

# IT, 데이터 및 인쇄 보안 공격의 위협 완화:

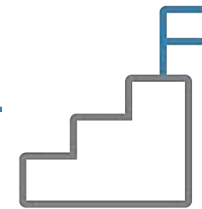
---

기업이 IT 보안 회복 탄력성을  
강화하는 방법

# 성공을 위한 혁신: 비즈니스를 위한 디지털 트랜스포메이션

후지필름비즈니스이노베이션은 위기를 넘어 혁신으로: 비즈니스 회복 탄력성을 활용한 경쟁 우위 확보' 보고서에서 급변하는 환경에서 기업이 회복 탄력성을 유지하여 조직을 강화하고 성공하는 방법을 제시한 바 있습니다. 명확하고 효율적인 워크플로 프로세스 및 인력 구성을 갖춘 기업들은 위기가 발생했을 때 더 높은 회복 탄력성을 발휘했습니다.

전 세계 기업들은 2023년부터 2027년까지 자사 조직의 대 전환을 추진하는데 있어서 다음과 같은 트렌드를 예상할 수 있습니다.



일찌감치 디지털 트랜스포메이션을 적극 수용한 기업들은 이러한 과정을 더디게 진행한 경쟁사 대비 **5배 이상 높은 성장률**을 보였습니다.<sup>1</sup>




## 이제는 민첩성이 생명입니다.

대기업이든 중소기업이든 관계없이 회복 탄력성이 높고 전략적인 기업들은 디지털 트랜스포메이션을 통해 자사 하이브리드 및 원격 팀의 역량을 강화하고 비즈니스 성공을 보장하고 사회적 책임을 강화하는 능력을 보여왔습니다.


다른 많은 기업들도 이를 따라잡기 위해 노력하고 있으며 그 중 일부는 다른 기업보다 더 나은 성과를 보이고 있습니다. 오늘날의 비즈니스 환경은 이러한 후발주자들도 기술 도입과 혁신 문화를 선도하는 기업들과의 격차를 따라잡을 수 있는 기회를 제공합니다. 이러한 후발주자들은 앞서 가는 기업들로부터 얻은 교훈을 활용하여 자사의 디지털화 및 성장을 촉진합니다.

회복 탄력성과 올바른 조직 문화 마인드셋을 구축하려는 노력의 일환으로서의 장기적 디지털 트랜스포메이션이란 커넥티드 워크스페이스를 구축하고 하이브리드 및 원격 팀의 협업을 강화하며 비즈니스 워크플로 자동화를 통한 미래의 직무를 구상하고 자사 인력의 기술 역량을 키워 혁신에 대비하도록 하는 활동을 의미합니다.

이번 시리즈를 통해 더 많은 인사이트를 발견하세요.

<p style="text-align: center;"><b>1</b></p>  <p style="text-align: center;"><b>미래 인력: 보다 스마트한 팀 생산성을 위한 워크플로 간소화</b></p>	<p style="text-align: center;"><b>2</b></p>  <p style="text-align: center;"><b>IT, 데이터 및 인쇄 보안 공격의 위협 완화: 기업이 IT 보안 회복 탄력성을 강화하는 방법</b></p>	<p style="text-align: center;"><b>3</b></p>  <p style="text-align: center;"><b>디지털 시대에 성공하기 위한 워크플레이스 혁신: 워크플레이스 혁신을 위한 트렌드 및 전략</b></p>
---	--	--

디지털 트랜스포메이션을 통해 업무 속도와 생산성을 향상시키고 비즈니스 성공을 실현하세요.



기대치를  
상회한 기업들은  
혁신 수용에 가장 더딘  
기업들보다 **4배 이상 빠른**  
성장률<sup>2</sup>을 기록했습니다.  
이는 선도 기업들의  
성장률보다도 높은 것으로,  
수익성에서 손해를  
보지 않고도 디지털  
트랜스포메이션을  
실현할 수 있음을 증명합니다.

