니다. 여기에는 시작과 함께 실행되는 파일, 자동 실행으로 설정되어 있는 파일, 그리고 사용자가 직접 실행하는 파일까지 모두 포함됩니다.
- **분석**: 파일의 악성 또는 안전성 여부를 식별하는 방법.
    - **위협 점수의 클라우드 조회**: 클라우드의 수학적 모델로서 파일에 점수를 할당하는 데 사용됩니다.
    - **로컬**: 에이전트에 추가되는 수학적 모델. 장치가 인터넷에 연결되지 않아도 분석이 가능합니다.
- **작업**: 파일이 위협 요소로 식별되었을 때 에이전트가 하는 작업.
    - **전역**: *전역 격리* 및 *안전 목록* 등 정책 설정을 확인합니다.
    - **로컬**: 수동으로 *격리*되거나 *면제*된 파일을 확인합니다.

본 가이드 정보

사용자는 끝점에 에이전트를 설치하기 전에 먼저 클라우드 기반 콘솔에 대해 알아두는 것이 좋습니다. 끝점의 관리 방식에 대해 알아두면 보안 및 유지보수가 더욱 쉽습니다. 따라서 이러한 워크플로우를 권장합니다. 사용자는 이해하기 쉽도록 환경에 배포하는 접근 방식을 취할 수 있습니다.

예: 영역은 조직에서 장치를 그룹화하는 데 효과적입니다. 예를 들어 영역 규칙으로 영역을 구성하면 새로운 장치가 선택한 기준(운영 체제, 장치 이름 또는 도메인 이름 등)에 따라 자동으로 영역에 추가됩니다.

참고: 정책 및 영역에 대해 먼저 설명한 후 에이전트 설치에 대한 지침이 이어집니다. 하지만 필요하다면 에이전트 설치부터 시작할 수도 있습니다.

콘솔

Threat Defense 콘솔은 로그인하여 조직의 위협 정보를 확인할 수 있는 웹사이트를 말합니다. 콘솔에서는 장치를 그룹으로 구분하거나(영역), 장치에서 위협 요소가 발견되었을 경우 필요한 작업을 구성하거나(정책), 설치 파일을 다운로드(에이전트)하는 일이 매우 쉽습니다.

Threat Defense 콘솔은 다음 언어를 지원합니다.

프랑스어	독일어	이탈리아어	일본어
포르투갈어(이베리아)	한국어	스페인어	포르투갈어(브라질)

표 1: 지원되는 Threat Defense 콘솔 언어

로그인

계정을 활성화하면 Threat Defense 콘솔에 대한 로그인 정보가 이메일로 사용자에게 발송됩니다. 이메일에 포함된 링크를 클릭하면 로그인 페이지로 이동하거나, 혹은 아래와 같은 웹페이지로 이동할 수 있습니다.

- 북미 지역: http://dellthreatdefense.com
- 유럽: http://dellthreatdefense-eu.cylance.com

장치 정책

발견되는 맬웨어에 대한 에이전트의 처리 방식을 정의하는 것이 정책입니다. 예를 들어 특정 폴더에 있는 경우 자동으로 맬웨어를 *격리*하거나 무시합니다. 모든 장치는 정책을 따라야 하며, 장치 1 개에 적용할 수 있는 정책의 수도 1 개로 제한됩니다. 장치를 단일 정책으로 제한할 경우 해당 장치에서 허용해야 하는 파일을 차단하는 등 기능이 서로 충돌하는 것을 방지할 수 있습니다. 할당된 정책이 없을 때는 장치가 기본 정책으로 할당됩니다.

기본 정책에서는 실행 제어만 활성화되기 때문에 실행하는 경우에 한해 프로세스를 분석합니다. 이 경우에도 기본적으로 장치를 보호하기 때문에 장치에서 실행되는 작업을 중단할 필요는 없으며, 정책을 프로덕션 환경에 배포하기 전에 먼저 정책 기능을 테스트할 수 있는 시간도 충분합니다.

정책을 추가하는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 정책 생성은 관리자만 가능하기 때문입니다.
2. **설정** > **장치 정책**을 선택합니다.
3. **새 정책 추가**를 클릭합니다.
4. 정책 이름을 입력하고 정책 옵션을 선택합니다.
5. **생성**을 클릭합니다.

파일 작업

설정 > 장치 정책 > [정책 선택] > F 파일 작업

파일 작업에서는 Threat Defense 에서 감지되는 파일에 대한 처리 옵션을 *안전하지 않음* 또는 *비정상*으로 제공합니다.

팁: *안전하지 않음* 또는 *비정상* 파일 분류에 대한 자세한 내용은 보호 - 위협 섹션을 참조하십시오.

실행 제어를 이용한 자동 격리

이 기능은 *안전하지 않음* 또는 *비정상* 파일을 *격리* 또는 차단하여 이러한 파일이 실행되는 것을 방지합니다. 파일을 *격리*하면 파일이 원래 위치에서 *격리* 디렉터리인 **C:\ProgramData\Cylance\Desktop\q** 로 이동합니다.

맬웨어 중에는 특정 디렉터리에 있는 다른 파일을 삭제하는(drop) 맬웨어가 있습니다. 이러한 맬웨어는 파일이 성공적으로 삭제될 때까지 계속해서 시도합니다. 하지만 Threat Defense 가 삭제된 파일을 수정하여 이러한 유형의 맬웨어가 계속해서 제거된 파일을 삭제하지 못하도록 막습니다.

팁: 적은 수의 장치에서 *자동 격리*를 테스트한 후 프로덕션 환경에 적용하는 것이 좋습니다. 테스트 결과를 보면서 비즈니스에 중요한 응용 프로그램 실행이 차단되지 않는지 확인해야 합니다.

자동 업로드

안전하지 않음 및 *비정상* 파일 모두에 자동 업로드를 활성화하는 것이 좋습니다. Threat Defense 는 감지된 *안전하지 않음* 또는 *비정상* 파일을 Cylance Infinity 클라우드에 자동으로 업로드하여 파일을 심층적으로 분석하고 추가 세부 정보를 제공합니다.

Threat Defense 는 알 수 없는 PE(Portable Executable) 파일만 업로드하여 분석합니다. 조직의 여러 장치에서 알 수 없는 파일이 동일하게 발견되면 Threat Defense 가 파일을 1 개만 업로드하여 분석합니다. 여기에서 파일 1 개란 장치마다 파일 1 개를 의미하지 않습니다.

정책 안전 목록

안전하다고 판단되는 파일을 정책 수준에 따라 추가합니다. 에이전트는 이 목록의 파일에 대해 위협 요소 작업을 적용하지 않습니다.

다른 수준(*로컬*, *정책* 또는 *전역*)에서 파일 예외 처리(*격리* 또는 *안전*)에 대한 자세한 내용은 부록 B:예외 처리를 참조하십시오.

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 정책 생성은 관리자만 가능하기 때문입니다.
2. **설정** > **장치 정책**을 선택합니다.
3. 새로운 정책을 추가하거나 기존 정책을 편집합니다.
4. *정책 안전 목록*에서 **파일 추가**를 클릭합니다.
5. **SHA256** 정보를 입력합니다. 옵션으로서 알고 있는 경우에 한해 MD5 와 파일 이름을 추가합니다.
6. 이 파일의 용도를 식별할 수 있도록 **범주**를 선택합니다.
7. 이 파일을 *정책 안전 목록*에 추가하는 이유를 입력합니다.
8. **제출**을 클릭합니다.

보호 설정

설정 > 장치 정책 > [정책 선택] > 보호 설정

실행 제어

Threat Defense 는 항상 악의적인 프로세스의 실행 여부를 감시하여 *안전하지 않음* 또는 *비정상* 실행 시도가 있는 경우 경고를 표시합니다.

장치의 서비스 종료 방지

이 기능을 선택하면 수동이든 다른 프로세스든 상관없이 Threat Defense 서비스가 종료되는 것을 방지합니다.

맬웨어 샘플 복사

맬웨어 샘플을 복사할 네트워크 공유 위치를 지정할 수 있습니다. 네트워크 공유를 지정하면 사용자가 Threat Defense 에서 *안전하지 않음* 또는 *비정상*으로 간주된 파일을 분석할 수 있습니다.

- CIFS/SMB 네트워크 공유를 지원합니다.
- 네트워크 공유 위치를 1 개 지정합니다. 예: **`c:\test`**
- 중복 파일을 포함해 기준을 만족하는 모든 파일이 네트워크 공유 위치로 복사됩니다. 고유성 테스트는 실시하지 않습니다.
- 파일이 압축되지 않습니다.
- 파일이 암호로 보호되지 않습니다.

경고: 파일이 암호로 보호되지 않습니다. 따라서 부주의로 악성 파일을 실행하지 않도록 주의가 필요합니다.

스크립트 제어

스크립트 제어는 악의적인 Active 스크립트와 PowerShell 스크립트가 실행되지 않도록 차단하여 장치를 보호합니다.

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **장치 정책**을 선택합니다.
3. 정책을 선택하고 **보호 설정**을 클릭합니다.
4. 확인란을 선택하여 **스크립트 제어**를 클릭합니다.
    a. **경고**: 환경에서 실행되는 스크립트를 모니터링합니다. 초기 배포 시 권장됩니다.
    b. **차단**: 특정 폴더에서 실행되는 스크립트만 허용합니다. Alert!(경고) 모드를 먼저 테스트한 후 사용하십시오.
    c. **이러한 폴더 및 하위 폴더에서 스크립트 승인**: 스크립트 폴더를 제외할 때는 폴더의 상대 경로를 지정해야 합니다.

d. **PowerShell 콘솔 사용 차단**: PowerShell 콘솔 실행을 차단합니다. PowerShell 의 온라인 사용을 방지하여 보안을 강화합니다.

   참고: 스크립트 제어가 PowerShell 콘솔을 차단하도록 설정된 경우 스크립트에서 PowerShell 콘솔을 실행하면 스크립트가 실패합니다. PowerShell 스크립트를 적용하려면 사용자가 PowerShell 콘솔이 아닌 스크립트를 변경하도록 권장합니다.

5. **저장**을 클릭합니다.

에이전트 로그

설정 > 장치 정책 > [정책 선택] > 에이전트 로그

콘솔에서 에이전트 로그를 활성화하면 로그 파일이 업로드되어 콘솔에서도 볼 수 있습니다.

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **장치 정책**을 선택합니다.
3. 정책을 선택하고 **에이전트 로그**를 클릭합니다. 로그 파일에서 선택한 장치가 이 정책에 할당되어 있는지 확인합니다.
4. **로그 파일 자동 업로드 활성화**를 선택하고 **저장**을 클릭합니다.
5. **장치** 탭을 클릭하고 장치를 선택합니다.
6. **에이전트 로그**를 클릭합니다. 로그 파일이 표시됩니다.
7. 로그 파일을 클릭합니다. 로그 파일 이름은 로그 날짜에 따라 결정됩니다.

정책 모범 사례

정책을 처음 생성할 때는 단계적 접근 방식으로 정책 기능을 구현하여 성능 및 작업에 영향을 미치지 않도록 하는 것이 좋습니다. 또한 추가 기능을 활성화하여 새로운 정책을 생성할 때는 환경에서 Threat Defense 의 작동 원리를 이해하는 것이 중요합니다.

1. 초기 정책을 생성할 때 **자동 업로드**만 활성화합니다.

   a. 에이전트는 실행 제어 및 프로세스 모니터링 기능을 사용하여 실행 중인 프로세스만 분석합니다.

      여기에는 시작과 함께 실행되는 파일, 자동 실행으로 설정되어 있는 파일, 그리고 사용자가 직접 실행하는 파일까지 모두 포함됩니다.

      에이전트는 경고 메시지만 콘솔에게 보냅니다. 파일이 차단되거나 *격리*되지 않습니다.

b. 콘솔의 위협 경고 메시지 유무를 확인하십시오.

끝점에서 실행해야 하는 응용 프로그램 또는 프로세스 중에서 위협 요소(*비정상* 또는 *안전하지 않음*)로 판단되는 응용 프로그램 또는 프로세스를 찾기 위해서입니다.

위협 요소를 찾은 경우 이러한 파일의 실행을 *허용*하려면 정책 또는 콘솔 설정을 구성합니다. 예를 들어, 정책에서 폴더를 *제외*하거나 해당 장치의 파일을 *면제*하거나 *안전 목록*에 파일을 추가합니다.

c. 먼저 하루 동안 초기 정책을 사용하여 일반적으로 장치에 사용되는 응용 프로그램 및 프로세스를 실행한 후 분석하십시오.

중요: 장치에서 정기적으로(1 개월 1 회 등) 실행되는 응용 프로그램이나 프로세스 중에서도 위협 요소로 판단되는 응용 프로그램이나 프로세스가 있을 수도 있습니다. 초기 정책에서 자동 업로드 기능을 실행할 것인지, 아니면 예약 실행할 때 장치를 모니터링할 것인지 결정하는 것은 사용자의 몫입니다.

2. 실행 제어 및 프로세스 모니터링 완료 후 보호 설정에서 **안전하지 않은 실행 프로세스 삭제**를 활성화합니다.

   안전하지 않은 실행 프로세스와 그 하위 프로세스까지 종료를 활성화하면 위협이 감지되었을 때(EXE 또는 MSI) 상태와 상관없이 프로세스(및 하위 프로세스)가 종료됩니다.

3. 파일 작업에서 **자동 격리**를 설정합니다.

   *자동 격리*는 모든 유해한 파일을 *격리* 폴더로 이동합니다.

4. 보호 설정에서 **스크립트 제어**를 설정합니다.

   스크립트 제어는 악의적인 스크립트가 장치에서 실행되지 못하도록 차단하여 사용자를 보호합니다.

   사용자는 특정 폴드에서 실행되는 스크립트만 허용할 수 있습니다.

   스크립트 제어 폴더를 제외할 때는 폴더의 상대 경로를 지정해야 합니다.
   예:**`\Cases\ScriptsAllowed`**

영역

영역은 장치를 구성 및 관리할 수 있는 방법입니다. 예를 들어 지역이나 기능에 따라 장치를 분할 구성할 수 있습니다. 미션 크리티컬 장치를 위한 그룹이 있으면 이 장치들을 하나의 그룹으로 구성하여 최우선순위를 영역에 할당할 수 있습니다. 그 밖에도 정책이 영역 수준으로 적용되기 때문에 장치에 적용되는 정책에 따라 해당 장치들을 모두 하나의 영역으로 그룹화할 수 있습니다.

조직은 관리자에게만 액세스가 허용되는 기본 영역(미지정 영역)이 있습니다. 장치를 영역에 자동 할당하는 영역 규칙이 없다면 새로운 장치는 미지정 영역으로 할당됩니다.

영역 관리자와 사용자를 영역에 할당하면 이들은 영역의 구성 방식을 볼 수 있습니다. 이에 따라 영역 관리자와 사용자는 자신이 관리하는 장치에 액세스할 수 있습니다. 영역은 영역 관리자 또는 사용자 역할을 하는 모두가 볼 수 있도록 1 개 이상 생성해야 합니다.

하나의 장치가 다중 영역에 속할 수는 있지만, 장치 1 개에 적용할 수 있는 정책의 수는 1 개로 제한됩니다. 다중 영역을 허용하기 때문에 장치의 그룹 방식에서도 유연성을 발휘할 수 있습니다. 장치를 단일 정책으로 제한할 경우 해당 장치에서 *허용*해야 하는 파일을 차단하는 등 기능이 서로 충돌하는 것을 방지할 수 있습니다.

장치가 다중 영역에 속할 수 있는 이유는 다음과 같습니다.

