ForeScout의 의뢰로 실시된
Forrester Consulting의
Thought Leadership Paper

2017년 11월

계획의 실패, 실패를 위한 계획

IoT 환경의 보안에서 LoB 실무자와 SOC의 역할 이해

FORRESTER®

목차

프로젝트 책임자:
Chris Taylor,
시장 영향 담당 선임 컨설턴트

관련 연구:
Forrester 보안 및 위험 연구 그룹

FORRESTER CONSULTING 정보

Forrester Consulting은 조사 결과를 토대로 한 독립적이고 객관적인 컨설팅을 통해 조직의 리더들이 성공하도록 돕습니다. 단기 전략 세션에서 맞춤 프로젝트까지 다양한 범위를 아우르는 Forrester의 컨설팅 서비스는 구체적인 사업상의 문제에 대해 전문적인 통찰력을 제공해 줄 조사 애널리스트와 고객을 직접 연결해 줍니다. 자세한 내용은 forrester.com/consulting을 참조하십시오.

FORRESTER®

개요

기술적 진보로 인해 새로운 유형의 연결 장치인 사물 인터넷(IoT)의 발생이 폭주했고, 결국 기업이 대응하거나 심지어 인식하기 위한 장비도 아직 제대로 갖추어지지 않은 새로운 보안 위협이 생겨났습니다. 많은 기업들이 이러한 새로운 보안 요구 사항 해결에 충분히 준비되지 않아, 낡은 전략과 정책으로 새로운 위협에 대응하고 있습니다. 또한, 운영 기술(OT)을 자주 활용하는 개별 사업 부서(LOB)와 보안 운영 센터(SOC)와 같은 기존의 보안 팀은 IoT 연결 장치가 어떻게 관리되어야 하는지에 대해 의견이 다른 경우가 흔히 발생합니다.

2017년 8월, ForeScout는 Forrester Consulting에 기업 전체에서 사용되든 특정 업무 영역을 지원하든 관계없이 네트워크 상에 연결된 IoT 장치의 폭발적인 증가에 따라 조직이 적절하고 정확하게 해당 네트워크를 보호할 수 있는지 여부를 확인해달라고 의뢰했습니다. 회사 내에서 운영 기술을 사용하는 개별 사업 부서는 종종 필수적인 보안 감독 없이 이러한 새로운 장치나 애플리케이션을 구현하여 네트워크 내 보안 취약성을 야기시킵니다. 보안 팀은 "볼" 수 없는 것을 방어할 수는 없습니다. 따라서, 모든 장치에 대한 정보는 안전한 운영의 핵심입니다. 설문 조사에 따르면, 기업들은 새로운 연결 시대의 네트워크 보안에 대해 진심으로 우려하고 있으며, 이렇게 커지고 있는 보안 문제를 해결할 수 있는 적절한 도구, 리소스 및 프로세스를 찾기 위해 애쓰고 있습니다.

Forrester는 사물 인터넷을 사물과 인프라가 인터넷 형태의 네트워크를 통해 모니터링, 분석 및 제어 시스템과 인터랙션할 수 있게 해주는 기술로 정의합니다. 여기에는 특정 장치, 즉 사물뿐만 아니라, 이 기술이 가능하게 하는 프로세스 및 기능, 즉 운영 기술(OT)이 포함됩니다. 이 연구를 위해, 우리는 IoT라는 광범위한 카테고리 밑에 연결된 "사물"(즉, 장치)과 OT를 함께 묶었습니다.

주요 조사 결과

- IoT는 보안 리더들이 네트워크를 보호하는 방식을 재평가하도록 하고 있습니다.
- IoT 보안에 대한 위험 감수성향은 놀라울 정도로 높아서, 보안 팀이 보안 전략을 발전시켜야만 합니다.
- IoT 보안은 보안 리더 의 50% 이상에게 불안감을 주고 있습니다.
- IoT 관리 및 보안 책임 주체에 대한 개별 사업 부서와 IT 부서 간의 공통된 견해는 거의 없습니다.
- 규정 준수에는 보이는 장치를 기반으로 하는 감사만으로도 충분할 수 있지만, 보안에 있어서는 알려진 장치와 알려지지 않은 장치 모두에 대한 정보가 결정적으로 중요합니다.
- IoT 보안을 향상시키기 위해서는 장치 정보를 아는 것과 규정 준수를 향상시키는 것이 핵심 절차입니다.

사물 인터넷(IoT)은 새로운 보안 접근법을 요합니다

세계는 커넥티드 제품(사물 인터넷) 혁명의 한가운데에 있으며, 기업의 90%는 향후 몇 년 동안 연결된 기기의 양이 증가할 것으로 예상하고 있습니다. 기업은 비즈니스 프로세스 및 기능을 향상시키기 위해 기존에는 연결되지 않았던 장치를 네트워크에 연결함으로써 얻을 수 있는 이점을 이미 접하고 있습니다. 하지만, 기업들은 이러한 새로운 장치들이 보안 요구 사항 추가라는 부담을 가져온다는 것도 알고 있습니다. 기업의 77%는 IoT 장치의 사용 증가가 심각한 보안 문제를 야기한다는 것을 인정합니다.