# 목차

05

IT 보안: 아태 지역 기업들 사이에서 증가하는 우려

08

아태 지역 기업들이 직면한 주요 IT 보안 과제

19

IT 전략 수립을 위한 체크리스트

22

후지필름비즈니스이노베이션과 함께 성공하기

26

참고 자료

07

아태 지역의 보안 위협 환경에 대한 인사이트

13

IT 위협으로부터 조직 보호하기

21

최우선 비즈니스 과제인 IT 네트워크 보안

24

후지필름비즈니스이노베이션과 함께  
디지털 트랜스포메이션 여정을 위한 역량 강화하기

# IT 보안: 아태 지역 기업들 사이에서 증가하는 우려

무단 액세스로부터 컴퓨터, 네트워크 및 데이터를 비롯한 조직의 자산을 보호하는 사이버보안 전략을 포함하는 IT 보안의 강화가 아태 지역 기업들의 최대 관심사로 떠오르고 있습니다.

사이버 위협 환경은 빠르게 진화하고 있으며 이러한 공격의 피해는 점점 더 커지고 있습니다. 이러한 공격에 노출된 기업은 금전적 손실 외에도 데이터 손실, 평판 훼손, 업무 중단과 같은 손실을 감수해야 합니다.



## 이러한 트렌드는 아태 지역의 기업들이 자사의 IT 보안 역량을 강화해야 하는 노력의 시급성을 보여줍니다.

기업은 효과적인 보안 전략이 필요합니다. 하지만 이러한 전략의 수립은 목적지가 아닌 하나의 여정입니다. IT 보안이라고 하면 대규모 솔루션이 요구되는 계획으로 생각하기 쉽지만 사실 작은 변화들도 귀사의 보안 태세를 강화하는 데 도움이 될 수 있습니다.

이번 가이드에서는 아태 지역의 보안 위협 환경과 기업들이 직면한 주요 IT 보안 과제에 대해 살펴봄으로써 기업들이 자사의 기존 전략에서 보완할 점을 식별하여 IT 보안을 개선하는 데 필요한 솔루션을 구현할 수 있도록 도움 예정입니다.



아태 지역은 전 세계에서 발생하고 수습된 모든 사이버보안 사고의 31%를 차지하는 등 전 세계에서 사이버 위협 발생 건수가 가장 높은 지역입니다.<sup>3</sup>

2023년 1분기에 아태 지역은 주간 사이버 공격 건수에서 전 세계에서 가장 높은 전년대비 증가율(주당 1,835 건)을 기록했습니다.

이는 전 세계 평균(주당 1,248 건)보다 무려 47%나 더 높은 수치입니다.<sup>4</sup>



# 아태 지역의 보안 위협 환경에 대한 인사이트



가장 많이 발생한 사이버 공격 유형은 백도어 프로그램 배포였고, 랜섬웨어와 MalDoc이 그 뒤를 이었습니다.<sup>5</sup>

말레이시아와 필리핀의 기업들은 아태 지역에서 가장 많은 보안 사고를 경험했습니다.<sup>6</sup>



호주의 기업들은 사고 대응 계획을 운영할 가능성이 가장 적었고, 반대로 홍콩의 기업들은 그러한 가능성이 가장 높았습니다.<sup>7</sup>



싱가포르의 기업들은 가장 큰 우려 사항으로 비즈니스 중단을 꼽았습니다.<sup>8</sup>



기업이 IT 보안 사고에  
대응하여 실시한 상위  
5개 조치<sup>9</sup>

68% 정기 훈련 또는 모의 훈련 실시

64% 사고 대응 플레이북, 계획 또는 정책의 실행

62% 사이버 침해 복구 계획의 운영

62% 데이터 보안 책임자 임명

62% 외부 사이버보안 전문가 이용



# 아태 지역 기업들이 직면한 주요 IT 보안 과제

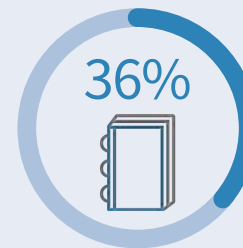
IT 보안 과제를 이해함으로써 회사의 운영 중단, 매출 손실, 데이터 도난 사고 등을 방지할 수 있습니다.