- 장치는 수동으로 다중 영역에 추가됩니다.
- 장치는 1 개 이상의 영역 규칙을 따릅니다.
- 장치는 먼저 1 개 영역에 포함되며 이후 다른 영역의 규칙을 따릅니다.

영역을 사용하는 권장 방법은 영역 관리 모범 사례를 참조하십시오.

영역을 추가하는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 영역 생성은 관리자만 가능하기 때문입니다.
2. **영역**을 클릭합니다.
3. **새 영역 추가**를 클릭합니다.
4. 영역 이름을 입력하고, 정책을 선택하고, 값을 선택합니다. 영역은 정책과 연동되어야 합니다. 값이란 영역의 우선순위를 말합니다.
5. **저장**을 클릭합니다.

장치를 영역에 추가하는 방법

1. 관리자 또는 영역 관리자 계정으로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **영역**을 클릭합니다.
3. *영역 목록*에서 영역을 클릭합니다. 해당 영역의 현재 장치가 페이지 하단의 *영역 장치 목록*에 표시됩니다.

4. **장치를 영역에 추가**를 클릭합니다. 장치 목록이 표시됩니다.
5. 영역에 추가할 장치를 각각 선택하고 **저장**을 클릭합니다. (선택사항) **선택한 장치에 영역 정책 적용**을 선택합니다. 장치를 영역에 추가하더라도 영역 정책까지 자동으로 적용되지는 않습니다. 이는 영역이 해당 장치의 정책 관리가 아니라 장치를 구성하는 데 사용될 수도 있기 때문입니다.

영역을 제거하는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 영역 제거는 관리자만 가능하기 때문입니다.
2. **영역**을 클릭합니다.
3. 제거할 영역의 확인란을 선택합니다.
4. **제거**를 클릭합니다.
5. 선택한 영역을 제거할지 확인하는 메시지에서 **예**를 클릭합니다.

영역 속성

영역 속성은 필요에 따라 편집할 수 있습니다.

영역 우선순위 정보

영역은 속한 장치의 중요성 또는 위험 상태에 따라 우선순위가 분류되어(낮음, 보통, 높음) 다르게 할당됩니다. 대시보드의 일부 섹션에서는 장치가 우선순위를 기준으로 표시되어 즉시 문제를 해결해야 하는 장치를 식별하는 데 도움이 됩니다.

우선순위는 영역을 생성할 때 또는 영역을 편집할 때 설정하여 우선순위 값을 변경할 수 있습니다.

영역 속성을 편집하는 방법

1. 관리자 또는 영역 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **영역**을 클릭합니다.
3. *영역 목록*에서 영역을 클릭합니다.
4. 영역 이름을 변경하려면 **이름** 필드에 새 이름을 입력합니다.
5. 정책을 변경하려면 **정책** 드롭다운 메뉴에서 다른 정책을 선택합니다.
6. **낮음**, **보통** 또는 **높음** 값을 선택합니다.
7. **저장**을 클릭합니다.

영역 규칙

장치는 일정한 기준에 따라 자동으로 영역에 할당할 수 있습니다. 이 자동화 기능은 다수의 장치를 영역에 추가할 때 유용합니다. 단, 새로운 장치를 영역에 자동 할당할 때는 추가할 장치가 해당 영역 규칙을 만족해야 합니다. **모든 기존 장치에 지금 적용**을 선택한 경우 규칙과 일치하는 모든 기존 장치는 해당 영역에 추가됩니다.

참고: 영역 규칙에 따라 장치가 영역으로 자동 추가되기는 하지만 영역 규칙이 장치를 제거할 수는 없습니다. 장치의 IP 주소나 호스트 이름을 변경하더라도 해당 장치가 영역에서 제거되지는 않습니다. 장치는 수동으로만 영역에서 제거할 수 있습니다.

영역 규칙을 만족하는 장치를 영역에 추가할 때 영역 정책을 적용할 수 있는 방법이 있습니다. 이 말은 장치의 기존 정책이 특정 영역 정책으로 바뀐다는 것을 의미합니다. 따라서 영역 규칙을 기준으로 정책을 자동 적용할 때는 주의가 필요합니다. 장치가 영역 규칙을 만족했다는 이유로 관리가 부실할 경우에는 잘못된 정책에 할당될 수도 있기 때문입니다.

콘솔의 장치 세부 정보 페이지를 보면서 어떤 정책이 장치에 적용되는지 확인하십시오.

영역 규칙을 추가하는 방법

1. 관리자 또는 영역 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **영역**을 클릭하고 *영역 목록*에서 영역을 선택합니다.
3. 영역 규칙에서 **규칙 생성**을 클릭합니다.
4. 선택한 영역의 기준을 지정합니다. 더하기 기호를 클릭하여 조건을 추가합니다. 빼기 기호를 클릭하여 조건을 제거합니다.
5. **저장**을 클릭합니다.

영역 규칙 기준

- **새 장치를 조직에 추가하는 경우**: 새로운 장치를 조직에 추가할 때는 영역 규칙을 만족하는 장치가 영역에 추가됩니다.
- **장치의 속성이 변경되었을 때**: 기존 장치의 속성이 변경되어 영역 규칙을 만족할 때는 기존 장치가 영역에 추가됩니다.
- **범위 내 IPv4 주소**: IPv4 주소 범위를 입력합니다.

- **장치 이름**:
    - 시작 문자: 장치 이름은 이 문자열로 시작해야 합니다.
    - 포함: 장치 이름은 이 문자열을 포함해야 하지만 이름에 포함되는 위치는 어디든 상관없습니다.
    - 끝 문자: 장치 이름은 이 문자열로 끝나야 합니다.
- **운영 체제**:
    - 일치: 운영 체제가 선택한 시스템이어야 합니다.
    - 제외: 운영 체제가 선택한 시스템이 아니어야 합니다. 예를 들어 영역 규칙에 따라 운영 체제가 Windows 8 이 아니어야 하는 경우에는 Windows 이외의 장치를 포함해 모든 운영 체제가 이 영역에 추가됩니다.
- **도메인 이름**:
    - 시작 문자: 도메인 이름은 이 문자열로 시작해야 합니다.
    - 포함: 도메인 이름은 이 문자열을 포함해야 하지만 이름에 포함되는 위치는 어디든 상관없습니다.
    - 끝 문자: 도메인 이름은 이 문자열로 끝나야 합니다.
- **고유 이름**:
    - 시작 문자: 고유 이름은 이 문자열로 시작해야 합니다.
    - 포함: 고유 이름은 이 문자열을 포함해야 하지만 이름에 포함되는 위치는 어디든 상관없습니다.
    - 끝 문자: 고유 이름은 이 문자열로 끝나야 합니다.
- **(LDAP) 구성원**:
    - 일치: (그룹) 구성원이 이것과 일치해야 합니다.
    - 포함: (그룹) 구성원이 이것을 포함해야 합니다.
- **다음 조건 충족**:
    - All(모두): 영역 규칙의 모든 조건을 충족해야 장치가 추가됩니다.
    - Any(1 개 이상): 영역 규칙의 조건을 1 개 이상 충족해야 장치가 추가됩니다.

- **영역 정책 적용**:
    - Do not apply(적용하지 않음): 장치를 영역에 추가할 때 영역 정책은 적용하지 않습니다.
    - Apply(적용): 장치를 영역에 추가할 때 영역 정책을 적용합니다.

      경고: 영역 정책을 자동으로 적용할 경우 일부 네트워크 장치에 부정적인 영향을 끼칠 수 있습니다. 영역 규칙에서 이 특정 영역 정책이 *반드시* 있어야 하는 *장치만* 찾은 *경우에만* 영역 규칙을 자동으로 적용합니다.
- **모든 기존 장치에 지금 적용**: 영역 규칙을 조직의 모든 장치에 적용합니다. 이때 영역 정책은 적용되지 않습니다.

고유 이름(DN) 정보

영역 규칙에서 고유 이름(DN)을 사용할 때 알고 있어야 할 몇 가지 사항이 있습니다.

- 와일드카드는 사용하지 못하지만 "포함" 조건으로 비슷한 결과를 얻을 수 있습니다.
- 에이전트와 관련된 DN 오류 및 예외는 로그 파일에 수집됩니다.
- 에이전트가 장치에 대한 DN 정보를 발견하면 콘솔로 자동 전송합니다.
- DN 정보를 추가할 때는 다음과 같은 형식을 따라야 합니다.
    - 예: CN=JDoe,OU=Sales,DC=dell,DC=COM
    - 예: OU=Demo,OU=SEngineering,OU=Sales

영역 장치 목록

*영역 장치 목록*은 이 영역에 할당된 모든 장치를 표시합니다. 장치는 다중 영역에 속할 수 있습니다. *영역 장치 목록*의 모든 장치에 대한 정보가 포함된 CSV 파일을 다운로드하려면 **내보내기**를 사용합니다.

참고: 영역을 볼 수 있는 권한이 없는 상태에서 영역 열의 영역 링크를 클릭할 경우 리소스를 찾을 수 없음 페이지가 표시됩니다.

영역 관리 모범 사례

영역은 모든 장치가 다중 영역에 속할 수 있다는 점에서(또는 다중 태그를 지정할 수 있다는 점에서) 태그로 간주해도 좋습니다. 생성할 수 있는 영역의 수에 제한은 없지만 모범 사례에 따라 조직 내 영역을 테스트, 정책 및 사용자 역할 등 세 가지로 세분화하여 구분하는 것이 좋습니다.

이 세 가지 영역은 다음과 같이 구성됩니다.

- 업데이트 관리
- 정책 관리
- 역할 기반 액세스 관리

업데이트 관리를 위한 영역 구성

영역의 공통적인 용도 한 가지는 에이전트 업데이트의 관리입니다. Threat Defense 는 최신 버전의 에이전트와 이전 버전을 지원합니다. 이로써 조직은 변경 동결 범위를 지원할 뿐만 아니라 새로운 버전의 에이전트도 철저하게 테스트할 수 있습니다.

에이전트 테스트 및 프로덕션 단계를 진행하면서 이를 지정하는 데 사용되는 영역 유형은 세 가지가 권장됩니다.

- **업데이트 영역 - 테스트 그룹**: 이 영역에서는 조직의 장치(및 장치에 사용되는 소프트웨어)를 올바로 나타낼 테스트 장치가 필요합니다. 이를 통해 최신 에이전트를 테스트함으로써 에이전트를 프로덕션 장치에 배포하더라도 비즈니스 프로세스가 중단될 염려가 없습니다.
- **업데이트 영역 - 파일럿 그룹**: 이 영역은 보조 테스트 영역으로, 또는 보조 프로덕션 영역으로 사용할 수 있습니다. 보조 테스트 영역으로 사용할 때는 프로덕션 단계로 진행하기에 앞서 규모가 큰 장치 그룹에서 새로운 에이전트 테스트가 가능합니다. 보조 프로덕션 영역으로 사용할 때는 다른 에이전트 버전 2 개가 가능하지만 이때는 관리해야 하는 프로덕션 영역도 2 개가 됩니다.
- **업데이트 영역 - 프로덕션**: 대부분 장치는 프로덕션에 할당된 영역에 속해야 합니다.

참고: 에이전트를 프로덕션 영역으로 업데이트 하는 방법에 대해서는 에이전트 업데이트를 참조하십시오.

테스트 또는 파일럿 영역을 추가하는 방법

1. 관리자 또는 영역 관리자 계정으로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **에이전트 업데이트**를 선택합니다.
3. 테스트 또는 파일럿 영역의 경우:
    a. **테스트 영역 선택** 또는 **파일럿 영역 선택**을 클릭합니다.
    b. 영역을 클릭합니다.

    프로덕션 영역을 **자동 업데이트**로 설정한 경우 테스트 및 파일럿 영역을 사용할 수 없습니다. 이때는 프로덕션 영역의 자동 업데이트를 다른 것으로 변경하면 테스트 및 파일럿 영역을 사용할 수 있습니다.

4. **버전 선택**을 클릭합니다.
5. 테스트 또는 파일럿 영역에 적용할 에이전트 버전을 선택합니다.
6. **적용**을 클릭합니다.

정책 관리를 위한 영역 구성

이번에 생성하는 또 다른 영역은 끝점 유형에 따라 다른 정책을 적용하는 데 유용합니다. 다음과 같은 예를 생각해볼 수 있습니다.

- 정책 영역 – 워크스테이션
- 정책 영역 – 워크스테이션 – 제외
- 정책 영역 – 서버
- 정책 영역 – 서버 – 제외
- 정책 영역 – 실행 파일 – 강력한 보호

Dell 은 이와 같은 모든 영역마다 각각 속하는 모든 장치에 기본적으로 정책을 적용하도록 권장합니다. 단, 다중 정책 영역에 장치를 1 개만 할당해서는 안 됩니다. 정책 적용 시 충돌이 일어날 수 있기 때문입니다. 또한 영역 규칙 엔진은 IP, 호스트 이름, 운영 체제 및 도메인을 기준으로 호스트를 자동 구성하는 데 효과적이라는 점도 잊지 마십시오.

역할 기반 액세스 관리를 위한 영역 구성

역할 기반 액세스는 콘솔 사용자가 관리하는 장치의 하위 집합에 대한 액세스 권한을 제한하는 데 사용됩니다. 여기에는 IP 범위, 호스트 이름, 운영 체제 또는 도메인에 따른 권한 분리도 포함될 수 있습니다. 그 밖에 지리적 위치나 유형, 또는 둘 다를 기준으로 그룹화하는 방법도 생각해볼 수 있습니다.

예:

- RBAC 영역 – 데스크톱 – 유럽
- RBAC 영역 – 서버 – 아시아
- RBAC 영역 – Red Carpet(실행 파일)

위의 영역 예를 사용하여 영역 관리자를 *RBAC 영역 – 데스크톱 – 유럽*으로 할당하고 해당 영역 안에서만 장치에 액세스할 수 있습니다. 이 영역 관리자 역할의 사용자가 나머지 영역을 보려고 하면 볼 수 있는 권한이 없다는 오류 메시지가 표시됩니다. 장치가 다중 영역에 속해 있어서 영역 관리자가 해당 장치를 볼 수 있다고 하더라도 장치가 연동되어 있는 다른 영역을 보려고 할 경우에는 오류 메시지가 표시되면서 볼 수 없습니다.

대시보드 같은 콘솔의 다른 부분에서 *RBAC 영역 – 데스크톱 – 유럽*의 영역 관리자가 볼 수 있는 권한은 해당 영역 또는 영역에 할당된 장치에 관련된 위협 및 다른 정보로 제한됩니다.

영역에 할당되어 있는 사용자 역시 동일한 제한이 적용됩니다.

사용자 관리

관리자에게는 전역적 권한이 있기 대문에 사용자를 추가 또는 제거하거나, 사용자를 영역에 (사용자 또는 영역 관리자로) 할당하거나, 장치를 추가 또는 제거하거나, 정책을 생성하거나, 영역을 생성할 수 있습니다. 그 밖에 사용자, 장치, 정책 및 영역을 콘솔에서 영구적으로 삭제하는 것도 가능합니다.

사용자와 영역 관리자는 자신이 할당되어 있는 영역에 대한 액세스 권한만 있습니다. 이러한 액세스 권한은 영역에 할당되어 있는 장치, 이 장치에서 발견되는 위협 요소, 그리고 대시보드의 정보에 적용됩니다.

각 사용자에게 허용되는 사용자 권한에 대한 전체 목록은 부록 C:사용자 권한을 참조하십시오.