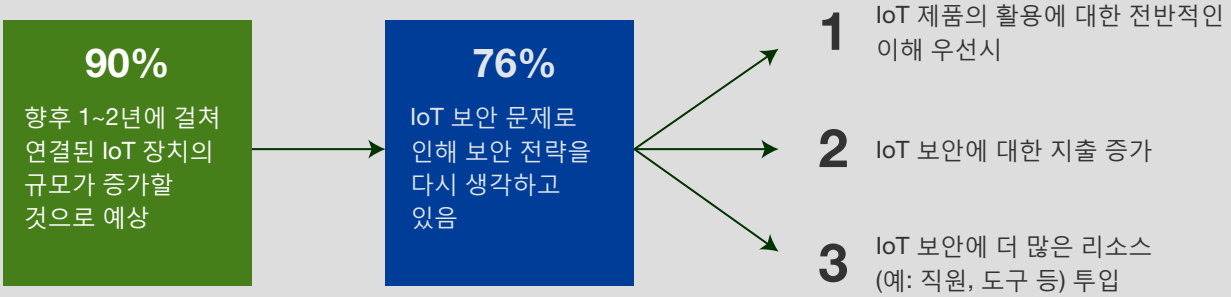
이러한 보안 과제들은 대부분의 조직들이 이들을 관리할 준비가 제대로 되어 있지 않다는 것에 문제가 있습니다. 보안 팀은 항상 해 오던 방식으로 보안을 수행하는 것에 아주 익숙해져 있지만, 그런 기술과 프로세스가 필요한 보안을 제공하지 못 한다는 것도 알고 있습니다. 결과적으로, 76%의 기업이 IoT 보안 문제 때문에 IT 및 사업 부서의 보안 전략을 재고해야 한다고 말합니다(그림 1 참조). 이러한 전략 개편에는 다음이 포함됩니다.

- IoT 제품의 활용에 대한 전반적인 이해 우선시.
- IoT 보안에 대한 지출 증가.
- IoT 보안에 더 많은 리소스(예: 직원, 도구 등) 투입.

기업의 77%는 IoT 장치의 사용 증가가 심각한 보안 문제를 야기한다는 것에 동의합니다.

그림 1

IoT 성장으로 기업은 보안 전략을 조정해야 합니다.



조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

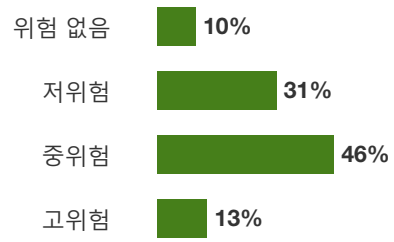
위험 감수성향이 너무 높습니다.

59%의 기업은 IoT 보안 준수와 관련하여 중/고위험을 감수할 용의가 있다고 말합니다. 이는 IoT 보안 위협에 대해 기업들이 얼마나 잘못 이해하고 있는지에 대해 경각심을 일깨워 줍니다(그림 2 참조). 기업들이 IoT에 대해 이러한 수준의 위험을 기꺼이 받아들이려 한다는 사실은, 문제에 대한 이해가 놀라울 정도로 부족함을 보여주고 있으며, 미래의 다양한 사이버 공격의 토대를 제공하게 됩니다. IoT와 관련된 높은 위험을 용인하는 것은 대부분의 운송수단이 기계적 문제를 가지고 있음을 알면서도 최상의 결과가 나올 것으로 기대하는 운송 회사와 같습니다.

위험 수준에 대한 반응이 충격적이어서, 드러난 것 외에 다른 것이 있을 수도 있습니다. 77%의 기업이 IoT가 심각한 보안 문제를 야기한다고 말하고 있는 맥락상에서 이러한 위험 감수성향을 놓고 볼때, 기업의 "감수성향"은, 괜찮다고 생각해서라기보다는, 통제할 능력이 없기 때문인 것처럼 보입니다. 기업의 44%가 예산 제약을 IoT 보안 향상에 있어서 가장 큰 장애물이라고 생각한다는 점도 문제의 일부입니다. 기업이 급증하는 IoT 장치 및 관련 규정 준수 요구 사항을 처리하는 데 어려움을 겪고 있기 때문에, 보안 예산은 급증하는 속도와 같은 속도로 증가해야 합니다. 그렇지 않으면, 기업이 준비가 부족하여 더 높은 수준의 위험을 수용할 수 밖에 없게 됩니다.

그림 2

"IoT 보안 규제 요건과 관련하여 회사가 용인할 수 있는 보안 위험은 어느 정도입니까?"



조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

IOT 보안은 보안 전문가에게 불안감을 줍니다.