기업은 IT 보안의 모든 측면을 포괄하는 조직 전략에 투자해야 합니다.

중요한 과제들을 심층적으로 이해하여 귀사의 IT 보안 프로세스에서 보완해야 할 점을 식별하고 해결할 수 있습니다.

## 비즈니스 우선 사항과 IT 보안 우선 사항 간 불일치 극복

최고정보책임자(CIO)와 경영진의 비즈니스 목표가 일치하지 않는 경우 효과적인 보안 조치를 실행하는 데 방해가 될 수 있습니다. 이러한 목표의 불일치는 불충분한 IT 보안 투자로 이어집니다.



2022년에 아태 지역 기업의 36%는 사고 대응 플레이북, 계획 또는 정책을 운영하지 않았습니다.



38%는 데이터 보안 책임자를 임명하거나 외부 사이버보안 전문가를 이용하지 않았습니다.<sup>10</sup>



57%는 자사의 IT 보안이 사이버 공격자들의 새로운 전략에 맞설 수 있을 만큼 충분히 강력한지 확신하지 못했습니다.<sup>11</sup>



## 직원을 위한 데이터 보안 교육

클라우드 데이터 침해 사고를 가장 많이 일으키는 원인은 사람의 실수입니다.<sup>12</sup> 다양한 요인이 사람의 실수에 영향을 미치는데, 대표적으로 기회, 환경 및 인식 부족이 있습니다.<sup>13</sup>

데이터 침해로 이어지는 사람의 실수의 예로는 감염된 소프트웨어 다운로드, 취약한 비밀번호 사용, 부적절한 IT 주소 관리 등이 있습니다.

### 사람의 실수에 영향을 미치는 요인:

#### 기회

실수가 발생할 기회가 많을 수록 실제로 발생하는 실수의 수도 증가합니다.



#### 환경

워크플레이스의 물리적 환경과 직장 문화는 사람의 실수에 영향을 미칩니다. 직원들이 어떤 조치를 취해야 할지 알더라도 제대로 이행하지 못하는 경우도 있습니다.



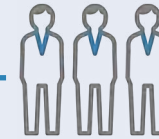
#### 인식 부족

사용자가 어떤 조치를 취해야 하는지 모를 수도 있습니다.



## IT 보안 인력난 해결

2022년에 전 세계 사이버보안 부족 인력은 26.2% 증가한 342만 명을 기록했습니다.<sup>14</sup>



아태 지역의 사이버보안 부족 인력은 216만 명으로, 전 세계에서 가장 심각한 인력난에 직면해 있습니다.<sup>15</sup>

이러한 인력난의 원인으로는 IT 보안 교육에 초점을 맞춘 대학 교육 과정의 부재<sup>16</sup>, 보안 산업에 대한 오해, 너무도 빠른 기술 발전 속도 등을 들 수 있습니다.<sup>17</sup>

이러한 인력난을 고려하면 민감한 데이터 및 디지털 자산을 보호할 수 있는 더 나은 방법을 찾는 것은 더욱 중요합니다.

## 클라우드 도입에 따른 보안 과제 해결

아태 지역의 클라우드 도입은 기업들이 자사의 IT 니즈를 해결하기 위해 클라우드로 관심을 돌리면서 빠르게 증가하고 있습니다.

하지만 클라우드 컴퓨팅으로의 전환은 복잡한 프로세스이며, 처음부터 바로 보안을 통합하는 것이 매우 중요합니다. 효과적인 클라우드 마이그레이션 전략 없이는 데이터 침해, 데이터 손실 및 클라우드 구성 오류의 위험에 놓일 수 있습니다.