사용자를 추가하는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 사용자 생성은 관리자만 가능하기 때문입니다.
2. **설정** > **사용자 관리**를 선택합니다.
3. 사용자의 이메일 주소를 입력합니다.
4. 역할 드롭다운 메뉴에서 역할을 선택합니다.
5. 영역 관리자 또는 사용자를 추가할 때는 영역을 선택하여 할당합니다.
6. **추가**를 클릭합니다. 암호를 생성할 수 있도록 링크와 함께 이메일이 해당 사용자에게 발송됩니다.

사용자 역할을 변경하는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 사용자 생성은 관리자만 가능하기 때문입니다.
2. **설정** > **사용자 관리**를 선택합니다.
3. 사용자를 클릭합니다. 사용자 세부 정보 페이지가 표시됩니다.
4. 역할을 선택하고 **저장**을 클릭합니다.

사용자를 제거하는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 사용자 생성은 관리자만 가능하기 때문입니다.
2. **설정** > **사용자 관리**를 선택합니다.
3. 제거할 사용자(들)의 확인란을 선택합니다.
4. **제거**를 클릭합니다.
5. 제거할지 확인하는 메시지에서 **예**를 클릭합니다.

네트워크 관련

Threat Defense 에이전트가 인터넷을 통해 콘솔과 통신할 수 있도록 네트워크를 구성합니다. 여기에서는 방화벽 설정과 프록시 구성에 대해서 알아보겠습니다.

방화벽

장치 관리가 필요한 온프레미스 소프트웨어는 없습니다. Threat Defense 에이전트는 콘솔(클라우드 기반 사용자 인터페이스)에게 보고하며, 관리도 콘솔을 통해 이루어집니다. 포트 443(HTTPS)가 통신하는 데 사용되기 때문에 에이전트가 콘솔과 통신하려면 방화벽에서 반드시 열려 있어야 합니다. 콘솔은 Amazon Web Service(AWS)에 의해 호스트되며 고정 IP 가 없습니다. 에이전트는 다음 사이트와 통신이 가능해야 합니다.

- login.cylance.com
- data.cylance.com
- my.cylance.com
- update.cylance.com
- api2.cylance.com
- download.cylance.com

또한 HTTPS 트래픽을 *.cylance.com 으로 전송할 수 있어야 합니다.

프록시

Threat Defense 에 대한 프록시 지원은 레지스트리 항목을 통해 구성합니다. 프록시를 구성하면 에이전트가 콘솔 서버로 향하는 모든 아웃바운드 통신에 레지스트리 항목의 IP 주소와 포트를 사용합니다.

1. 레지스트리에 액세스합니다.

   참고: 에이전트의 설치 방법(보호 모드 활성화/비활성화)에 따라 승격된 권한 또는 레지스트리 관리자 권한이 필요할 수도 있습니다.

2. 레지스트리 에디터에서 **HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop** 으로 이동합니다.
3. 다음과 같이 새로운 문자열 값(REG_SZ)을 생성합니다.
    - 값 이름 = ProxyServer
    - 값 데이터 = 프록시 설정(예: http://123.45.67.89:8080)

에이전트가 인증된 환경에서 외부 인터넷으로 통신할 때는 현재 로그인 사용자의 자격 증명을 사용하려고 합니다. 따라서 인증된 프록시 서버가 구성되어 있더라도 사용자가 장치에 로그인하지 않으면 에이전트가 프록시를 인증하지 못하여 콘솔과 통신할 수 없습니다. 이러한 경우에는 다음 중 한 가지 방법을 사용합니다.

- 프록시를 구성하고 모든 트래픽을 *.cylance.com 으로 전송할 수 있는 규칙을 추가합니다.
- 다른 프록시 정책을 사용하여 인증되지 않은 프록시에서도 Cylance 호스트(*.cylance.com)에 액세스할 수 있도록 허용합니다.

이렇게 하면 사용자가 장치에 로그인하지 않더라도 에이전트의 인증 필요성이 사라져 클라우드에 연결하여 콘솔과 통신할 수 있습니다.

장치

에이전트가 끝점에 설치되면 콘솔에서 장치로 사용할 수 있습니다. 식별된 *위협 요소*를 처리하기 위해 정책을 할당하여 장치 관리를 시작하고 *영역*을 사용하여 장치를 그룹화하고 각 장치에 수동으로 조치(*격리* 및 *면제*)를 취합니다.

장치 관리

여기에서 장치란 Threat Defense 에이전트가 설치되어 있는 컴퓨터를 말합니다. 이러한 장치는 콘솔에서 관리합니다.

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다. 장치 관리는 관리자만 가능하기 때문입니다.
2. **장치**를 클릭합니다.
3. 다음 작업을 허용할 장치의 확인란을 선택합니다.
    - **내보내기**: CSV 파일을 생성하여 다운로드합니다. 이 파일에는 조직에 속한 모든 장치의 정보(이름, 상태 및 정책)가 저장됩니다.

- **제거**: *장치 목록*에서 선택한 장치를 제거합니다. 그렇다고 에이전트까지 장치에서 삭제되지는 않습니다.
- **정책 할당**: 선택한 장치를 정책에 할당할 수 있습니다.
- **영역에 추가**: 선택한 장치를 영역(들)에 추가할 수 있습니다.

4. 장치 세부 정보 페이지에 표시할 장치를 클릭합니다.
    - **장치 정보**: 호스트 이름, 에이전트 버전, 운영 체제 버전 등의 정보가 표시됩니다.
    - **장치 속성**: 장치 이름, 정책, 영역 및 로깅 레벨 등을 변경할 수 있습니다.
    - **위협 요소 및 활동**: 장치와 관련된 위협 정보와 기타 활동이 표시됩니다.
5. 에이전트 설치 프로그램을 다운로드할 수 있는 설치 토큰 및 링크를 포함한 대화 상자를 표시하려면 **새 장치 추가**를 클릭합니다.
6. 영역 열에서 영역 세부 정보 페이지에 표시할 영역 이름을 클릭합니다.

위협 요소 및 활동

선택한 장치와 관련된 위협 정보와 기타 활동이 표시됩니다.

위협

장치에서 발견되는 위협 요소를 모두 표시합니다. 기본적으로 위협 요소는 상태(*안전하지 않음*, *비정상*, *격리됨* 및 *면제됨*)를 기준으로 그룹화됩니다.

- **내보내기**: 선택한 장치에서 발견되는 모든 위협 요소에 대한 정보가 저장된 CSV 파일을 생성하여 다운로드합니다. 여기에는 이름, 파일 경로, Cylance 점수 및 상태 같은 위협 정보가 포함됩니다.
- **격리**: 선택한 위협 요소를 *격리*합니다. 이를 *로컬 격리*라고 하며 이 위협 요소는 이 장치에서만 *격리*됩니다. 조직의 모든 장치에서 위협 요소를 *격리*하려면 파일을 *격리*할 때 *전역 격리*에서 **다른 모든 장치에서 발견될 때마다 이 위협 요소 차단** 확인란을 선택합니다.
- **면제**: 선택한 위협 요소의 상태를 *면제됨*으로 변경합니다. *면제됨* 파일은 실행이 허용됩니다. 이를 *로컬 면제*라고 하며 이 파일은 이 장치에서만 허용됩니다. 조직의 모든 장치에서 이 파일을 허용하려면 파일을 *면제*할 때 *안전 목록*에서 **다른 모든 장치에서도 안전함으로 표시** 확인란을 선택합니다.

익스플로잇 시도

장치에 대한 익스플로잇 시도를 모두 표시합니다. 여기에는 프로세스 이름, ID, 유형 및 작업에 대한 정보가 포함됩니다.

에이전트 로그

에이전트가 장치와 관련하여 업로드한 로그 파일이 표시됩니다. 로그 파일 이름은 로그 날짜에 따라 결정됩니다.

에이전트 로그 파일을 보는 방법

1. 단일 장치의 현재 로그 파일을 업로드합니다.
   a. 장치 > 에이전트 로그를 클릭합니다.
   b. **현재 로그 파일 업로드**를 클릭합니다. 로그 파일 크기에 따라 몇 분 정도 소요될 수 있습니다.

또는

1. 정책 설정:
   a. 설정 > 장치 정책 > [정책 선택] > 에이전트 로그를 클릭합니다.
   b. 로그 파일 자동 업로드 활성화를 클릭합니다.
   c. **저장**을 클릭합니다.

자세한 정보 표시 로그를 보려면 로그 파일을 업로드하기 전에 에이전트 로깅 레벨을 변경합니다.

1. 콘솔에서 다음과 같이 실행합니다. **장치 > [장치 클릭]**, 에이전트 로깅 레벨 드롭다운 메뉴에서 **자세한 정보 표시**를 선택하고 **저장**을 클릭합니다. 자세한 정보 표시 로그 파일을 업로드한 후에는 에이전트 로깅 레벨을 다시 *정보*로 설정하는 것이 좋습니다.
2. 장치에서 Threat Defense 사용자 인터페이스를 닫습니다. 시스템 트레이에서 Threat Defense 아이콘을 오른쪽 클릭한 후 **종료**를 클릭합니다.

또는

1. 관리자 권한으로 명령줄을 엽니다. 다음 명령줄을 입력하고 **Enter** 키를 누릅니다.

   ```
   cd C:\Program Files\Cylance\Desktop
   ```

2. 다음 명령줄을 입력하고 **Enter** 키를 누릅니다.

   ```
   Dell.ThreatDefense.exe –a
   ```

3. Threat Defense 아이콘이 시스템 트레이에 표시됩니다. 마우스 오른쪽 단추를 클릭하고 **로깅**을 선택한 다음 콘솔의 자세한 정보 표시와 마찬가지로 **모두**를 클릭합니다.

또는 (macOS 용)

1. 현재 실행 중인 사용자 인터페이스에서 나옵니다.
2. 단말기에서 다음 명령을 실행합니다.

   ```
   sudo /Applications/Cylance/CylanceUI.app/Contents/MacOS/CylanceUI -a
   ```

3. 새로운 사용자 인터페이스가 열리면 오른쪽 클릭합니다. **로깅** > **모두**를 선택합니다.

스크립트 제어

거부된 스크립트를 포함하여 스크립트 제어와 관련된 모든 활동이 표시됩니다.

중복 장치

처음에 Threat Defense 에이전트를 장치에 설치할 때는 콘솔에서 해당 장치를 식별하고 참조할 수 있도록 고유 식별자가 생성됩니다. 하지만 가상 시스템 이미지를 사용해 다수의 시스템을 생성할 때처럼 일부 이벤트의 경우 동일한 장치에서 두 번째 식별자를 생성하게 될 수도 있습니다. 중복 항목이 콘솔의 장치 페이지에 표시되는 경우 장치를 선택하고 **제거**를 클릭합니다.

중복 장치를 식별하려면 장치 페이지에서 열 정렬 기능을 사용하십시오. 그러면 장치 이름을 기준으로 장치를 정렬 및 비교할 수 있습니다. 또는 *장치 목록*을 .CSV 파일로 내보내어 Microsoft Excel 이나 강력한 정렬/구성 기능이 있는 유사한 응용 프로그램에서 데이터를 볼 수 있습니다.

Microsoft Excel 의 사용 예

1. 장치 CSV 파일을 Microsoft Excel 에서 엽니다.
2. 장치 이름 열을 선택합니다.
3. 홈 탭에서 조건부 서식 > 셀 강조 규칙 > 중복 값을 선택합니다.
4. **중복**을 선택한 다음 강조 표시된 옵션을 선택합니다.
5. **확인**을 클릭합니다. 중복 항목이 강조됩니다.

참고: 제거 명령은 장치 페이지에서 장치만 제거합니다. 제거 명령으로 Threat Defense 에이전트에 대한 삭제 명령이 실행되지는 않습니다. 에이전트 삭제는 끝점에서만 가능합니다.

에이전트 업데이트

Threat Defense 에이전트의 유지보수 및 관리는 매우 간편합니다. 에이전트가 업데이트를 자동으로 콘솔에서 다운로드할 뿐만 아니라 콘솔은 Cylance 에서 관리하기 때문입니다.

에이전트는 1~2 분마다 콘솔에 체크인합니다. 콘솔은 에이전트의 현재 상태(*온라인* 또는 *오프라인*, *안전하지 않음* 또는 *보호됨*), 버전 정보, 운영 체제 및 위협 요소 상태를 보고합니다.

Threat Defense 는 1 개월을 기준으로 에이전트에게 업데이트를 배포합니다. 이 업데이트에는 구성 설정, 새 모듈 및 프로그램 변경이 포함될 수 있습니다. 에이전트 업데이트가 있을 경우에는(콘솔의 설정 > 에이전트 업데이트에서 알 수 있음) 에이전트가 업데이트를 자동으로 다운로드하여 적용합니다. 에이전트 업데이트 중에는 네트워크 트래픽 제어를 위해 모든 조직이 최대 1,000 개의 장치를 동시에 업데이트할 수 있도록 설정됩니다. 사용자는 필요에 따라 자동 업데이트 기능을 비활성화할 수 있습니다.

참고: 동시 업데이트가 가능한 최대 장치 수는 Dell Support 에서 변경할 수 있습니다.

영역 기반 업데이트

영역 기반 업데이트는 조직이 전체 환경(프로덕션)에 배포하기 전에 장치의 하위 집합에서 새로운 에이전트를 평가할 수 있는 기능입니다. 1 개 이상의 현재 영역을 테스트 영역 2 개(테스트 및 파일럿) 중 1 개에 일시적으로 추가하여 프로덕션이 아닌 다른 에이전트를 사용해볼 수 있습니다.

영역 기반 업데이트를 구성하는 방법:

1. 관리자 계정으로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **에이전트 업데이트**를 선택합니다. 최신 에이전트 버전 3 개가 표시됩니다.

   프로덕션 영역을 **자동 업데이트**로 설정한 경우 테스트 및 파일럿 영역을 사용할 수 없습니다. 이때는 프로덕션 영역의 자동 업데이트를 다른 것으로 변경하면 테스트 및 파일럿 영역을 사용할 수 있습니다.
3. 프로덕션 드롭다운 목록에서 특정 에이전트 버전을 선택합니다.
4. 프로덕션 영역의 경우에는 자동 업데이트 또는 업데이트하지 않음을 선택합니다.
   a. **자동 업데이트**는 모든 프로덕션 장치를 *지원되는 에이전트 버전 목록*의 최신 버전으로 자동으로 업데이트합니다.
   b. **업데이트하지 않음**은 모든 프로덕션 장치에서 에이전트를 업데이트하지 않습니다.
5. 테스트 영역의 경우에는 영역 드롭다운 목록에서 영역을 1 개 이상 선택한 다음 버전 드롭다운 목록에서 특정 에이전트 버전을 선택합니다.
6. 필요하다면 파일럿 영역에서도 단계 5 를 반복합니다.

참고: 장치를 테스트 또는 파일럿 영역에 포함된 영역에 추가할 경우에는 해당 장치가 처음에 테스트 또는 파일럿 영역의 에이전트 버전을 사용합니다. 장치가 다수의 영역에 속하고, 이러한 영역 중 하나가 테스트 또는 파일럿 영역에 속하는 경우에는 테스트 또는 파일럿 영역 에이전트 버전이 우선합니다.

에이전트 업데이트를 트리거하는 방법

다음 시간 주기 이전에 에이전트 업데이트를 트리거하는 방법

1. 시스템 트레이에서 Threat Defense 에이전트 아이콘을 오른쪽 클릭한 다음 **업데이트 확인**을 선택합니다.
2. Threat Defense 서비스를 다시 시작합니다. 그러면 콘솔에 바로 강제 체크인됩니다.

또는

- 업데이트는 명령줄에서도 시작할 수 있습니다. Cylance 디렉터리에서 다음 명령을 실행합니다.