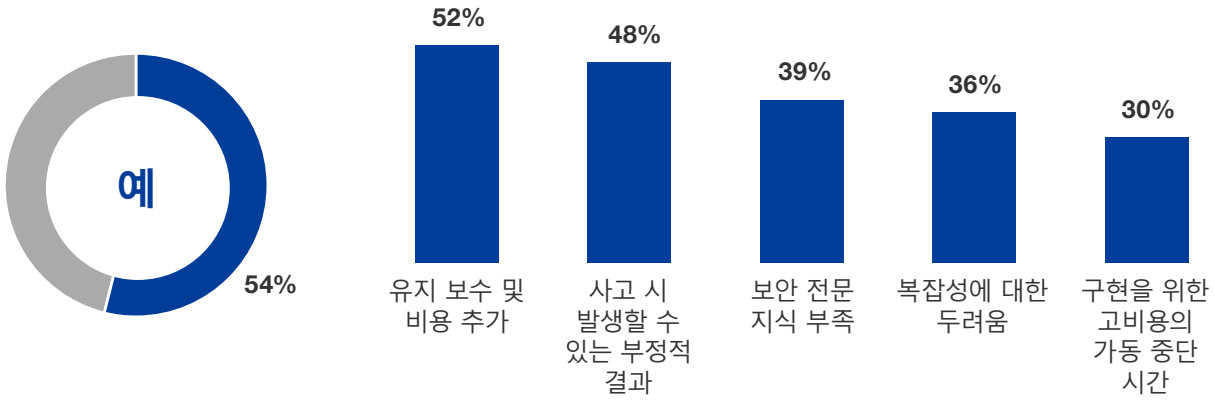
많은 보안 리더들이 받아들여야 하는 위험을 감안할 때, 54%가 IoT 보안이 그들에게 불안감을 안겨 준다고 말하는 것은 그리 놀라운 일이 아닙니다. 그러나, 기업들이 당면한 어려움을 봤을때, 우리는 이 수치가 더 높을 것으로 기대했습니다. 보안 리더들은 통제할 수 없는 것에 대해서는 우려할 필요가 없다고 보기 때문에 아마 수치가 더 높지 않았을 겁니다. 사업 부서의 보안 의사결정권자가 IoT 보안에 대해 우려하는 비율(58%)이 IT 보안 담당자(51%)에 비해 높은 것으로 나타났습니다. 이는 IoT 보안에 접근하는 방법이 연결되지 않고 끊겨 있거나 실패했다는 것을 보여줍니다. 기술적으로 문제를 해결해야 하는 IT 팀이 IoT에 대해 동일한 우려를 나타내지 않는다면, LoB 리더가 필요로 하는, 장치 안전에 대한 확신을 얻는 것은 어려울 겁니다. IoT에 대한 불안감은 세 가지 주요 원인에 의해 발생합니다(그림 3 참조).

- **관리에 드는 비용과 시간.** IoT는 네트워크 상의 접촉면을 기하급수적으로 늘리므로, 보안 전문가가 적절히 관리하는 데 훨씬 더 많은 시간을 필요로 합니다. 또한 상대적으로 새로운 것이기 때문에 어떻게 관리해야 하는지 정확히 아는 것이 다른 보안 절차만큼 간단하지 않습니다.
- **보안 위반으로 인한 잠재적인 부정적 영향.** 네트워크 상에서 한 장치의 보안 실패는 전체 네트워크를 위태롭게 할 수 있습니다.
- **보안 기술의 부족.** IoT를 관리하기 어렵다면, 보안을 유지하는 것 또한 어렵습니다. 신기술은 많은 보안 팀이 해결 방법을 제대로 훈련받지 못한 새로운 보안 요구 사항들을 발생시킵니다.

IoT와 관련된 높은 위험을 용인하는 것은 대부분의 운송수단이 기계적 문제를 가지고 있음을 알면서도 최상의 결과가 나올 것으로 기대하는 운송 회사와 같습니다.

그림 3

"IoT 보안이 귀하에게 불안감을 주나요? 왜 그런가요?*"



조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
*조사 기반: IoT 보안이 불안감을 주고 있다고 답변한 IT 및 비즈니스 의사 결정권자 327명.
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

IT와 비즈니스 리더는 IoT 보안 관리에 대한 생각이 다릅니다

IT와 사업 부서는 IoT 장치와 보안을 구성 및 관리하는 방법에 대해 인식차가 있습니다. 일부에서는 개별 사업 부서가 자신의 보안을 책임져야 한다고 생각하고, 다른 일부에서는 다른 누군가가 책임을 져야 한다고 생각합니다. 기업 IT 네트워크에서 누가 IoT 장치의 보안에 주로 책임을 지는지 묻는 질문에, IT 응답자의 44%는 SOC를 언급했지만, LoB는 일반적으로 자신을 주요 책임자라고 밝혔습니다. 반대로, IT 응답자의 45%는 LoB가 기본 장치 구성을 담당해야 한다고 생각하고, 46%의 LoB 응답자는 IT가 담당해야 한다고 생각합니다. 여기에서 두 가지의 시나리오가 생성됩니다. 1) 회사 전체를 아우르는 가용성이 제한되어 있는 사일로(IT는 IT가, LoB는 LoB가)에서 IoT 보안을 관리하는 환경, 또는 2) 다른 사람이 책임지기를 모두가 기대하는 환경(그림 4 참조). 회사가 어떤 결과를 마주하고 있는지에 관계 없이, 장치가 없어지거나 부적절하게 구성되면 보안 과실이 발생할 수 있습니다.