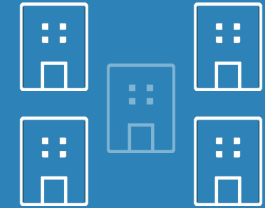
## 아태 지역의 클라우드 도입 현황



아태 지역 기업들의 클라우드 지출액은 2024년까지 2,000억 달러에 도달할 것으로 전망됩니다.<sup>18</sup>

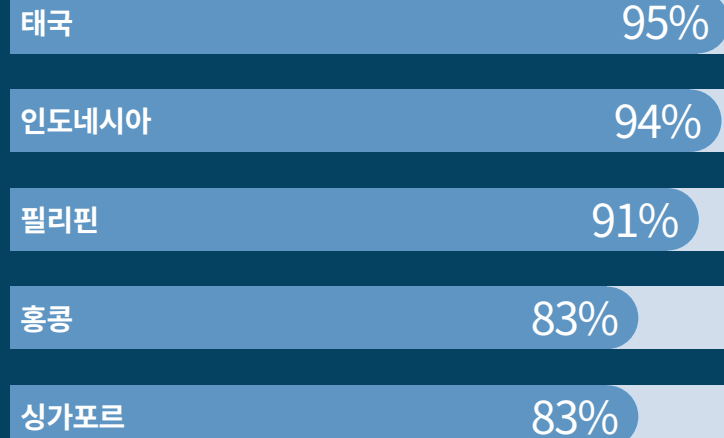


클라우드 서비스를 이미 이용 중인 기업도 자사의 클라우드 투자를 늘릴 것으로 전망됩니다.



아시아 기업 다섯 곳 중 네 곳(84%)은 2024년까지 전면적인 클라우드 마이그레이션을 계획하고 있습니다.

클라우드 투자가 증가할 것으로 가장 많이 예상되는 국가는 다음과 같습니다.<sup>19</sup>



## 네트워크 복호화에 대비

기업들이 자사의 데이터 및 컴퓨팅을 클라우드로 이전하면서 보안팀은 암호화된 트래픽을 통해 자사의 디지털 발자국을 보호해야만 합니다.

하지만 사이버 공격자들은 암호화된 메시지, 비밀번호 및 키를 복호화하거나 노출시켜 민감한 정보를 드러내고 시스템을 위태롭게 만들 수 있습니다.

양자 컴퓨팅이 개발되고 있는 상황에서 이러한 중요한 정보가 악의적인 사람의 수중에 들어가는 것은 기업에 상당한 위협이 될 수 있습니다.



2023년에 아태 지역 기업들이 직면한 주요 네트워크 보안 과제 중 하나는 양자 컴퓨팅 보안 위협인 네트워크 복호화입니다.

아태 지역 기업의 약 60%는 양자 컴퓨팅 보안 위협과 관련한 가장 큰 우려 사항으로 네트워크 복호화를 꼽았습니다.<sup>20</sup>



## 디지털 공간의 보호

커넥티드 디바이스 수가 계속 늘어나면서 기업들이 이러한 장치들을 위협으로부터 보호하는 것이 갈수록 더 어려워지고 있습니다. 이러한 현상의 원인은 다음과 같습니다.

1

직원들이 데스크톱, 랩톱, 스마트폰, 태블릿, 복합기를 비롯한 다양한 커넥티드 디바이스를 사용하여 일상 업무를 수행하는 것이 일반화되면서 직원들이 보유한 **커넥티드 디바이스의 수가 전례 없이** 늘어났습니다.

2

사용되는 커넥티드 디바이스의 수가 증가하면 **이러한 장치들 사이에서 수집되고 전송되는 데이터의 양도 증가합니다.** 그 결과, 사이버 공격자가 이용할 수 있는 공격 표면이 넓어집니다.