  `Dell.ThreatDefense.exe – update`

대시보드

Threat Defense 콘솔에 로그인하면 대시보드 페이지가 표시됩니다. 대시보드는 환경의 위협 요소에 대해 간략히 설명하면서 다른 콘솔 정보 페이지로 이동하는 수단을 제공하기도 합니다.

위협 통계

위협 통계는 조직의 *전체* 및 *지난 24 시간* 내 발생한 위협 요소의 개수를 제공합니다. 보호 페이지로 이동하고 통계에 관련된 위협 목록을 표시하려면 *위협 통계*를 클릭합니다.

- **실행 중인 위협**: 현재 조직 장치에서 실행 중이지만 위협 요소로 식별된 파일의 수입니다.
- **자동 실행 위협**: 자동으로 실행하도록 설정된 위협 요소의 수입니다.
- **격리된 위협**: 지난 24 시간 내 및 전체 *격리된* 위협 요소의 수입니다.
- **Cylance 고유 위협**: 다른 안티바이러스 소스가 아닌 Cylance 에서 식별된 위협 요소의 수입니다.

보호율

위협 차단 및 장치 보호를 나타내는 비율이 표시됩니다.

- **위협 차단**: 이미 조치(격리, 전역적 격리, 면제, 안전 목록)를 취한 위협 요소의 비율
- **장치 보호**: 자동 격리를 활성화한 정책과 연동되어 있는 장치의 비율

우선순위 기준 위협

조치(*격리*, *전역 격리*, *면제*, *안전 목록*)가 필요한 위협 요소의 전체 개수를 표시합니다. 위협 요소는 우선순위(높음, 보통, 낮음)를 기준으로 구분됩니다. 여기에서는 조치가 필요한 위협 요소의 총 수 외에도 우선순위 기준 총 수, 총 비율, 그리고 감염된 장치의 수가 따로 표시됩니다.

위협 요소는 대시보드 페이지 왼쪽 하단 모퉁이에 우선순위를 기준으로 나열됩니다. 여기에는 조직에 존재하는 위협 요소의 총 수가 우선순위 분류를 기준으로 명시됩니다.

위협 요소는 다음 속성의 수에 따라 낮음, 보통 및 높음으로 분류됩니다.

- 파일의 Cylance 점수가 80 을 넘습니다.
- 파일이 현재 실행 중입니다.
- 파일을 이전에 실행한 적이 있습니다.
- 파일이 자동 실행으로 설정되어 있습니다.
- 위협 요소가 발견된 영역의 우선 순위입니다.

이 분류는 관리자가 어떤 위협과 장치를 먼저 해결할지 결정하는 데 도움이 됩니다. 위협 요소 또는 장치 수를 클릭하면 위협 요소 및 장치 세부 정보를 볼 수 있습니다.

위협 이벤트

지난 30 일간 발견된 위협 요소의 수가 선 그래프로 표시됩니다. 선은 *안전하지 않음*, *비정상*, *격리됨*, *면제됨* 및 *삭제됨* 파일에 대해 색상으로 구분됩니다.

- 그래프의 점 위로 마우스 포인터를 가져가면 세부 정보가 나타납니다.
- 범례에서 색상 하나를 클릭하면 해당 선이 표시되거나 숨겨집니다.

Threat Classifications(위협 분류)

바이러스나 맬웨어처럼 조직에서 발견된 위협 요소의 유형을 히트 맵으로 표시합니다. 히트 맵의 항목을 클릭하면 보호 페이지로 이동하면서 해당 유형의 위협 요소 목록이 표시됩니다.

상위 5 개 목록

대부분 장치에서 가장 많이 발견된 상위 5 개 위협 요소, 대부분 위협 요소가 가장 많이 존재하는 상위 5 개 장치, 그리고 조직에서 대부분 위협 요소가 가장 많이 존재하는 상위 5 개 영역이 나열됩니다. 목록 항목을 클릭하면 세부 정보를 볼 수 있습니다.

대시보드의 상위 5 개 목록은 조직에서 *격리됨* 또는 *면제됨*과 같은 조치를 취하지 않은 *안전하지 않음* 위협 요소를 강조 표시합니다. 이러한 목록은 대부분 비어 있어야 합니다. *비정상* 위협에 조치도 취해야 하지만 상위 5 개 목록의 주요 목적은 위험한 위협 요소에 사용자의 주의를 끌기 위한 것입니다.

보호 - 위협

Threat Defense 는 파일을 단순히 *안전하지 않음*이나 *비정상*으로 분류하는 것 외에 더 많은 기능을 수행할 수 있습니다. 파일의 정적 및 동적 특징에 대한 세부 정보를 제공할 수 있습니다. 여기서 관리자는 위협을 차단할 뿐 아니라 더 나아가 위협을 완화하거나 이에 대응하기 위해 위협 특성을 이해할 수 있습니다.

파일 형식

안전하지 않음: 점수가 60~100 범위에 있는 파일입니다. *안전하지 않음* 파일은 Threat Defense 엔진에서 맬웨어와 매우 유사한 속성을 발견한 파일입니다.

비정상: 점수가 1~59 범위에 있는 파일입니다. 비정상 파일에는 몇 가지 맬웨어 속성이 있기는 하지만 *안전하지 않음* 파일보다는 적기 때문에 맬웨어일 가능성이 떨어집니다.

참고: 표시된 점수가 분류 범위와 일치하지 않더라도 파일이 *안전하지 않음*이나 *비정상*으로 분류되는 경우가 종종 있습니다. 초기 검색 이후에 결과가 업데이트되었거나 추가 파일 분석이 이루어졌기 때문일 수 있습니다. 최신 분석을 위해서는 장치 정책에서 자동 업로드를 활성화하십시오.

Cylance 점수

*비정상*이나 *안전하지 않음*으로 간주되는 각 파일에 Cylance 점수가 할당됩니다. 점수는 파일이 맬웨어라는 신뢰 수준을 나타냅니다. 숫자가 높을수록 신뢰 수준이 높습니다.

위협 정보 보기

콘솔의 보호 탭에서는 자세한 위협 정보와 함께 위협 요소가 발견된 장치, 그리고 해당 위협 요소에 대해 장치에 취한 조치가 표시됩니다.

참고: 보호 탭의 *위협 목록*에는 구성 가능한 열이 있습니다. 어떤 열에서든지 아래 화살표를 클릭하면 메뉴에 액세스하여 다양한 위협 정보를 표시하거나 숨길 수 있습니다. 메뉴에는 필터링 하위 메뉴가 포함되어 있습니다.

위협 세부 정보를 보는 방법

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. 해당 조직에서 발견한 위협 목록을 표시하려면 **보호** 탭을 클릭합니다.
3. 왼쪽 메뉴 바의 필터를 사용해 우선 순위(높음, 보통 또는 낮음) 및 상태(*안전하지 않음*, *격리됨*, *면제됨*, *비정상*)를 기준으로 필터링합니다.

   참고: 왼쪽 창에서 빨간색으로 표시되는 숫자는 *격리* 또는 *면제*되지 않은 미해결 위협을 나타냅니다. 이러한 항목을 필터링하면 검사가 필요한 파일 목록이 표시됩니다.

4. 위협 정보를 더 볼 수 있도록 열을 추가하려면 먼저 열 이름 옆에 있는 아래 화살표를 클릭한 다음 열 이름을 선택합니다.
5. 특정 위협에 대한 추가 정보를 보려면 위협 이름 링크를 클릭하거나(새로운 페이지로 세부 정보가 표시됨), 혹은 위협 행에서 아무 곳이나 클릭합니다(페이지 하단에 세부 정보가 표시됨). 두 보기 모두 같은 내용을 표시하지만 표시 스타일이 다릅니다. 세부 정보에는 파일 메타데이터의 개요, 위협이 발생한 장치 목록 및 증거 보고서가 포함됩니다.
    a. 파일 메타데이터
        - 분류[Cylance Advanced Threat and Alert Management (ATAM) 팀에서 할당]
        - Cylance 점수(신뢰도)
        - AV Industry 평가(기타 공급업체와 비교를 위한 VirusTotal.com 링크)
        - 처음 발견된 날짜, 마지막으로 발견된 날짜
        - SHA256
        - MD5
        - 파일 정보(작성자, 설명, 버전 등)
        - 서명 세부 정보
    b. 장치

        위협에 대한 *장치/영역 목록*은 위협의 상태(*안전하지 않음*, *격리됨*, *면제됨*, *비정상*)를 기준으로 필터링할 수 있습니다. 해당 상태의 위협이 존재하는 장치를 표시하려면 상태 필터 링크를 클릭하십시오.

        - *안전하지 않음*: 파일이 *안전하지 않음*으로 분류되었지만 아무 조치를 취하지 않았습니다.
        - *격리됨*: 정책 설정이 적용되어 이미 *격리*되었습니다.
        - *면제됨*: 관리자가 파일을 *면제* 또는 *화이트 리스트*로 분류했습니다.
        - *비정상*: 파일이 *비정상*으로 분류되었지만 아무 조치를 취하지 않았습니다.

c. 증거 보고서

- **위협 표시기**: Cylance Infinity 엔진이 분석한 파일에 대한 기록입니다. 이 표시기는 파일의 분류에 대한 이유를 이해하고 파일의 특성과 동작에 대한 통찰력을 제공할 수 있도록 도와줍니다. 위협 표시기는 컨텍스트에 도움을 주기 위해 범주로 그룹화됩니다.
- **상세 위협 데이터**: 상세 위협 데이터에서는 추가 파일 메타데이터, 파일 구조 세부 정보 및 동적 동작(삭제된 파일, 생성되거나 수정된 레지스트리 키 및 통신을 시도한 URL)을 포함해 파일의 정적 및 동적 특징에 대한 포괄적인 요약을 제공합니다.

위협 표시기를 보는 방법

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. 위협 목록을 보려면 상단 메뉴에서 **보호**를 클릭하거나 **장치**를 클릭한 다음 장치를 선택합니다.
3. 임의의 위협 이름을 클릭합니다. 위협 세부 정보 페이지가 표시됩니다.
4. **증거 보고서**를 클릭합니다.

위협 표시기 카테고리:

각 카테고리는 1 억 개가 넘는 바이너리에 대한 심층 분석을 바탕으로 악성 소프트웨어에서 자주 발견되는 항목을 의미합니다. 위협 표시기 보고서는 파일에 존재하는 이러한 카테고리의 수를 나타냅니다.

변칙

파일에는 어떠한 방식으로든 일치하지 않거나 변칙적인 요소들이 있습니다. 이러한 요소들은 파일 구조의 불일치를 야기하는 경우가 빈번합니다.

수집

파일에는 데이터 수집의 증거가 있습니다. 여기에는 장치 구성 열거 또는 민감한 정보 수집이 포함됩니다.

데이터 손실

파일에는 데이터 유출의 증거가 있습니다. 여기에는 발신 네트워크 연결, 브라우저 사용 증거, 또는 기타 네트워크 통신이 포함됩니다.

기만

파일에는 기만을 시도한 증거가 있습니다. 여기에서 기만이란 숨은 구간, 탐지를 피하기 위한 코드 삽입, 그리고 메타데이타 또는 기타 구간의 부적절한 레이블 지정 등의 형태로 나타날 수 있습니다.

파괴

파일에는 파괴적 기능의 증거가 있습니다. 여기에는 파일이나 디렉터리 같은 장치 리소스를 삭제하려는 시도가 포함됩니다.

기타

나머지 카테고리에 해당하지 않는 기타 모든 표시기가 여기에 포함됩니다.

참고: 위협 표시기와 상세 위협 데이터 섹션은 결과를 표시하지 않거나 사용할 수 없는 경우도 있습니다. 이는 파일이 업로드되지 않은 경우에 발생합니다. 파일이 업로드되지 않은 이유는 디버그 로깅을 통해 알 수도 있습니다.

위협 해결

일부 위협은 취할 수 있는 조치 유형이 장치에 할당된 사용자에 따라서 달라지기도 합니다. 위협에 대한 조치는 장치 또는 전역 수준에서 적용할 수 있습니다. 아래는 탐지된 위협 요소 또는 파일에 대해 취할 수 있는 몇 가지 조치들입니다.

- ***격리***: 특정 파일을 *격리*하면 해당 장치에서 파일을 실행할 수 없습니다.

  참고: 장치에서 명령줄을 사용하여 위협을 격리할 수 있습니다. 이 기능은 Windows Agent 에서만 사용할 수 있습니다. 자세한 내용은 명령줄을 사용하여 격리를 참조하십시오.

- ***전역 격리***: 파일을 *전역 격리*하면 전체 조직의 모든 장치에서 파일을 실행할 수 없습니다.

  참고: 파일을 *격리*하면 파일이 원래 위치에서 *격리* 디렉터리(**`C:\ProgramData\Cylance\Desktop\q`**)로 이동합니다.

- ***면제***: 파일을 *면제*하면 해당 파일을 지정된 장치에서 실행할 수 있습니다.

- ***전역 안전***: 파일을 *전역 안전 목록*에 나열하면 전체 조직의 모든 장치에서 파일을 실행할 수 있습니다.

  참고: 경우에 따라 Threat Defense 에서는 "양호한" 파일을 *격리*하거나 보고할 수 있습니다. 해당 파일의 기능이 유해한 파일과 매우 비슷할 경우에 이러한 문제가 발생할 수 있습니다. 파일을 *면제*하거나 *전역적으로 안전 목록에 나열*하면 이러한 경우에 도움이 될 수 있습니다.

- ***파일 업로드***: 분석을 위해 파일을 Cylance Infinity 에 수동으로 업로드합니다. 자동 업로드 기능이 활성화되어 있는 경우 새로운 파일(Cylance 의 분석이 끝나지 않은 파일)은 Cylance Infinity 에 자동 업로드됩니다. Cylance Infinity 에 파일이 존재할 때는 Upload File(파일 업로드) 버튼이 회색으로 바뀌며 사용할 수 없습니다.

- ***파일 다운로드***: 자신이 직접 테스트할 목적으로 파일을 다운로드합니다. 조직에서는 이 기능을 활성화해야 합니다. 그리고, 사용자는 관리자이어야 합니다. 또한 위협은 에이전트 버전 1320 이상을 사용해 탐지해야 합니다.

  참고: Cylance Infinity 에서 사용할 수 있는 파일이어야 하며, 세 가지 해시(SHA256, SHA1 및 MD5)가 Cylance Infinity 와 에이전트 사이에서 모두 일치해야 합니다. 그렇지 않으면 Download File(파일 다운로드) 버튼을 사용할 수 없습니다.

특정 장치의 위협 해결

1. 관리자 또는 영역 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **장치** 탭을 클릭합니다.
3. 장치를 검색하여 선택합니다.
4. 그 밖에 관련 위협 요소가 함께 나열되어 있는 경우에는 보호 탭에서 장치 링크를 사용하는 방법도 있습니다.
5. 해당 장치의 모든 위협 요소가 페이지 하단에 표시됩니다. 해당 장치에서 파일을 *격리* 또는 *면제*할 위협을 선택합니다.

전역적 위협 해결

전역 격리 목록 또는 *전역 안전 목록*에 추가된 파일은 모든 영역의 모든 장치에서 *격리*되거나 *허용*됩니다.

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **전역 목록**을 클릭합니다.
3. 전역적 격리 또는 안전을 클릭합니다.
4. **파일 추가**를 클릭합니다.
5. 파일의 SHA256(필수), MD5, 이름 및 *전역 목록*에 배치한 이유를 추가합니다.
6. **제출**을 클릭합니다.