기업이 IoT 보안을 관리하는 방법을 고려할 때, 대부분의 기업들은 기존 지식을 고수하며, 보안 운영 센터와 같은 IT의 범주 내에 보안을 두려고 합니다. 이러한 접근 방식이 대개 동작하기는 하지만, 일반적으로 조직에서 이미 어떤 장치가 있는지 파악하고 있는 경우에 한해서 입니다. 모든 SOC가 장치를 관리하거나 지원할 수 있지만, 자산 관리자, LoB 팀 및 장치를 연결시키는 네트워크 팀과 조정하고 협업하는 것 또한 아주 중요합니다. 다음 두 가지 이유에서 입니다.

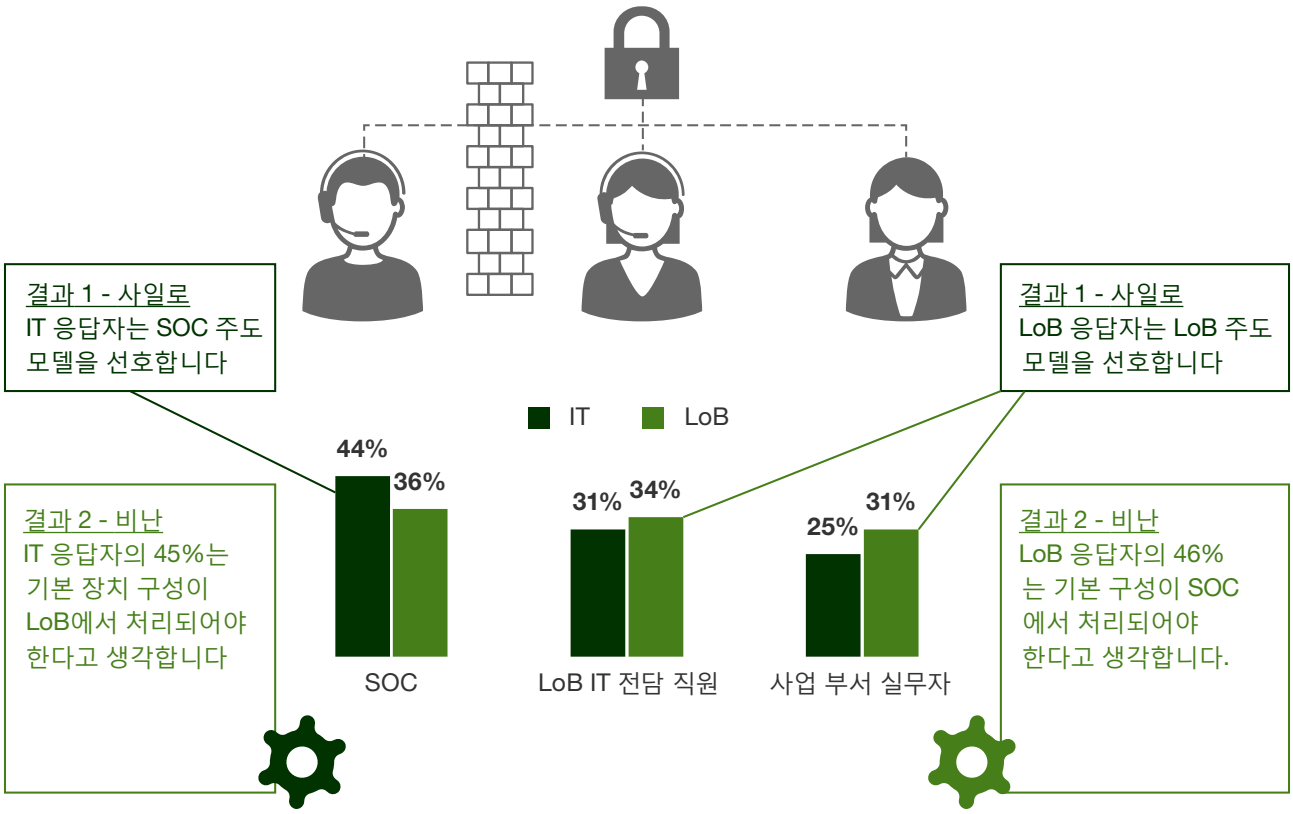
- **기본 보안 구성 관리.** 50%의 기업은 IoT 장치의 기본 구성을 SOC에서 처리해야 한다고 말합니다. 그러나, 직위별로 분류해 보면, LoB 응답자의 54%는 기본 구성이 LoB 직원 또는 장치 제조업체에 의해 관리되어야 한다고 생각합니다. 이 결과는, LoB 사용자들이 IoT 보안 요구 사항에 대한 지위 통제 지점으로서 SOC를 활용할 필요조차 느끼지 않으면서, 모든 적절한 제어가 갖춰져 있다는 가정 하에서 장치를 배치하고 있음을 보여줍니다. 또한, IT 응답자의 45%는 LOB가 이런 생각을 보유하고 있다고 생각하기 때문에, 함께 일할 동기 부여가 되지 않습니다.
- **네트워크 상에서 장치의 적절한 가시성 확보.** SOC가 장치 설정 중에 자산 관리자 및 LoB 팀과 함께 적극적으로 관여하지 않는 한, 연결된 장치의 수를 정확히 알기는 어렵습니다. 네트워크 상에서 한 장치의 보안 실패는 전체 네트워크를 위태롭게 할 수 있기 때문에, SOC는 100%의 가시성을 확보해야 합니다.