3

**대부분의 커넥티드 디바이스는 보안을 염두에 두고 설계되지 않습니다.** 이러한 장치들은 주기적인 소프트웨어 업데이트나 제조사 또는 벤더의 보안 패치와 같은 사이버 공격을 예방하기 위한 보안 조치를 충분히 갖추지 못하고 있습니다.



### 모바일 보안 위협:

- 피싱 공격, 악성 애플리케이션, 취약한 네트워크, 중간자(MiTM) 공격<sup>21</sup>



### 인쇄 보안 위협:

- **내부 위협:** 다른 사용자에 의한 무단 사용, 부주의한 실수로 인한 데이터 침해
- **외부 위협:** 소프트웨어 탬퍼링, 장치에 저장된 문서 데이터 침해, 감사 로그 탬퍼링, 도청 및 통신 데이터 탬퍼링, 관리자 기능 무단 액세스

# IT 위협으로부터 조직 보호하기

기업은 식별된 IT 보안 과제를  
해결하기 위한 강력한 보안 계획을  
수립해야 합니다.

보안 위협으로부터 조직을 보호하기 위한  
권장 사항은 다음과 같습니다.

과제



권장 사항



비즈니스 우선 사항과 IT 보안  
우선 사항 간 불일치 극복

조직 내 사이버 회복 탄력성  
구축

직원을 위한 데이터 보안  
교육

직장 내 사이버 보안 인식  
강화

IT 보안 인력난 해결

클라우드 도입에 따른 보안  
과제 해결

외부 IT 전문가 서비스를  
이용하여 IT 부서를 지원

네트워크 복호화에 대비

디지털 공간의 보호

사용되는 장치들에 대한  
보안 계획 마련

# 조직 내 사이버 회복 탄력성 구축

사이버 회복 탄력성이란  
사이버 공격을 예측하고 공격이  
발생했을 때 대응하고 회복할 수  
있는 조직의 능력을 말합니다.

갈수록 정교해지는 사이버 공격에  
대비하려면 반드시 사이버 회복 탄력성을  
우선 사항으로 삼아야 합니다. 과거에는  
시스템을 해킹하는 데 수 일이 걸렸던  
반면에 오늘날의 사이버 공격은 불과 수  
시간 내에 일어날 수 있습니다.  
기업이 공격을 신속하게 방어하려면  
통합되고 현대화된 IT 보안 계획 및  
시스템을 구축하는 것이 중요합니다.<sup>22</sup>

## 사이버 회복 탄력성을 구축하기 위한 요소<sup>23</sup>



1



### 예측

조직의 자산, 취약점 및 잠재적 위협을 파악합니다.

2



### 방어

시스템, 프로세스 및 툴을 실행하여 데이터 및 커넥티드  
디바이스를 보호합니다.

3



### 회복

적시 회복이 중요하므로 이를 위해 보안 사고의 영향을  
최소화하기 위한 사고 대응 계획을 수립합니다.

4



### 발전

발생한 사고를 통해 학습하고 이를 통해 얻은 인사이트를  
바탕으로 조직의 IT 보안 조치의 잠재적 허점을 개선합니다.

## 직장 내 사이버 보안 인식 강화

IT 보안의 경우 최첨단 기술을 갖추더라도 직원이 조직 내 가장 약한 고리인 경우가 많습니다.

사이버 보안 인식 훈련 프로그램을 시행하면 이러한 문제를 해결하는 데 도움이 될 수 있습니다. 이러한 프로그램을 통해 팀은 최신 보안 위협, 베스트 프랙티스 및 업종별 규제 준수 요구사항에 대한 지식을 습득할 수 있습니다.

그 결과 보안 사고의 위험을 최소화하고 관련 산업 규제 준수를 촉진하여 조직의 보안 태세를 강화할 수 있습니다.

### 워크플레이스 내 사이버 인식 베스트 프랙티스



#### 사이버 보안 인식 훈련을 전사적인 프로그램으로 시행하세요.

임직원의 니즈를 해결할 수 있는 방향으로 훈련 내용을 맞춤화하세요.