보호 - 스크립트 제어

Threat Defense 는 차단 또는 경고 조치된 Active 및 PowerShell 스크립트에 대해 세부 정보를 제공합니다. 스크립트 제어 기능을 활성화하면 그 결과가 보호 페이지의 스크립트 제어 탭에 표시됩니다. 여기에는 스크립트와 감염된 장치에 대한 세부 정보가 있습니다.

스크립트 제어 결과를 보는 방법

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. 보호를 클릭합니다.
3. Script Control(스크립트 제어)을 클릭합니다.
4. 테이블에서 스크립트를 선택합니다. 세부 정보 테이블이 감염된 장치의 목록으로 업데이트됩니다.

스크립트 제어 열 설명

- **파일 이름**: 스크립트의 이름입니다.
- **해석기**: 스크립트를 식별한 스크립트 제어 기능입니다.
- **최근 발견**: 스크립트를 마지막으로 실행한 날짜와 시간입니다.
- **드라이브 종류**: 스크립트가 발견된 드라이브의 종류입니다(예: 내장 하드 드라이브).
- **SHA256**: 스크립트의 SHA 256 해시입니다.
- **장치의 수**: 스크립트에 감염된 장치의 수입니다.
- **경고**: 지금까지 스크립트를 경고한 횟수입니다. 동일 장치에 대한 경고 횟수가 다수일 수도 있습니다.
- **차단**: 스크립트가 차단된 횟수입니다. 동일 장치에 대한 경고 횟수가 다수일 수도 있습니다.

세부 정보 열 설명

- **장치 이름**: 스크립트에 감염된 장치의 이름입니다. 장치 이름을 클릭하면 장치 세부 정보 페이지로 이동합니다.
- **상태**: 장치 상태(온라인 또는 오프라인)입니다.
- **에이전트 버전**: 현재 장치에 설치된 에이전트의 버전입니다.
- **파일 경로**: 스크립트가 실행된 파일 경로입니다.
- **시기**: 스크립트가 실행된 날짜와 시간입니다.
- **사용자 이름**: 스크립트가 실행되었을 때 로그인한 사용자의 이름입니다.
- **작업**: 스크립트에 대한 조치(경고 또는 차단)입니다.

전역적 목록

*전역 목록*을 사용하여 조직의 모든 장치에서 파일을 *격리*하거나 *허용* 하도록 표시할 수 있습니다.

- **전역적 격리:** 조직의 모든 에이전트가 해당 장치에서 발견된 *전역 격리 목록*의 모든 파일을 *격리*합니다.
- **안전:** 조직의 모든 에이전트가 해당 장치에서 발견된 *안전 목록*의 모든 파일을 *허용*합니다.
- **할당되지 않음:** 조직에서 식별되었지만 *전역 격리* 또는 *안전 목록*에 할당되지 않은 위협 요소입니다.

위협 상태 변경

위협 상태(*전역 격리*, *안전* 또는 *할당되지 않음*)를 변경하려면:

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **전역 목록**을 선택합니다.
3. 위협 요소가 할당된 현재 목록을 선택합니다. 예를 들어 할당되지 않음을 클릭하면 할당되지 않은 위협 요소를 *안전* 또는 *전역 격리*로 변경합니다.
4. 변경할 위협 요소의 확인란을 선택한 후 상태 버튼을 클릭합니다.
    a. 안전: 파일을 *안전 목록*으로 이동합니다.
    b. 전역적 격리: 파일을 *전역 격리 목록*으로 이동합니다.
    c. 목록에서 제거: 파일을 *할당되지 않은 목록*으로 이동합니다.

파일 추가

전역 격리 또는 *안전 목록*으로 파일을 수동으로 추가합니다. 파일을 추가하려면 SHA256 해시 정보가 필요합니다.

1. 관리자로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **전역 목록**을 선택합니다.
3. 파일을 추가할 목록(*전역 격리* 또는 *안전*)을 선택합니다.
4. **파일 추가**를 클릭합니다.
5. SHA256 해시 정보를 입력합니다. 옵션으로서 MD5 와 파일 이름 정보를 입력합니다.
6. 이 파일을 추가하는 이유를 입력합니다.
7. **제출**을 클릭합니다.

인증서 기준 안전 목록

고객은 서명한 인증서를 기준으로 *안전 목록*에 대한 기능을 이용합니다. 이 기능으로 중단되지 않고 실행하도록 올바르게 서명된 사용자 지정 소프트웨어를 허용합니다.

참고: 이 기능은 현재 Windows 운영 체제에서만 지원됩니다.

- 이 기능을 통해 고객은 SHA1 지문으로 표시되는 서명한 인증서로 *화이트 리스트*/*안전 목록*을 설정할 수 있습니다.
- 인증서 정보는 콘솔에서 추출됩니다(타임스탬프, 제목, 발급 기관 및 지문). 인증서는 콘솔에 업로드되거나 저장되지 않습니다.
- 인증서를 생성하면 인증서 타임스탬프가 나타납니다.
- 콘솔은 인증서의 유효성 또는 만료 여부를 확인하지 않습니다.
- 인증서가 변경되면(갱신 또는 신규) 콘솔의 *안전 목록*에 추가해야 합니다.

1. 인증서 세부 정보를 인증서 저장소에 추가합니다.
    a. 서명된 PE(Portable Executable)에 사용할 인증서 지문을 확인합니다.
    b. **설정** > **인증서**를 선택합니다.
    c. **인증서 추가**를 클릭합니다.
    d. **추가할 인증서 찾아보기**를 클릭하거나 메시지 상자에 인증서를 끌어서 놓습니다.
    e. 인증서를 찾는 경우에는 인증서를 선택할 수 있도록 열기 창이 표시됩니다.
    f. 옵션으로 이 인증서에 대한 메모를 추가합니다.
    g. **제출**을 클릭합니다. 발급 기관, 제목, 지문 및 메모(입력한 경우)가 저장소에 추가됩니다.
2. *안전 목록에* 인증서를 추가합니다.
    a. **설정** > **전역 목록**을 선택합니다.
    b. **안전** 탭을 선택합니다.
    c. **인증서**를 클릭합니다.
    d. **인증서 추가**를 클릭합니다.
    e. *안전 목록*에서 인증서를 선택합니다. 옵션으로 카테고리를 선택한 후 이 인증서를 추가하는 이유를 입력합니다.
    f. **제출**을 클릭합니다.

위협 요소에 사용할 지문 보기

이제 보호 탭의 위협 세부 정보에 인증서 지문이 표시됩니다. 화면에서 **인증서에 추가**를 선택하여 리포지토리에 인증서를 추가합니다.

권한

인증서에 추가는 관리자만 사용할 수 있는 기능입니다. 인증서가 이미 인증서 리포지토리에 추가된 경우 콘솔에 **인증서로 이동**이 표시됩니다. 인증서는 영역 관리자에게 보기 전용이므로 영역 관리자에게도 **인증서로 이동** 옵션이 표시됩니다.

프로파일

프로파일 메뉴(상단 오른쪽 모퉁이)에서는 계정 관리, 콘솔 감사 로그 보기, 그리고 제품 도움말 액세스가 가능합니다.

내 계정

내 계정 페이지에서는 암호화 이메일 알림 설정을 변경합니다.

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. 상단 오른쪽 모퉁이에서 프로파일 메뉴를 클릭하고 **내 계정**을 선택합니다.
3. 암호를 변경하는 방법:
    a. 암호 변경을 클릭합니다.
    b. 이전 암호를 입력합니다.
    c. 새로운 암호를 입력하고 다시 한 번 입력하여 확인합니다.
    d. 업데이트를 클릭합니다.
4. 확인란을 선택 또는 선택 해제하여 이메일 알림을 활성화하거나 비활성화합니다. 확인란을 선택하거나 선택 해제하면 자동으로 저장됩니다. 이메일 알림 기능은 관리자만 사용할 수 있습니다.

감사 로깅

사용자 아이콘 드롭다운 목록(콘솔의 상단 오른쪽 모퉁이)

감사 로그에는 콘솔에서 실행하는 다음 작업에 대한 정보가 포함됩니다.

- 로그인(성공, 실패)
- 정책(추가, 편집, 제거)

- 장치(편집 제거)
- 위협(격리, 면제, 전역적 격리, 안전 목록)
- 사용자(추가, 편집, 제거)
- 에이전트 업데이트(편집)

감사 로그는 콘솔 상단 오른쪽에 있는 프로파일 드롭다운 목록으로 이동하고 **감사 로그**를 선택하여 콘솔에서 볼 수 있습니다. 감사 로그는 관리자만 볼 수 있습니다.

설정

설정 페이지에는 응용 프로그램, 사용자 관리, 장치 정책, 전역적 목록, 그리고 에이전트 업데이트 탭이 표시됩니다. 설정 메뉴 항목은 관리자만 사용할 수 있습니다.

응용 프로그램

Threat Defense 에이전트

Threat Defense 에이전트를 각 끝점에 설치하면 장치가 조직에 추가됩니다. 일단 콘솔에 연결된 이후에는 식별된 위협 요소 관리를 위해 정책을 적용한 후 조직 요건에 따라 장치를 구성합니다.

Threat Defense 에이전트는 시스템 리소스의 사용량을 최소화하도록 설계되었습니다. 에이전트는 악성일 수도 있는 파일이나 프로세스를 실행 우선순위에 따라 처리합니다. 디스크에 저장되어 있으나 실행되지 않는 파일 역시 악성일 수도 있지만 즉각적인 위협이 되지 않기 때문에 우선순위가 낮습니다.

Windows 에이전트

시스템 요구사항

Dell 은 끝점 하드웨어(CPU, GPU 등)가 해당 운영 체제의 권장 요구사항을 만족하거나 초과하도록 권장합니다. 예외는 아래와 같습니다(RAM, 사용 가능한 하드 드라이브 공간 및 추가 소프트웨어 요구사항)

운영 체제	• Windows 7*(32 비트 및 64 비트)* • Windows Embedded Standard 7*(32 비트)* 및 Windows Embedded Standard 7 Pro*(64 비트)* • Windows 8 및 8.1*(32 비트 및 64 비트)** • Windows 10(*32 비트 및 64 비트*)** • Windows Server 2008 및 2008 R2*(32 비트 및 64 비트)**** • Windows Server 2012 및 2012 R2*(64 비트)**** • Windows Server 2016 – Standard, Data Center 및 Essentials*****

RAM	• 2GB
사용 가능한 하드 드라이브 공간	• 300MB
추가 소프트웨어/요구사항	• .NET Framework 3.5(SP1) 이상(*Windows 전용*) • 인터넷 브라우저 • 로그인, 설치 프로그램 액세스 및 제품 등록을 위한 인터넷 연결 • 소프트웨어를 설치하기 위한 로컬 관리자 권한
기타 요구 사항	• TLS 1.2 는 Agent 1422 이상에 지원되며 .NET Framework 4.5 이상이 필요

표 2: Windows 시스템 요구사항

*지원되지 않음: Windows 8.1 RT

** Windows 10 1 주년 업데이트에는 에이전트 1402 이상이 필요합니다.

***지원되지 않음: Server Core(2008 및 2012) 및 최소 서버(2012)

****Agent 1412 이상이 필요합니다.

설치 파일을 다운로드하는 방법

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **응용 프로그램**을 선택합니다.
3. **설치 토큰**을 복사합니다.

   설치 토큰은 임의 생성 문자열로서 이를 통해 에이전트가 콘솔에서 할당된 계정에 보고할 수 있습니다. 설치 토큰은 설치 도중 설치 마법사에서, 또는 설치 매개변수 설정 시 필요합니다.
4. 설치 프로그램을 다운로드합니다.
   a. 운영 체제를 선택합니다.
   b. 다운로드할 파일 형식을 선택합니다.

      Windows 의 경우에는 에이전트를 설치할 수 있도록 MSI 파일 사용을 권장합니다.

팁: 영역 규칙을 설정하는 경우에는 장치가 영역 규칙 기준을 만족해야만 영역에 자동 할당됩니다.

에이전트 설치 – Windows

Threat Defense 를 설치하기 전에 모든 전제 조건을 만족하였는지 확인합니다. 시스템 요구사항을 참조하십시오.

1. DellThreatDefenseSetup.exe(또는 MSI)를 두 번 클릭하여 설치를 시작합니다.
2. Threat Defense 설치 창에서 **설치**를 클릭합니다.

3. Threat Defense 테넌트에서 제공한 설치 토큰을 입력합니다. **다음**을 클릭합니다.

   참고: 설치 토큰에 액세스하지 못하는 경우에는 Threat Defense 관리자에게 문의하거나 KB 기술 문서 방법:Threat Defense 관리를 참조하십시오.

4. 옵션으로 Threat Defense 의 대상 폴더를 변경합니다.

   확인을 클릭하여 설치를 시작합니다.

5. **마침**을 클릭하여 설치를 완료합니다. Threat Defense 를 시작하려면 확인란을 선택합니다.

Windows 설치 매개변수

에이전트는 GPO, Microsoft System Center Configuration Manager(SCCM) 및 MSIEXEC 를 통해 대화식으로 또는 비대화식으로 설치할 수 있습니다. MSI 는 기본적으로 제공되는 매개변수(아래 참조)를 이용해 사용자 지정하거나, 혹은 명령줄에서 매개변수를 입력할 수도 있습니다.

속성	값	설명
PIDKEY	<설치 토큰>	설치 토큰 자동 입력
LAUNCHAPP	0 또는 1	0: 시스템 트레이 아이콘과 시작 메뉴 폴더가 런타임에서 숨겨집니다. 1: 시스템 트레이 아이콘과 시작 메뉴 폴더가 런타임에서 숨겨지지 않습니다(기본 설정).
SELFPROTECTIONLEVEL	1 또는 2	1: 로컬 관리자만 레지스트리와 서비스를 변경할 수 있습니다. 2: 시스템 관리자만 레지스트리와 서비스를 변경할 수 있습니다(기본 설정).
APPFOLDER	<대상 설치 폴더>	에이전트 설치 디렉터리를 지정합니다. 기본 위치는 C:\Program Files\Cylance\Desktop 입니다.

속성	값	설명
VenueZone	"Zone_Name"	에이전트 버전 1382 이상 필요 •장치를 영역에 추가합니다. •영역이 없는 경우 입력한 이름을 사용하여 영역을 생성합니다. •zone_name 을 기존 영역 또는 생성하려는 영역의 이름으로 바꿉니다. **경고**: 영역 이름의 앞이나 뒤에 공백을 추가하면 새로운 영역이 생성됩니다.

표 3: Windows 설치 매개변수

다음 명령줄 예제는 Microsoft Windows 설치 프로그램 도구(MSIEXEC)를 PIDKEY, APPFOLDER 및 LAUNCHAPP 설치 매개변수로 전달하여 실행하는 방법을 나타냅니다.

```
msiexec /i DellThreatDefenseSetup_x64.msi /qn PIDKEY=<INSTALLATION TOKEN>
LAUNCHAPP=0 /L*v C:\temp\install.log
```

설치는 자동 설치로 진행되며 설치 로그는 **C:\temp** 에 저장됩니다. 에이전트 실행 중에는 시스템 트레이 아이콘과 시작 메뉴의 Threat Defense 폴더가 숨겨집니다. MSIEXEC 에서 사용할 수 있는 다른 명령줄 스위치에 대한 추가 정보는 KB 227091 에 있습니다.

Wyse Device Manager(WDM)를 사용한 Windows 에이전트 설치

여기에서는 설치 스크립트 생성 방법, WDM 에 사용할 RSP 패키지 생성 방법, 그리고 패키지를 WDM 에 추가하여 사용자 상호작용 없이 다수의 씬 클라이언트에 동시에 설치할 수 있는 방법에 대해서 설명합니다.