자신에게 물어 보십시오.

귀사의 SOC 또는 사업 부서 팀은 IoT 구성 및 보안 관리를 담당할 사람이 누구라고 이야기합니까?

그림 4

네트워크 상에서 IoT 장치를 안전하게 유지할 책임이 누구에게 있는지에 대한 혼란은 두 가지 결과를 가져옵니다



조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

보안에 대한 안일함은 문제를 발생시킬 수 있습니다

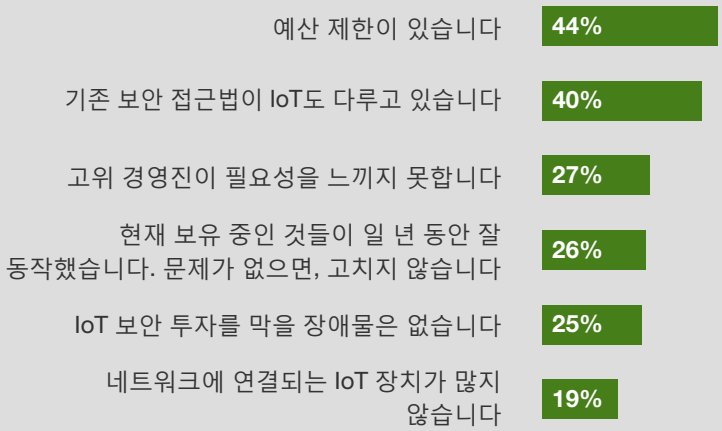
IoT 보안이 중요한 도전이자 문제임을 알기에, 우리는 IoT 보안의 개선을 방해하는 주요 장애물을 밝혀달라고 응답자에게 요청했습니다. IT 및 LOB 응답자들은 유사한 문제들을 지적했으며, IoT 보안에 병렬적으로 접근(비효율적인 경우)하고 있음을 보여주었습니다. 간단히 말해서, 두 그룹 모두 동시에 같은 방식으로 어려움을 겪고 있는 것처럼 보입니다. 가장 많이 나온 응답은 다음과 같습니다(그림 5 참조).

- **전통적인 보안 접근법이 IoT를 다룰 수 있다는 믿음.** 보안 팀은 수년간 기존 시스템의 보안을 담당해 왔습니다. IoT에 기존과 똑같은 방법을 적용하는 것이 쉬울 거라고 믿고 있습니다. 그러나, 상대적으로 테스트가 부족하거나 확인되지 않은 신기술에 대해 작업할 때는 "문제가 없으면, 고치지 않습니다"라는 생각은 적용될 수 없습니다.
- **고위 경영진의 지원 부족.** 현재의 방법이 충분하다는 믿음때문에, 많은 고위 경영진들은 새로운 도구나 인력에 대한 투자를 정당화시키기 어려울 수 있습니다. 불행히도, 사고가 발생해서 주의를 끌게 될 수도 있지만, 그때는 너무 늦습니다.
- **예산 제한.** 기업의 44%가 예산을 주요 장애물로 꼽았습니다. 예산 부족은, 기업이 적절한 기술 습득을 위해 필요한 고용과 IoT 보안 관리에 적합한 도구를 구입할 수 있는 능력에 영향을 끼칩니다(각각 기업의 31%, 25%가 문제점으로 응답). 이것은 유지 보수 및 비용이 IoT 보안을 둘러싼 불안감의 가장 일반적인 원인이 되는 이유를 설명하는 데에도 도움이 됩니다. 조직은, 예산이 증액되는 경우에도, IoT 장치의 증가에 비례하여 IoT 보안 예산 증액이 되도록 보장해야 합니다. 현재의 보안이 적절하다는 잘못된 신념과 경영진의 지원에 어려움을 겪고있는 상황에서, 필요한 예산을 확보하는 것은 힘든 싸움일 수 있습니다.

불행히도, 사고가 발생해서 일부 고위 경영진의 주의를 끌게 될 수도 있습니다. 그때는 너무 늦습니다.

그림 5

"귀사가 IoT 보안에 더 많은 투자를 하지 못 하게 하는 가장 큰 장애물은 무엇입니까?"



조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

조직은, 예산이 증액되는 경우에도, IoT 장치의 증가에 비례하여 IoT 보안 예산 증액이 되도록 보장해야 합니다.