#### 일회성 접근법은 지양하세요.

정기 훈련을 통해 최신 위협 및 공격 기법에 대한 업데이트를 팀에 제공하세요.



#### 피싱 모의 훈련 및 시험 일정을 수립하세요.

조직의 보안 전략에 있는 취약점을 식별하고 직원들이 모의 훈련 과정에서 피싱 공격을 인지하고 회피할 수 있도록 지원하세요.





## 외부 IT 전문가 서비스를 이용하여 IT 부서를 지원

대규모 네트워크 복호화 공격에 대비하거나 원활한 클라우드 마이그레이션 과정을 보장하는 일과 같이 대부분의 비즈니스 보안팀이 수행하기 어려운 새로운 과제들을 고려할 때, 신뢰할 수 있고 역량 있는 IT 전문가 서비스를 제공함으로써 IT팀이 사이버 공격자보다 한발 앞서 나가도록 지원할 수 있습니다.

예를 들어, 네트워크 복호화에 대응하는 데 있어서 IT 전문가는 기업에 다음과 같은 역량을 제공할 수 있습니다.

- ✓ 민감한 데이터가 손쉽게 복호화될 위험이 있는지 판단
- ✓ 암호화 기술을 지속적으로 업데이트



클라우드 마이그레이션의 경우, IT 전문가는 전체 마이그레이션 과정을 모니터링하고 안내할 수 있습니다. 또한 규제 요건을 만족하기 위한 적절한 절차, 사고 대응 계획 및 정기 훈련 및 모의 훈련이 수행되도록 보장할 수 있습니다.

외부 IT 전문가 서비스를 통해 기업은 잠재적 이슈 및 보안 침해 위험을 제거할 수 있습니다. IT 전문가는 수시로 평가를 수행하고 적시에 업그레이드를 수행합니다. 이를 통해 기업은 규제 준수 상태를 유지하고 사후 대응이 아닌 선제적 대응을 수행할 수 있습니다.



### 아태 지역의 기업들이 관리형 및 전문 보안 서비스 업체와 함께 하는 이유 <sup>24</sup>:

아태 지역 내 데이터 침해 사고 증가

디지털 트랜스포메이션 진행으로 클라우드  
사용 증가

IT 보안 전문가 인력난 극복

외부 보안 전문 서비스 및 규제 준수  
인사이드에 대한 필요성 증가

자체 보안 전문가를 고용하여 비용을  
절약하고 효과적인 보안 관리 서비스를  
이용

## 사용되는 장치들에 대한 보안 계획 마련

기업은 데스크톱, 랩톱, 태블릿, 서버, 스마트폰, 기타 커넥티드 디바이스를 포함한 모든 엔드포인트에 대한 보호를 제공하는 IT 보안 솔루션을 도입해야 합니다.

또한 사이버 공격으로부터 자사의 인쇄 장치도 보호해야 합니다. 인쇄는 모든 조직이 수시로 수행하는 일반적인 업무이기 때문에 방대한 양의 비즈니스 정보가 프린터를 거쳐갑니다.

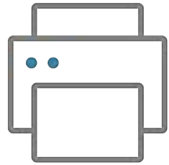


보안 인쇄 전략을 수립하려면 다음과 같은 요구사항을 만족해야 합니다.

- ✓ 조직의 네트워크에 연결되는 모든 장치가 보호되도록 합니다.
- ✓ 조직 내 모든 커넥티드 디바이스가 동일한 보안 기준 및 정책의 적용을 받도록 합니다.
- ✓ 보안 인쇄 출력 기능을 제공하는 솔루션을 통해 프린터 출력을 보호합니다.
- ✓ 갈수록 정교해지는 사이버 위협에 대한 최신 보안 기능을 제공하는 관리형 인쇄 서비스를 활용합니다. 이러한 서비스는 인쇄를 자주 하고 분산된 인쇄 환경을 가진 기업에 이상적입니다.