Threat Defense 의 명령줄 설치를 실행할 배치 파일 스크립트를 작성합니다. WDM 은 배포 시 이 스크립트를 실행합니다.

1. 메모장을 엽니다. 위에서 언급한 명령줄 매개변수를 사용하여 다음 명령을 입력하고 설치를 실행합니다. 이때 **<INSTALLATION TOKEN>**을 사용자의 토큰으로 바꿉니다.
   msiexec /i C:\TDx86\DellThreatDefense_x86.msi PIDKEY=<INSTALLATION TOKEN> /q

   C:\TDx86 은 설치 중에 씬 클라이언트의 이 위치에 복사되는 폴더이므로 Threat Defense 의 디렉터리에 사용됩니다.

2. TDx86 폴더에 **.bat** 확장명으로 파일을 저장합니다. 예: **TDx86_Install.bat**

   Threat Defense Agent 응용 프로그램을 사용자 상호작용 없이 여러 씬 클라이언트에 동시에 설치할 수 있는 RSP 패키지를 생성합니다.

3. WDM 이 설치되어 있는 컴퓨터에서 스크립트 빌더를 엽니다.
4. 패키지 이름과 패키지 설명을 입력합니다.
    - 패키지 카테고리에서 기타 패키지를 선택합니다.
    - 운영 체제에서 Windows Embedded Standard 7 을 선택합니다.
5. 스크립트 명령을 추가하여 대상 시스템이 WES7 또는 WES7p 인지 확인합니다.
    - 스크립트 명령)에서 운영 체제 확인(CO)을 선택합니다.
    - 장치 OS 값으로 해당하는 운영 체제를 입력합니다.
6. 이중 화살표를 사용하여 항목을 추가합니다.
7. 프롬프트에서 **확인**을 누릅니다.
8. 명령을 추가하여 씬 클라이언트를 잠그고 사용자 상호작용을 차단합니다.
    - Select **스크립트 명령** > **사용자 잠금(LU)**을 선택합니다. 값을 입력할 필요는 없습니다. 하지만 이 예에서 **값**에 **예**를 입력하면 설치가 실패하거나 오류가 발생하는 경우 시작 화면이 제거됩니다.
9. 명령을 추가하여 파일을 씬 클라이언트로 복사합니다.
    - 스크립트 명령 **X Copy (XC**)를 선택합니다.
    - **리포지토리 디렉터리** 값의 경우, 기존 **<regroot>** 값 끝에 *****를 추가합니다.
    - **장치 디렉터리** 값의 경우, 대상 씬 클라이언트에 복사할 파일의 경로를 입력합니다. 이번 예에서는 패키지 이름을 사용합니다.
10. 명령을 추가하여 .bat 설치 스크립트를 실행합니다.
    - **스크립트 명령** > **장치에서 실행(EX)**을 선택합니다.
    - 장치 파일 이름 값에서는 경로(**C:\TDx86\TDx86_install.bat**)를 입력합니다. 그러면 TDx86 폴더가 이전 명령인 XC 에서 복사됩니다.
    - 동기 실행 값으로 **+**를 추가합니다. 이 기호는 WDM 에게 파일 실행이 완료될 때까지 기다렸다가 계속하라고 지시하는 의미입니다.
11. 명령을 추가하여 씬 클라이언트에서 복사된 파일을 삭제합니다.
    - 스크립트 명령 **트리 삭제(DT)**를 추가합니다.

12. 명령을 추가하여 잠금을 비활성화합니다.
    - 스크립트 명령 **잠금 종료(EL)**를 추가합니다.
13. 지금까지 결과를 살펴보면 스크립트 패키지가 다음과 비슷한 모습이어야 합니다.
    - Threat Defense 를 WES7P 시스템에 배포하는 경우에는 운영 체제 섹션을 WES7P 로 업데이트합니다. 그렇지 않으면 패키지가 설치되지 않습니다.
14. 패키지를 저장합니다.
    - **저장**을 클릭하고 **TDx86** 폴더의 위치를 찾습니다. 여기 있는 지침을 따른 경우라면 폴더는 바탕 화면에 있습니다.
15. 스크립트 빌더를 닫습니다.
16. WDM 에 패키지를 추가하려면 **WyseDeviceManager** 를 실행합니다.
17. **WyseDeviceManager > 패키지 관리자 > 기타 패키지**로 이동합니다.
18. 메뉴 표시줄에서 **작업 >새로 만들기 > 패키지**를 선택합니다.
19. **스크립트 파일(.RSP)에서 패키지 등록**을 선택하고 **다음**을 클릭합니다.
20. 이전 단계에서 생성한 RSP 파일의 위치로 이동한 후 **다음**을 클릭합니다.
21. **활성**을 선택하고 **다음**을 클릭합니다.
22. WDM 에서 패키지를 등록할 준비가 되면 **다음**을 클릭합니다.
23. 패키지가 등록되면 **마침**을 클릭합니다.
24. 이제 패키지가 **기타 패키지**에 표시됩니다.
25. 다음과 같이 패키지 내용을 확인합니다.
    - 파일 탐색기를 열고 **C:\inetpub\ftproot\Rapport** 로 이동하여 **TDx86 폴더**를 찾습니다.
    - TDx86 폴더를 열고 설치 프로그램과 .bat 파일이 포함되어 있는지 확인합니다.

이제 WDM 에서 패키지를 사용하여 Threat Defense 를 사용자 상호작용 없이 다수의 WES7 씬 클라이언트에 배포할 수 있습니다.

명령줄을 사용하여 격리

장치에서 명령줄을 사용하여 파일을 격리할 수 있습니다. 이렇게 하려면 위협에 대한 SHA256 해시를 알고 있어야 합니다.

참고: 이 기능은 Windows 전용이며 Agent 1432 이상이 필요합니다.

1. Windows 장치에서 명령줄을 엽니다. 예: 시작 메뉴에서 cmd.exe 를 검색합니다.
2. Dell.ThreatDefense.exe 를 호출하고 인수 **-q:<hash>**를 포함합니다. 여기서 <hash>는 파일의 SHA256 해시입니다. 이렇게 하면 에어전트가 파일을 차단된 폴더로 보냅니다.

   명령줄 예(Dell Threat Defense 가 기본 위치에 설치):

   ```
   "C:\Program Files\Cylance\Desktop\Dell.ThreatDefense.exe" -q:
   14233d4875e148c370a6bbe40fccabccdbfa194dac9e8bd41b0eadcf2351f941
   ```

에이전트 삭제

Windows 시스템에서 Agent 를 제거하려면 프로그램 추가/제거 기능을 사용하거나 명령줄을 사용합니다.

Agent 를 제거해도 콘솔에서 장치가 제거되지 않습니다. 콘솔에서 장치를 수동으로 제거해야 합니다.

Agent 를 제거하기 전에 다음을 수행하십시오.

- **Agent 제거에 암호 필요**가 활성화된 경우 제거하기 위한 암호가 있는지 확인하십시오.
- **장치에서 서비스 종료 방지**가 활성화된 경우 정책에서 해당 서비스를 비활성화하거나 Agent 를 제거할 장치에 다른 정책을 적용하십시오.

프로그램 추가/제거를 사용하여 제거

1. **시작** > **제어판**을 선택합니다.
2. **프로그램 제거**를 클릭합니다. 범주 대신 아이콘을 선택한 경우에는 프로그램 및 기능을 클릭하십시오.
3. **Dell Threat Defense** 를 선택한 다음, **제거**를 클릭합니다.

명령줄 사용

1. 관리자 권한으로 명령 프롬프트를 엽니다.
2. Agent 를 설치하는 데 사용한 설치 패키지에 따라 다음 명령을 사용하십시오.
   a. DellThreatDefense_x64.msi
      i. 표준 제거: msiexec /uninstall DellThreatDefense_x64.msi
      ii. Windows 설치 프로그램: msiexec /x DellThreatDefense_x64.msi

b. DellThreatDefense_x86.msi

i. 표준 제거: msiexec /uninstall DellThreatDefense_x86.msi

ii. Windows 설치 프로그램: msiexec /x DellThreatDefense_x86.msi

3. 다음 명령은 선택 사항입니다.

a. 자동 제거의 경우: /quiet

b. 자동 및 숨김의 경우: /qn

c. 암호 보호 제거의 경우 UNINSTALLKEY=<password>

d. 제거 로그 파일의 경우: /Lxv* <path>

i. 이렇게 하면 지정된 경로(<path>)에 로그 파일이 생성되고 파일 이름을 포함합니다.

ii. 예: C:\Temp\Uninstall.log

macOS Agent

시스템 요구사항

Dell 은 끝점 하드웨어(CPU, GPU 등)가 해당 운영 체제의 권장 요구사항을 만족하거나 초과하도록 권장합니다. 예외는 아래와 같습니다(RAM, 사용 가능한 하드 드라이브 공간 및 추가 소프트웨어 요구사항)

운영 체제	• Mac OS X 10.9 • Mac OS X 10.10 • Mac OS X 10.11 • macOS 10.12* • macOS 10.13**
RAM	• 2GB
사용 가능한 하드 드라이브 공간	• 300MB

표 4: macOS 의 시스템 요구 사항

*Agent 1412 이상이 필요합니다.

** Agent 1452 이상이 필요합니다.

설치 파일을 다운로드하는 방법

1. 콘솔(http://dellthreatdefense.com)에 로그인합니다.

2. **설정** > **응용 프로그램**을 선택합니다.

3. **설치 토큰**을 복사합니다.

   설치 토큰은 임의 생성 문자열로서 이를 통해 에이전트가 콘솔에서 할당된 계정에 보고할 수 있습니다. 설치 토큰은 설치 도중 설치 마법사에서, 또는 설치 매개변수 설정 시 필요합니다.

4. 설치 프로그램을 다운로드합니다.

   a. 운영 체제를 선택합니다.

   b. 다운로드할 파일 형식을 선택합니다.

팁: 영역 규칙을 설정하는 경우에는 장치가 영역 규칙 기준을 만족해야만 영역에 자동 할당됩니다.

Agent 설치 – macOS

Threat Defense 를 설치하기 전에 모든 전제 조건을 만족하였는지 확인합니다. 시스템 요구사항을 참조하십시오.

참고: macOS Agent 는 앞으로 Dell 브랜드로 출시될 예정입니다.

1. **`DellThreatDefense.dmg`** 를 더블 클릭하여 설치 프로그램을 탑재합니다.
2. 설치를 시작하려면 PROTECT 사용자 인터페이스에서 *보호* 아이콘을 더블 클릭합니다.
3. **계속**을 클릭하여 운영 체제 및 하드웨어가 요구 사항을 충족하는지 확인합니다.
4. 지침 화면에서 **계속**을 클릭합니다.
5. Threat Defense 테넌트에서 제공한 설치 토큰을 입력합니다. **계속**을 클릭합니다.

참고: 설치 토큰에 액세스하지 못하는 경우에는 Threat Defense 관리자에게 문의하거나 KB 기술 문서 방법:Threat Defense 관리를 참조하십시오.

6. 옵션으로 Threat Defense 의 설치 위치를 변경합니다.

   설치를 클릭하여 설치를 시작합니다.

7. 관리자의 사용자 이름과 암호를 입력합니다. **소프트웨어 설치**를 클릭합니다.
8. 요약 화면에서 **다음**을 클릭합니다.

macOS 설치 매개변수

Threat Defense 에이전트는 단말기의 명령줄 옵션을 사용해 설치할 수 있습니다. 아래는 PKG 설치 프로그램을 사용한 예입니다. DMG 를 사용하는 경우에는 명령에서 파일 확장자만 바꿔주면 됩니다.

참고: 대상 끝점이 시스템 요구사항을 만족해야 하고, 소프트웨어를 설치하는 사람은 설치에 적합한 자격 증명이 필요합니다.

속성	값	설명
InstallToken		콘솔에서 사용할 수 있는 설치 토큰
NoCylanceUI		시작할 때 에이전트 아이콘이 표시되어서는 안 됩니다. 기본 설정은 Visible(표시)입니다.
SelfProtectionLevel	0 또는 1	1: 로컬 관리자만 레지스트리와 서비스를 변경할 수 있습니다. 2: 시스템 관리자만 레지스트리와 서비스를 변경할 수 있습니다(기본 설정).
LogLevel	0, 1, 2 또는 3	0: 오류 – 오류 메시지만 로깅됩니다. 1: 경고 - 오류 및 경고 메시지가 로깅됩니다. 2: 정보(기본값) - 오류, 경고 및 정보 메시지가 로깅됩니다. 문제 해결 시 몇 가지 세부 정보를 얻을 수 있습니다. 3: 자세한 정보 표시 - 모든 메시지가 로깅됩니다. 문제 해결 시 권장되는 로그 레벨입니다. 하지만 자세한 정보 표시 로그 파일 크기가 너무 커질 수도 있습니다. 따라서 Dell 은 문제 해결 시 자세한 정보 표시를 활성화하고 문제가 해결된 후에는 다시 정보로 바꿀 것을 권장합니다.
VenueZone	"zone_name"	에이전트 버전 1382 이상 필요 •장치를 영역에 추가합니다. •영역이 없는 경우 입력한 이름을 사용하여 영역을 생성합니다. •zone_name 을 기존 영역 또는 생성하려는 영역의 이름으로 바꿉니다. **경고**: 영역 이름의 앞이나 뒤에 공백을 추가하면 새로운 영역이 생성됩니다.