FORRESTER®

기업은 IOT에 대해 완전한 보안 자신감이 부족합니다

많은 기업들이 현재의 보안 정책이 IoT를 다루는 데 충분하다고 믿고 있기 때문에, 현재의 IoT 보안에 대한 자신감을 평가해달라고 요청했습니다. 10이 완전한 자신감을 나타내는 1~10 범위의 척도에서, 대부분의 응답은 긍정적이었고, 70%는 8-10 범위 내에 있었습니다. 하지만, IoT 네트워크의 보안에 대해 중간에서 낮은 자신감을 갖고 있는 30%의 기업이 아직 있습니다. 특히 13%만이 10(완전한 자신감)으로 평가했습니다. 위태로운 상황과 보안 사고의 잠재적 파급 효과를 고려했을 때, 기업의 87%가 IoT 보안에 대한 완전한 자신감을 갖고 있지 않다는 사실은 다소 우려스럽습니다.

87%의 기업은 현재 IoT 보안에 대해 완전한 자신감이 없습니다.

이 점을 더 깊이 생각해 보면서, 우리는 다음과 같은 가설적인 질문을 던졌습니다.

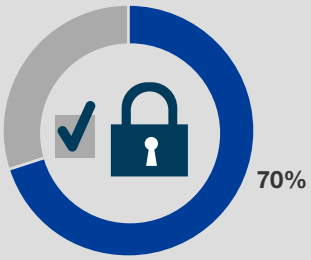
"만약 귀사가 감사를 받고, 귀사가 사용하고 있는 모든 IoT 커넥티드 장치와 솔루션을 식별하라고 요청 받는다면, 귀사가 사용 중인 IoT 커넥티드 장치와 솔루션을 100%를 정확하게 식별할 수있는 능력에 대해 얼마나 자신 있습니까?"

보안 자신감에 대한 결과와 마찬가지로, 대부분의 응답은 8 또는 9에 있었지만, 18%만이 완전한 자신감을 갖고 있었습니다. 기업의 82%가 네트워크에 있는 모든 장치를 인지하고 있다고 완전히 자신하지 못한다면 이것은 큰 문제입니다(그림 6 참조). 기업들이 현재 속해 있는 네트워크 및 보안 세계는 규정 준수에 의해 움직이고 감사에 초점을 맞추고 있습니다. 저희 연구에 따르면, 대부분의 조직이 IoT 통제에 초점을 맞춘 규정 준수 감사를 적절히 통과할 수 있다고 생각하지만, 사실 100% 확실하지 않다라는 것을 알고 있었습니다. 이것은 많은 기업들에게 네트워크 침입의 중요한 수단이 될 수도 있는 잠재적 실패 지점을 잘 보여줍니다.

현재의 IoT 보안에 대한 만족도는 높지만, 제대로 테스트될 때에는 견디지 못합니다.

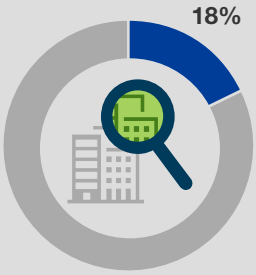
그림 6

"귀사의 IoT 네트워크가 안전하다는 것에 대해 얼마나 확신하십니까?"



70% 높은 확신

"감사를 받는다면, 사용 중인 IoT 연결 장치 또는 솔루션의 100% 식별 능력에 대해 얼마나 확신하십니까?"



18% 완전한 확신

조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

FORRESTER®

IoT 보안은 IoT 가시성에서 시작됩니다

우리는, IoT의 성장에 부응하기 위해 네트워크 보안 전략을 재정의하기 시작할 때, 점점 커지는 문제들을 해결하기 위해 기업이 취하는 네 가지 주요 단계를 확인했습니다(그림 7 참조).

- **IoT 장치에 대한 인식 및 가시성 향상.** 네트워크 상에 어떤 장치가 있는지 이해하는 것은 장치의 보안에 있어서 중요한 첫 번째 단계입니다. 볼 수 없는 것을 보호할 수는 없기 때문에: 이 항목이 가장 일반적인 단계로 됩니다(48%).
- **규제 준수 강화.** 현재 많은 기업들이 IoT 보안 규정 준수에서 중위험에서 고위험을 용인하고 있지만, 이것은 선택에 의한 것이 아닙니다. 네트워크 가시성을 높이기 위한 노력과 함께, 규정 준수를 반복하여 강조하면, 보안 리더가 감사 시 더욱 자신감을 갖게 하고, 위험 감수성향을 낮추게 합니다.
- **IoT 장치의 관리 및 구현 중앙 집중화.** 대부분의 기업이 현재 SOC 또는 IT 통제 하에서 중앙에서 장치를 관리하고 있지만, 누가 초기 구성 및 구현을 담당하는 지는 여전히 별도의 문제로 존재합니다. IoT 장치의 구현과 관리 모두를 중앙 집중화함으로써, 기업은 보다 일관된 구성과 새로운 장치에 대한 인지를 높일 수 있고, IT 및 LoB 팀 간의 보안 소유에 대한 혼란을 줄일 수 있습니다.
- **도구 및 전문 지식을 제공하는 IoT 보안 파트너 찾기.** 기업이 IoT 보안에 더 많은 투자를 함에 따라, 기술 격차를 메우고 적절한 도구를 갖추도록 도울 수 있는 파트너를 필요로 하게 됩니다. 차세대 IoT 보안 솔루션을 고려할 때 가장 중요한 기준을 묻는 질문에 대한 가장 많은 응답은 다음과 같습니다. 1) 솔루션은 기존 보안 시스템과 통합되어야 하며, 2) 구현이 쉬어야 함. 기업은 전체 보안 솔루션을 완전히 개편하지 않고도, 보안 기능을 원활하게 향상시킬 수 있는 파트너를 원합니다.