표 5: macOS 설치 매개변수

에이전트 설치

설치 토큰을 이용하지 않은 설치

```
sudo installer –pkg DellThreatDefense.pkg –target/
```

설치 토큰을 이용한 설치

```
echo [install_token] > cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

참고: **[install_token]** 을 해당 설치 토큰으로 바꿉니다. echo 명령은 **cyagent_install_token** 파일을 출력합니다. 이 파일은 한 줄당 설치 옵션 한 개가 있는 텍스트 파일입니다. 이 파일은 설치 패키지와 동일한 폴더에 저장되어야 합니다. 파일 확장명에 주의해야 합니다. 위의 예에서 cyagent_install_token 파일은 파일 확장명이 없습니다. macOS 에서는 확장명이 표시되지 않는 것이 기본 설정입니다. 텍스트 편집 또는 다른 텍스트 편집기로 이 파일을 수동으로 작성하면 자동으로 파일 확장명이 추가될 수 있습니다. 이 경우에 파일 확장명을 삭제해야 합니다.

설치 매개변수(옵션)

터미널에서 다음을 입력하여 설치 프로그램에서 입력한 옵션을 적용하기 위해 사용하는 파일(**cyagent_install_token**)을 생성합니다. 각 매개변수는 개별 라인에 입력되어야 합니다. 이 파일은 설치 패키지와 동일한 폴더에 저장되어야 합니다.

다음은 예제입니다. 파일에 모든 매개변수가 필요한 것은 아닙니다. 단말기에는 파일에서 작은 따옴표로 묶인 모든 것이 추가됩니다. 파일에서 각 매개변수 이후에는 Enter/Return 을 눌러서 개별적으로 각 라인을 유지할 수 있도록 해야 합니다.

각 매개변수를 추가하여(라인별로) 파일을 생성할 때는 텍스트 편집기를 사용해도 좋습니다. 이 파일은 설치 패키지와 동일한 폴더에 저장되어야 합니다.

예:

```
echo 'InstallToken
NoCylanceUI
SelfProtectionLevel=2
LogLevel=2'> cyagent_install_token

sudo installer –pkg DellThreatDefense.pkg –target/
```

에이전트 삭제

암호가 없는 경우

```
sudo
/Applications/Cylance/Uninstall\ DellThreatDefense.app/Contents/MacOS/
Uninstall\ DellThreatDefense
```

암호가 있는 경우

```
sudo
/Applications/Cylance/Uninstall\ DellThreatDefense.app/Contents/MacOS/
Uninstall\ DellThreatDefense --password=thisismypassword
```

참고: **thisismypassword** 를 콘솔에서 생성한 삭제 암호로 바꿉니다.

에이전트 서비스

서비스 시작

```
sudo launchctl load
/Library/launchdaemons/com.cylance.agent_service.plist
```

서비스 중단

```
sudo launchctl unload
/Library/launchdaemons/com.cylance.agent_service.plist
```

설치 확인

다음 파일을 보고 에이전트가 올바로 설치되었는지 확인합니다.

1. 프로그램 폴더가 생성되었습니다.
    - Windows 기본값: **C:\Program Files\Cylance\Desktop**
    - macOS 기본값: **/Applications/DellThreatDefense/**
2. Threat Defense 아이콘이 대상 장치의 시스템 트레이에 표시됩니다.

    매개변수 LAUNCHAPP=0(Windows) 또는 NoCylanceUI(macOS)를 사용하는 경우에는 표시되지 않습니다.
3. 대상 장치의 시작\모든 프로그램에 Threat Defense 폴더가 있습니다.

    매개변수 LAUNCHAPP=0(Windows) 또는 NoCylanceUI(macOS)를 사용하는 경우에는 표시되지 않습니다.

4. Threat Defense 서비스가 추가되어 실행됩니다. 대상 장치의 Windows 서비스 패널에 실행 중인 Threat Defense 서비스가 나열되어야 합니다.
5. Dell.ThreatDefense.exe 프로세스가 실행 중입니다. 대상 장치의 Windows 작업 관리자에서 프로세스 탭에 Dell.ThreatDefense.exe 프로세스가 나열되어야 합니다.
6. 장치가 콘솔에게 보고합니다. 콘솔에 로그인하여 장치 탭을 클릭했을 때 대상 장치가 온라인 상태로 표시되어야 합니다.

에이전트 사용자 인터페이스

에이전트 사용자 인터페이스는 기본적으로 활성화됩니다. 사용자 인터페이스를 보려면 시스템 트레이에서 에이전트 아이콘을 클릭합니다. 또는 에이전트 아이콘이 시스템 트레이에 보이지 않도록 에이전트를 설치할 수도 있습니다.

위협 탭

장치에서 발견된 모든 위협 요소와 실시한 조치가 표시됩니다. *안전하지 않음*은 해당 위협 요소에 아무 조치를 취하지 않았음을 의미합니다. *격리됨*은 해당 파일이 실행되지 않도록 위협 요소가 수정되고 *격리* 폴더로 이동되었음을 의미합니다. *면제됨*은 관리자가 파일을 안전하다고 간주하고 장치에서 실행을 *허용*한 것을 의미합니다.

이벤트 탭

장치에서 발생한 위협 이벤트가 모두 표시됩니다.

스크립트 탭

장치에서 실행된 악성 스크립트와 이 스크립트에 대한 조치가 표시됩니다.

에이전트 메뉴

에이전트 메뉴는 Threat Defense 도움말과 업데이트에 액세스할 수 있는 수단을 제공합니다. 그 밖에 더 많은 메뉴 옵션이 포함된 고급 사용자 인터페이스에 액세스할 수 있는 수단도 있습니다.

에이전트 메뉴

에이전트 메뉴에서는 사용자가 장치에 대한 몇 가지 작업을 실행할 수 있습니다. 에이전트 아이콘을 오른쪽 클릭하면 메뉴가 나타납니다.

- **업데이트 확인**: 에이전트가 유효한 업데이트 여부를 확인하여 설치합니다. 업데이트는 장치가 속한 영역에 허용되는 에이전트 버전으로 제한됩니다.

- **정책 업데이트 확인**: 에이전트는 정책 업데이트를 사용할 수 있는지 확인합니다. 기존 정책 또는 에이전트에 적용되는 다른 정책에 변경이 있는 것일 수 있습니다.

  참고: Windows 용 버전 1422(이상) 또는 macOS 용 버전 1432(이상)에서 정책 업데이트가 지원되는지 확인합니다.

- **정보**: 에이전트 버전, 장치에 할당된 정책 이름, 에이전트가 업데이트를 확인한 마지막 시간, 그리고 설치 시 사용한 설치 토큰이 대화 상자에 표시됩니다.

- **종료**: 시스템 트레이의 에이전트 아이콘을 닫습니다. 그렇다고 Threat Defense 서비스가 종료되지는 않습니다.

- **옵션 > 알림 표시**: 이 옵션을 선택하면 새로운 이벤트를 모두 알림 메시지로 표시합니다.

에이전트 사용자 인터페이스의 고급 옵션 활성화

Threat Defense 에이전트는 콘솔 연결 없이 사용자 인터페이스를 통해 장치에서 이용할 수 있는 몇 가지 고급 옵션을 제공합니다. 고급 옵션을 활성화하려면 CylanceSVC.exe 를 실행해야 합니다.

Windows

1. 에이전트 아이콘이 시스템 트레이에 표시되면 아이콘을 오른쪽 클릭하고 **종료**를 클릭합니다.
2. 명령 프롬프트를 실행하여 다음 명령을 입력합니다. 입력이 완료된 후에는 Enter 를 누릅니다.

   `cd C:\Program Files\Cylance\desktop`

   응용 프로그램이 다른 위치에 설치되어 있는 경우에는 명령 프롬프트에서 해당 위치로 이동합니다.
3. 다음 명령을 입력하고 Enter 를 누릅니다.

   `Dell.ThreatDefense.exe –a`

   에이전트 아이콘이 시스템 트레이에 표시됩니다.
4. 아이콘을 오른쪽 클릭합니다. *로깅*, *탐지 실행* 및 *위협 관리* 옵션이 표시됩니다.

macOS

1. 에이전트 아이콘이 상단 메뉴 표시되면 아이콘을 오른쪽 클릭하고 **종료**를 클릭합니다.
2. 터미널을 열고 다음을 실행합니다.

   a. Sudo /Applications/DellThreatDefense/DellThreatDefense.app/Contents/MacOS/DellThreatDefenseUI –a

   참고: Dell Threat Defense 의 기본 설치 경로입니다. 사용자 환경에 따라 경로를 편집해야 하는 경우도 있습니다.
3. 이제 에이전트 UI 가 추가 옵션과 함께 나타납니다.

로깅

에이전트에서 수집할 로그 정보 레벨을 선택합니다. 기본값은 정보입니다. Dell 은 문제 해결 시 로그 레벨을 모두(자세한 정보 표시)로 설정할 것을 권장합니다. 문제 해결이 완료되면 이 설정을 정보로 다시 바꾸십시오(모든 정보를 로깅할 경우 로그 파일 크기가 너무 커질 수 있습니다).

탐지 실행

사용자가 위협 요소를 스캔할 폴더를 지정할 수 있습니다.

1. **탐지 실행** > **폴더 지정**을 선택합니다.
2. 스캔할 폴더를 선택한 후 **확인**을 클릭합니다. 발견되는 위협 요소가 에이전트 사용자 인터페이스에 표시됩니다.

위협 관리

사용자는 이 기능으로 해당 장치에서 *격리됨* 파일을 삭제할 수 있습니다.

1. **위협 관리** > **격리됨 삭제**를 선택합니다.
2. **확인**을 클릭하여 확인합니다.

가상 시스템

Threat Defense 에이전트를 가상 시스템 이미지로 사용할 때는 몇 가지 권장 사항이 있습니다.

템플릿으로 사용할 가상 시스템 이미지를 생성할 때는 에이전트 설치에 앞서 가상 시스템 네트워크 설정을 분리합니다. 그래야만 에이전트가 콘솔과 통신하지 않아 장치 세부 정보를 구성하지 않습니다. 또한 콘솔에서 장치가 중복되는 것을 방지할 수 있습니다.

암호 보호 삭제

설정 > 응용 프로그램

관리자는 에이전트 삭제 시 암호를 요구할 수 있습니다. 암호를 이용해 에이전트를 삭제하는 경우:

- MSI 설치 프로그램을 사용해 설치한 경우 MSI 또는 제어판을 사용해 삭제할 수 있습니다.
- EXE 설치 프로그램을 사용해 설치한 경우 EXE 를 사용해 삭제합니다. EXE 설치 프로그램을 사용한 후 삭제 시 암호를 요구할 경우에는 제어판을 사용하지 못합니다.
- 명령줄을 사용해 삭제할 때는 다음과 같이 삭제 문자열을 추가합니다. **`UNINSTALLKEY = [MyUninstallPassword]`**.

삭제 암호를 생성하는 방법

1. 관리자 계정으로 콘솔(http://dellthreatdefense.com)에 로그인합니다.
2. **설정** > **응용 프로그램**을 선택합니다.
3. **에이전트 제거에 암호 필요** 확인란을 선택합니다.
4. 암호를 입력합니다.
5. **저장**을 클릭합니다.

통합

Threat Defense 콘솔에서는 타사의 프로그램을 통합할 수 있습니다.

Syslog/SIEM

Threat Defense 는 Syslog 기능을 사용해 Security Information Event Management(SIEM) 소프트웨어와 통합할 수 있습니다. Syslog 이벤트는 에이전트 이벤트가 콘솔에 지속될 때 동시에 지속됩니다.

Syslog 메시지를 위해 최신 IP 주소가 필요한 경우에는 Dell Support 에게 문의하십시오.

이벤트 유형

감사 로그

이 옵션을 선택하면 콘솔(웹사이트)에서 실행한 사용자 작업이 감사 로그로 Syslog 서버에 전송됩니다. 이 옵션을 선택 해제하더라도 감사 로그 이벤트는 감사 로그 화면에 항상 표시됩니다.

Syslog 로 전송되는 감사 로그 메시지의 예

장치

이 옵션을 선택하면 장치 이벤트가 Syslog 서버로 전송됩니다.

- 새 장치를 등록하면 등록 이벤트에 대한 메시지로 Registration 및 SystemSecurity 가 수신됩니다.

  장치 등록 이벤트의 메시지 예

- 장치를 제거할 경우

  장치 제거 이벤트의 메시지 예

- 장치 정책, 영역, 이름 또는 로깅 레벨이 변경된 경우

  장치 업데이트 이벤트의 메시지 예

위협

이 옵션을 선택하면 새롭게 발견된 위협 또는 기존 위협에서 관찰된 변경 사항이 Syslog 서버로 전송됩니다. 변경 사항에는 *제거*, *격리*, *면제*, *실행*되는 위협이 포함됩니다.

위협 이벤트는 아래와 같이 5 가지 유형이 있습니다.

- **위협_발견**: 새로운 위협이 *안전하지 않음* 상태에서 발견되었습니다.
- **위협_제거**: 기존 위협이 *제거*되었습니다.
- **위협_격리**: 새로운 위협이 *격리*된 상태로 발견되었습니다.
- **위협_면제**: 새로운 위협이 *면제*된 상태로 발견되었습니다.
- **위협_변경**: 기존 위협 요소의 특성이 변경됨(예: 점수, 격리 상태, 실행 상태)
- **threat_cleared**: 위협이 면제되거나 안전 목록에 추가되거나 장치의 격리 폴더에서 삭제되었습니다.

위협 이벤트의 메시지 예

Threat Classifications(위협 분류)

오늘날 수백 개에 이르는 위협 요소가 매일 맬웨어 또는 Potentially Unwanted Program(PUP)로 분류됩니다. 이 옵션을 선택하면 분류 이벤트 발생 시 알 수 있도록 알림 메시지를 구독합니다.

위협 분류의 메시지 예

SIEM(Security Information and Event Management)

이벤트를 전송할 Syslog 서버 또는 SIEM 의 유형을 지정합니다.

Protocol(프로토콜)

Syslog 서버의 구성과 일치해야 합니다. UDP 또는 TCP 중 하나를 선택할 수 있습니다. UDP 는 메시지 전송을 보증할 수 없기 때문에 일반적으로 권장하지 않습니다. Dell 은 TCP(기본 설정)를 권장합니다.

TLS/SSL

프로토콜을 TCP 로 지정한 경우에만 사용할 수 있습니다. TLS/SSL 은 Threat Defense 에서 Syslog 서버로 전송되는 Syslog 메시지를 암호화합니다. Dell 은 이 옵션 선택을 권장합니다. 이때 Syslog 서버는 TLS/SSL 메시지를 수신 대기할 수 있도록 구성해야 합니다.

IP/Domain(IP/도메인)

고객이 설정한 Syslog 서버의 IP 주소 또는 전체 주소 도메인 이름(FQDN)을 지정합니다. 내부 네트워크 전문가에게 문의하여 방화벽과 도메인 설정이 올바로 구성되었는지 확인하십시오.

포트

Syslog 서버가 메시지를 수신 대기하는 장치의 포트 번호를 지정합니다. 번호는 1~65535 가 되어야 합니다. 일반적인 값은 다음과 같습니다. UDP 의 경우 512, TCP 의 경우 1235 또는 1468, Secured TCP 의 경우 6514(예: TLS/SSL 이 활성화된 TCP).

Severity(심각도)

Syslog 서버에 표시되는 메시지의 심각도를 지정합니다. 이것은 주관적인 필드이므로 무엇이든 원하는 수준으로 설정할 수 있습니다. 심각도 값이 Syslog 로 전송되는 메시지를 바꾸지는 못합니다.

Facility(시설)

메시지를 로깅하는 응용 프로그램의 유형을 지정합니다. 기본 설정은 Internal(내부, 즉 Syslog)입니다. 이 옵션은 Syslog 서버에서 수신되는 메시지를 카테고리화하는 데 사용됩니다.

연결 테스트

IP/도메인, 포트, 프로토콜 설정을 테스트하려면 **테스트 연결**을 클릭합니다. 유효한 값을 입력하면 잠시 후 *성공* 확인이 표시됩니다.

사용자 지정 인증

외부 ID 공급자(IdP)를 사용하여 콘솔에 로그인합니다. 이를 위해서는 IdP 를 이용해 설정을 구성하여 IdP 로그인을 확인할 수 있는 X.509 인증서와 URL 을 가져와야 합니다. 사용자 지정 인증은 Microsoft SAML 2.0 에서 호환됩니다. 이 기능은 OneLogin, OKTA, Microsoft Azure 및 PingOne 에서도 호환되는 것으로 확인되었습니다. 그 밖에도 사용자 지정 설정을 제공하기 때문에 Microsoft SAML 2.0 을 기반으로 한 다른 ID 공급자에서도 호환되어야 합니다.

참고: 사용자 지정 인증 기능은 Active Directory Federation Service(ADFS)를 지원하지 않습니다.

- **강력한 인증**: 다단계 인증 액세스 기능을 제공합니다.
- **SSO(Single Sign-On)** Single Sign-On(SSO) 액세스 기능을 제공합니다.

  참고: 강력한 인증 또는 Single Sign-On 을 선택하더라도 사용자 지정 인증 설정값에는 아무런 영향도 끼치지 않습니다. 구성 설정값은 모두 ID 공급자(IdP)에서 처리하기 때문입니다.
- **암호 로그인 허용**: 이 옵션을 선택하면 SSO 를 사용하여 콘솔에 직접 로그인할 수 있습니다. 또한 콘솔에서 잠김 없이 SSO 설정 테스트가 가능합니다. SSO 를 통해 콘솔에 성공적으로 로그인한 후 이 기능을 비활성화하는 것이 좋습니다.
- **공급자:** 사용자 지정 인증에 필요한 서비스 공급자를 선택합니다.

- **X.509 인증서**: X.509 인증서 정보를 입력합니다.
- **로그인 URL**: 사용자 지정 인증에 필요한 URL 을 입력합니다.

위협 데이터 보고서

다음과 같이 조직 관련 정보가 포함된 스프레드시트입니다.

- **위협**: 조직에서 발견된 모든 위협 요소를 나열합니다. 이 정보에는 파일 이름과 파일 상태(*안전하지 않음*, *비정상*, *면제됨*, *격리됨*)가 포함됩니다.
- **장치**: 조직에서 Threat Defense 에이전트가 설치된 모든 장치를 나열합니다. 여기에는 장치 이름, 운영 체제 버전, 에이전트 버전 및 적용된 정책이 포함됩니다.
- **위협 표시기**: 각 위협 요소와 관련된 특성을 나열합니다.
- **삭제됨**: 조직에서 *삭제*된 모든 파일을 나열합니다. 이 정보는 *면제*된 파일, *안전 목록*에 추가된 파일 및 장치의 *차단된* 폴더에서 *삭제*된 파일을 포함합니다.
- **이벤트**: 지난 30 일 동안 위협 이벤트 그래프와 관련된 모든 이벤트를 대시보드에 나열합니다. 여기에는 파일 해시, 장치 이름, 파일 경로, 그리고 이벤트 발생 날짜가 포함됩니다.

이 기능을 활성화하면 보고서가 1:00 AM(PST)에 자동으로 업데이트됩니다. 업데이트를 수동으로 생성하려면 **보고서 재생성**을 클릭합니다.

위협 데이터 보고서는 콘솔에 로그인하지 않고도 보고서를 다운로드할 수 있도록 URL 과 토큰을 제공합니다. 토큰은 필요에 따라 삭제 또는 재생성이 가능하기 때문에 보고서에 대한 액세스 주체를 통제할 수 있습니다.

문제 해결

여기에서는 질문 목록을 비롯해 Threat Defense 의 문제 발생 시 수집해야 할 파일에 대해서 알아봅니다. Dell Support 에서 문제 해결을 지원하기 위해서는 이 정보가 필요하기 때문입니다.

또한 몇 가지 공통 문제와 권장 방안도 제시합니다.

지원

설치 매개변수

- 설치 방법은 무엇입니까? 사용할 매개 변수를 제공합니다.
    - 예 – Windows: 명령줄에서 설치하여 런타임 시 에이전트 아이콘과 시작 메뉴 폴더를 숨기려면 LAUCHAPP=0 을 사용합니다.
    - 예 – macOS: 명령줄에서 설치하여 에이전트의 자체 보호 기능을 비활성화려면 SelfProtectionLevel=1 을 사용합니다.
- 설치 단계 중 확인 가능한 단계는 무엇입니까?
    - 예 – Windows: MSI 또는 EXE 설치 프로그램의 사용 여부
    - 예 – 모든 OS: Quiet Mode 또는 No Agent user interface 등 명령줄 옵션의 사용 여부
- 설치 시 자세한 정보 표시 로깅을 활성화합니다.

성능 문제

- Threat Defense 프로세스 및 메모리 사용량을 나타내는 작업 관리자(Windows) 또는 Activity Monitor(macOS)의 스크린샷을 캡처합니다.
- Threat Defense 프로세스 덤프를 캡처합니다.
- 디버그 로그를 수집합니다.
- 문제 발생 시 출력되는 시스템 정보를 수집합니다.
    - Windows 의 경우: msinfo32 또는 winmsd
    - macOS 의 경우: 시스템 정보
- 관련 이벤트 로그(Windows) 또는 콘솔 정보(macOS)를 수집합니다.

업데이트, 상태 및 연결 문제

- 방화벽 포트 443 이 열려 있고, 장치 주소를 확인하여 Cylance.com 사이트에 연결할 수 있는지 확인합니다.
- 장치가 콘솔의 장치 페이지에 표시됩니까? 온라인 상태입니까, 혹은 오프라인 상태입니까? 마지막으로 연결한 시간이 언제입니까?
- 인터넷 연결을 위해 장치에서 프록시를 사용하고 있습니까? 자격 증명이 프록시에 올바로 구성되어 있습니까?
- 콘솔에 연결할 수 있도록 Threat Defense 서비스를 다시 시작합니다.

- 디버그 로그를 수집합니다.
- 문제 발생 시 출력되는 시스템 정보를 수집합니다.
    - Windows 의 경우: msinfo32 또는 winmsd
    - macOS 의 경우: 시스템 정보

디버그 로깅 활성화

Threat Defense 는 기본적으로 **C:\Program Files\Cylance\Desktop\log** 에 저장된 로그 파일을 유지합니다. Threat Defense 는 문제 해결을 위해 더 자세한 정보 표시 로그를 생성하도록 구성할 수 있습니다.

스크립트 제어 비호환성

문제:

일부 장치에서 스크립트 제어가 활성화되어 있는 경우 해당 장치에서 실행 중인 다른 소프트웨어와 충돌을 일으킬 수 있습니다. 이러한 충돌은 일반적으로 다른 소프트웨어에서 호출하는 일부 프로세스에 에이전트가 삽입되면서 비롯됩니다.

해결 방법:

이러한 문제는 소프트웨어에 따라 콘솔의 장치 정책에 특정 프로세스 제외를 추가하여 해결할 수 있습니다. 그 밖에 충돌 장치에서 호환성 모드(레지스트리 키)를 활성화하여 해결하는 방법도 있습니다. 하지만 제외하는 방법이 효과가 없을 때는 장치에 영향을 미치는 장치 정책에서 스크립트 제어를 비활성화하여 정상적인 장치 기능을 복구하는 것이 바람직합니다.

참고: 호환 모드 솔루션은 에이전트 버전 1370 용입니다. 에이전트 1382 이상 버전부터 다른 제품과의 호환을 위해 주입 프로세스가 업데이트되었습니다.

호환성 모드

다음 레지스트리 키를 추가하여 호환성 모드를 활성화합니다.

1. 레지스트리 에디터를 사용하여 **HKEY_LOCAL_MACHINE\SOFTWARE\Cylance\Desktop** 으로 이동합니다.
2. 마우스 오른쪽 단추로 **데스크톱**을 클릭한 뒤 **허용**을 클릭하고 소유권을 획득한 뒤 **모든 권한**을 부여합니다. **확인**을 클릭합니다.

3. 마우스 오른쪽 단추로 **데스크톱**을 클릭하고 **새로 만들기** > **이진 값**을 선택합니다.
4. 파일 이름을 **CompatibilityMode** 로 지정합니다.
5. 레지스트리 설정을 열고 값을 **01** 로 변경합니다.
6. **OK(확인)**를 클릭하고 레지스트리 에디터를 닫습니다.
7. 장치를 다시 시작해야 할 수도 있습니다.

명령줄 옵션

Psexec 사용:

```
psexec -s reg add HKEY_LOCAL_MACHINE\SOFTWARE
\Cylance\Desktop /v CompatibilityMode /t REG_BINARY /d 01
```

여러 장치에서 명령을 실행하려면 다음과 같이 **Invoke-Command cmdlet** 를 사용합니다.

```
$servers = "testComp1","testComp2","textComp3"

$credential = Get-Credential -Credential {UserName}\administrator

Invoke-Command -ComputerName $servers -Credential $credential -
ScriptBlock {New-Item -Path HKCU:\Software\Cylance\Desktop -Name
CompatibilityMode -Type REG_BINARY -Value 01}
```

부록 A: 용어집

비정상적	점수가 비교적 낮아(1~59) 맬웨어일 가능성이 적은 의심스러운 파일
관리자	Threat Defense 테넌트 관리자
에이전트	콘솔과 통신하는 Threat Defense 끝점 호스트
감사 로그	Threat Defense 콘솔에서 실행되는 작업을 기록한 로그
자동 격리	모든 *안전하지 않음* 및/또는 *비정상* 파일의 실행을 자동으로 방지합니다.
자동 업로드	*안전하지 않음* 또는 *비정상*으로 감지된 알 수 없는 모든 PE(Portable Executable) 파일을 Cylance Infinity 클라우드에 분석을 위해 자동으로 업로드합니다.
콘솔	Threat Defense 관리 사용자 인터페이스
장치 정책	조직 관리자가 모든 장치의 위협 요소 처리 방식을 정의하도록 구성할 수 있는 Threat Defense 정책
전역적 격리	전역적으로(조직 내 모든 장치) 파일 실행을 차단합니다.

전역적 안전 목록	전역적으로(조직 내 모든 장치) 파일 실행을 허용합니다.
인피니티(Infinity)	파일에 점수를 매기기 위해 사용되는 수학적 모델
조직	Threat Defense 서비스를 사용하는 테넌트 계정
격리	파일의 로컬(특정 장치) 실행을 차단합니다.
위협	Threat Defense 에서 탐지하는 잠재적인 유해한 파일로서 *안전하지 않음* 또는 *비정상*으로 분류됩니다.
안전하지 않음	점수가 비교적 높아(60~100) 맬웨어일 가능성이 많은 의심스러운 파일
면제	파일의 로컬(특정 장치) 실행을 허용합니다.
영역	조직 내에서 우선순위, 기능 등에 따라 장치를 구성 및 그룹화하는 방법
영역 규칙	IP 주소, 운영 체제 및 장치 이름에 따라 장치를 특정 영역에 자동 할당할 수 있는 기능

부록 B: 예외 처리

사용자가 파일을 수동으로 *격리* 또는 *허용*(*면제*)해야 하는 경우가 있습니다. Threat Defense 는 각 장치(*로컬*), 장치 그룹(*정책*), 전체 조직(*전역*)에 대한 예외를 처리하는 방법을 제공합니다.

파일

로컬: 해당 장치의 파일을 *격리* 또는 *면제*(*안전 목록*)합니다. 파일을 분석하기 전에 파일을 일시적으로 *차단* 또는 *허용*할 때 유용합니다. 한 장치에서 파일을 *면제*하면 이 장치가 해당 파일의 *실행*을 허용해야 하는 유일한 장치인 경우에도 유용합니다. 여러 장치에서 조치를 취해야 하는 경우라면 *정책* 또는 *전역*을 사용하는 것이 좋습니다.

정책: 정책에 할당한 모든 장치에서 파일을 *안전 목록*에 추가합니다. 장치 그룹에 따라 파일을 허용하는 데 유용합니다(예를 들어 IT 장치가 PsExec 같이 악의적인 목적으로 사용될 가능성이 있는 도구를 실행할 수 있습니다). 사용할 수 없는 정책 수준에서 파일을 *격리*합니다.

전역: 조직의 파일을 *격리*하거나 *안전 목록*에 추가합니다. 조직에서 알려진 악성 파일을 *격리*합니다. 조직에서 안전하다고 알려지고 사용 중이지만 에이전트에서 악성 파일로 표시한 파일을 *안전 목록*에 추가합니다.

스크립트

정책: 스크립트 제어는 지정 폴더에서만 스크립트를 실행할 수 있도록 허용하는 기능입니다. 폴더에서 스크립트를 실행하도록 허용하면 하위 폴더의 스크립트도 허용됩니다.

인증서

전역: 인증서를 콘솔에 먼저 추가하고 나서 *전역 안전 목록*에 추가합니다. 그러면 인증서에서 서명한 응용 프로그램을 조직에서 실행할 수 있습니다.

인증서를 추가하려면 **설정** > **인증서**를 선택한 다음 **인증서 추가**를 클릭합니다.

인증서를 *전역 안전 목록*에 추가하려면 **설정** > **전역 목록**, **안전** 탭, **인증서** 탭을 차례로 선택한 다음, **인증서 추가**를 클릭합니다.

부록 C: 사용자 권한

사용자에게 가능한 작업은 사용자에게 할당되는 권한(역할)에 따라 달라집니다. 일반적으로 관리자는 조직 내 어디에서든지 작업을 실행할 수 있습니다. 영역 관리자와 사용자는 자신이 할당된 영역으로 권한이 제한됩니다. 즉, 영역에 속하는 장치에 액세스하거나 이러한 장치 관련 위협 데이터를 볼 수 있는 권한으로만 제한됩니다. 영역 관리자 또는 사용자도 장치가 자신에게 할당된 영역에 속하는 않을 때는 장치 또는 위협 요소를 볼 수 없습니다.

	사용자	영역 관리자	관리자
에이전트 업데이트			
보기/편집			x
감사 로깅			
보기			x
장치			
장치 추가 - 전역적			x
장치를 영역에 추가			x
장치 제거 - 전역적			x
장치를 영역에서 제거		x	x
장치 이름 편집		x	x
영역			
영역 생성			x
영역 삭제			x
영역 이름 편집 - 모두			x
할당된 영역 이름 편집		x	x

	사용자	영역 관리자	관리자
정책			
정책 생성 - 전역적			X
영역 정책 생성			X
정책 추가 - 전역적			X
정책을 영역에 추가		X	X
정책 제거 - 전역적			X
정책을 영역에서 제거		X	X
위협			
파일 격리 - 전역적			X
영역에서 파일 격리	X	X	X
파일 면제 - 전역적			X
영역에서 파일 면제	X	X	X
전역적 격리/안전			X
설정			
설치 토큰 생성 또는 삭제			X
초대 URL 생성 또는 삭제			X
설치 토큰 복사	X	X	X
초대 URL 복사			X
사용자 관리			
사용자를 영역에 할당			X
사용자를 관리형 영역에 할당		X	X
영역 관리자 할당 - 전역적			X
영역 관리자를 관리형 영역에 할당		X	X
사용자를 콘솔에서 삭제			X
사용자를 영역에서 제거 - 전역적			X
사용자를 관리형 영역에서 제거		X	X

부록 D: 파일 기반 쓰기 필터

Dell Threat Defense Agent 는 Windows Embedded Standard 7 을 실행하는 시스템(씬 클라이언트)에 설치할 수 있습니다. 내장형 장치에서는 시스템 저장소에 쓰기 작업을 할 수 없습니다. 이러한 경우에 시스템에서는 파일 기반 쓰기 필터(FBWF)를 사용하여 시스템 저장소에 대한 쓰기 작업을 시스템 메모리의 캐시로 리디렉션합니다. 하지만 이렇게 하면 시스템을 다시 시작할 때마다 에이전트의 변경사항이 유실되는 문제가 발생할 수 있습니다.

내장형 시스템에서 에이전트를 사용하는 경우 다음 절차를 사용합니다.

1. 에이전트를 설치하기 전에 다음 명령을 사용하여 FBWF 를 비활성화합니다. `fbwfmgr /disable`
2. 시스템을 다시 시작합니다. 이렇게 하면 FBWF 가 비활성화됩니다.
3. Dell Threat Defense Agent 를 설치합니다.
4. 에이전트를 설치한 후 다음 명령을 사용하여 FBWF 를 다시 활성화합니다. `fbwfmgr /enable`
5. 시스템을 다시 시작합니다. 이렇게 하면 FBWF 가 다시 활성화됩니다.
6. FBWF 에서 다음 폴더를 제외합니다.
    a. C:\Program Files\Cylance\Desktop - 이 폴더를 제외하면 시스템을 다시 시작한 후 에이전트 업데이트가 지속됩니다.
7. 다음 명령을 사용하여 바탕 화면 폴더를 제외합니다. `/ addexclusion C: "\Program Files\Cylance\Desktop\"`
    a. 여기서는 기본 디렉터리에 설치하는 것으로 간주합니다. 에이전트를 설치한 폴더로 제외 폴더를 변경합니다.
8. 에이전트에 대한 테스팅용 시스템에 위협 요소를 저장하려는 경우 FBWF 의 저장소 위치(예: `C:\Samples`)도 제외해야 합니다.