이러한 다음 단계들을 지원하기 위해, 기업의 82%는 향후 1~2 년 동안 IoT 보안에 대한 지출이 증가할 것으로 예상합니다. 이론적으로, IoT에 쓰이는 상대적인 지출은 전통적인 보안 개선 에 대비하여 IoT 장치의 성장을 반영해야 합니다. 그러나, 응답자의 40%가 IoT에 대해 전통적인 보안 조치만으로도 충분하다고 생각하는 상황에서, 이는 힘든 설득 작업이 될 수 있습니다. 따라서, 보안 팀이 IoT 환경의 보안이 갖는 중요성과 이를 수행하지 않을 때의 위험을 경영진 에 보여주는 것이 그 어느 때보다 중요해지고 있습니다. 고위 경영진에게 IoT 보안의 중요성과 가치를 보여줌으로써, 보안 팀은 IoT 환경을 적절하게 보호하는 데 필요한 자금 및 리소스를 할당받을 수 있습니다. 자금 증액과 가시성 및 규정 준수에 중점을 둔 새로운 보안 전략을 통해, 기업은 IoT에 대한 불안감을 줄이고 네트워크가 안전하다는 자신감을 회복할 수 있습니다.

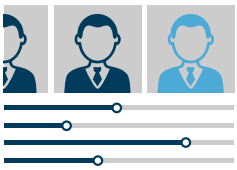
그림 7

"조직에서 IoT 보안을 향상시키기 위해 취하는 조치는 무엇입니까?"

인식 및 가시성 향상

규제 준수 강화

IoT 보안 관리의 중앙 집중화



올바른 도구와 전문 지식을 갖춘 파트너 찾기

조사 기반: 조직 내 네트워크 및 데이터 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

48%의 기업은 IoT 보안 향상을 위한 중요한 다음 단계로 IoT 장치에 대한 인지와 가시성 개선을 꼽았습니다.

FORRESTER®

주요 권장 사항

오늘날의 기업은 지속적이고 끊임없이 확장되는 연결의 세계에 직면해 있습니다. 매일, 기업의 성장과 번영을 위한 중요한 이점을 제공할 수 있는 새로운 장치와 기능이 온라인으로 제공됩니다. 그러나, 이런 장치 및 기술이 방치되고 사라진다면, 네트워크 침입과 궁극적으로는 조직의 중단까지 초래할 수 있는 시작점이 될 겁니다. IoT 가용 시스템을 보다 효과적으로 보호하려면, 기업에서는 다음을 수행하는 것이 좋습니다.

너 자신을 알라. 명확한 보안 전략 없이는, 귀사는 보안 불안감과 어려움에 계속 직면하게 될 것입니다. 자신에게 다음 질문을 하고 정직하게 대답하십시오.

- **진정으로 내 네트워크에 대한 완전한 가시성을 갖고 있는가? 어떤 수준의 위험을 수용할 의향이 있는가?** 네트워크에 접속하는 모든 장치에 대한 포괄적 지식과 제어가 없다면, 알려져 있는 장치를 기반으로 하는 감사는 통과할 수 있다고 하더라도 해당 네트워크는 안전하지 않습니다.
- **누가 새 장치의 구성과 구현을 책임지는가?** 귀사의 보안 팀과 네트워크 팀이 협력하여 IoT 구현 및 보안 프로토콜을 조정하고 총체적인 장치 감시를 가능하게 하는 것은 필수적입니다.
- **할 수 있는가? 해야 하는가?** 새로운 장치 나 기술이 팀의 솔루션으로 또는 "필요"에 의해 제공될 때마다 이 질문을 하십시오. 무선으로 작동되는 토스터를 사용할 수 있습니까? 물론입니다. 당신 개인의 편의를 위해 불필요한 위협 요소를 네트워크에 도입해야 합니까? 아마도 아닐겁니다.

표준을 넘어 서십시오. 규정 준수 표준 또는 감사 의무를 충족시키는 것은 단지 가진 역량의 최하위 수준을 달성하는 것입니다. 이는 실패하는 것보다 조금 나은 수준입니다. 팀은 이러한 기준선을 넘어서고, 비즈니스에 이익이 되는 새로운 기술을 안전하게 채택하면서 혁신과 최적화를 이끄는 계획과 전략으로 나아가야 합니다.

기술은 기술로 다투십시오. 인간이 오늘날 널리 보급된 네트워크 커넥티드 장치의 성장과 다양성에 뒤쳐지지 않게 따라가는 것은 불가능합니다. IoT 보안 및 계정에 관한 문제를 해결할 수 있는 기회를 조금이라도 잡으려 한다면, IoT 보안 컨트롤의 특성에 초점을 맞춘 전용 기술 솔루션을 활용해야 합니다. 기술 실패에 맞서기 위해 기술을 사용하고, 보안 및 LoB 팀이 IoT의 불규칙적인 배포를 해결하기 위해 노력할 수 있도록 권한을 부여하십시오.

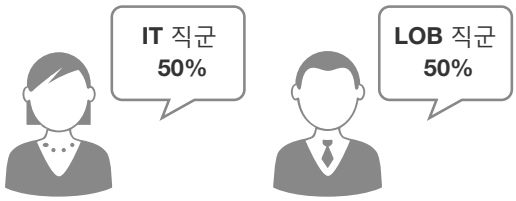
FORRESTER®

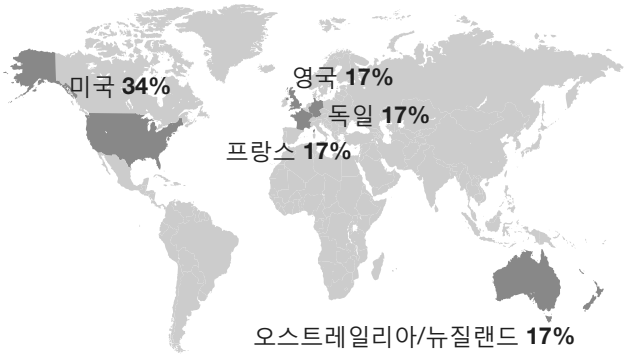
부록 A: 조사 방법

본 조사에서 Forrester는 조직 내 네트워크 및 데이터 보안/엔드포인트 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명과 인터뷰를 진행했습니다. 참가자들에게 제공된 질문은 IoT 보안 문제와 네트워크 상의 장치에 대한 전반적인 인식에 대해 물었습니다. 미국, 영국, 독일, 프랑스, 오스트레일리아/뉴질랜드의 종업원 수 2,500명 이상의 기업이 설문에 참여했습니다. 시간을 들여 참여해 준 것에 대한 감사의 표시로 응답자들에게 소정의 혜택을 드렸습니다. 이 조사는 2017년 8월에 완료되었습니다.

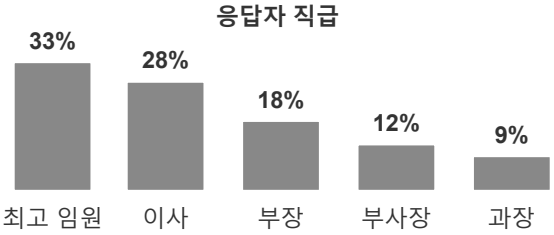
부록 B: 인구 집단/데이터

응답자 인구 집단:

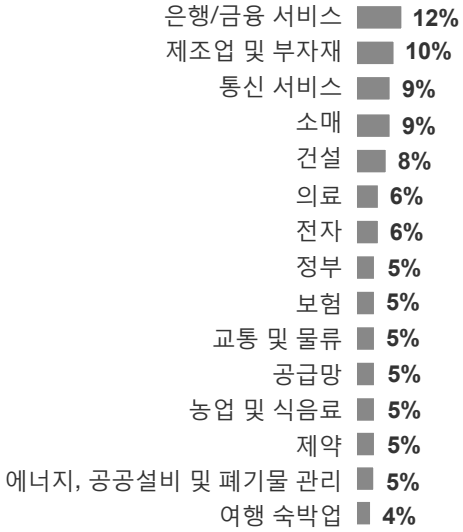




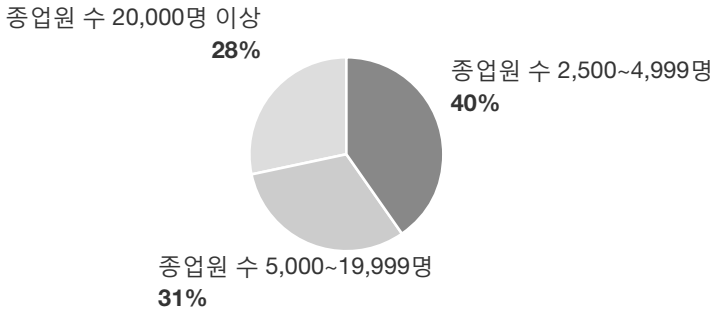
응답자 직급



업종



회사 규모



조사 기반: 조직 내 네트워크 및 데이터 보안 / 엔드포인트 보안 프로세스에 관여하는 IT 및 비즈니스 의사결정권자 603명.
출처: Forrester Consulting이 ForeScout의 의뢰로 2017년 8월에 실시한 조사

FORRESTER®