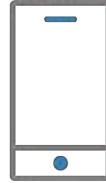
## 프린터 보안: 구현해야 할 주요 기능



### 보안 인쇄 출력

보안 인쇄 출력을 통해 사용자가 프린터로 이동하고 최종 인쇄 명령이 전달될 때까지 인쇄 작업을 보안 가상 대기열에 대기시킬 수 있습니다. 인쇄 작업을 출력하려는 직원은 반드시 먼저 PIN 번호, ID 카드, 모바일 앱 또는 QR 코드 스캔과 같은 다양한 방법을 통해 본인 인증을 해야 합니다.

이러한 기능을 통해 인쇄 작업을 수거하지 않거나 기밀 출력물을 프린터에 방치하거나 실수로 다른 사람의 중요 문서를 수거하는 등의 일반적인 프린터 사용자 실수를 최소화할 수 있습니다.



### 보안 모바일 인쇄

보안 모바일 인쇄는 직원들이 커넥티드 디바이스를 사용하여 안전하게 인쇄 작업을 제출할 수 있게 해주며, 일반적으로 인증, 암호화, 사용자 권한 할당, 로그 기록 및 감사와 같은 기능을 포함합니다.

보안 모바일 인쇄는 하이브리드 근무제를 운영하고 직원들이 외근 시 자신의 장치로부터 인쇄 작업을 해야 하는 등의 특정 업무 환경에서 매우 중요합니다.

특히 의료나 금융 분야에서처럼 문서 보안에 관한 규제 요건을 만족해야 하는 기업에는 필수적인 기능입니다.



### 360° 전방위 데이터 보안

360° 전방위 데이터 보안은 보안 스캐닝부터 무단 액세스 차단과 장치의 실시간 모니터링을 위한 감사 추적까지 보안을 위한 강력한 기능들을 포함합니다.

주요 기능으로는 원터치 사용자 인증 (사용자 및 인쇄 환경을 효과적으로 관리), 향상된 감사 기능 및 보안 네트워크를 통한 엔드투엔드 데이터 암호화 등이 있습니다.

# IT 전략 수립을 위한 체크리스트

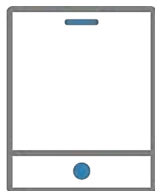
IT 전략 수립에 대한 권장 사항은 다음과 같습니다.

## 조직의 IT 보안 역량 평가



- 각 팀원이 보유한 기술과 전문 지식을 평가합니다.
- IT 보안팀에 대한 자원 할당 현황을 평가합니다. 예산이 조직의 보안 니즈에 부합하는지 평가합니다.
- 팀의 개선이 필요한 부분 및 기술 격차를 해결하기 위한 계획을 수립합니다.
- 외부 IT 전문가 서비스 이용과 같이 조직의 역량을 강화하는 데 도움이 될 수 있는 솔루션을 모색합니다.

## 사이버 회복 탄력성을 구축하기 위한 계획 이행



- 조직의 자산, 취약점 및 잠재적 위협을 식별하기 위한 평가를 수행합니다.
- 데이터 및 커넥티드 디바이스를 보호하기 위해 필요한 시스템, 프로세스 및 툴에 대한 개요를 작성합니다.
- 잘 짜여진 사고 대응 계획을 수립합니다. 주기적으로 모의 훈련 및 시뮬레이션을 통해 수립된 계획을 테스트 및 업데이트합니다.
- IT 보안 인프라를 모니터링합니다. 주기적으로 전략을 검토하고 업데이트합니다.

## 사이버 보안 인식 훈련 프로그램 실행



- 사이버 보안 인식 훈련 프로그램의 목표를 확인합니다.
- 훈련 프로그램을 위한 콘텐츠를 준비합니다.
- 누구나 쉽게 훈련 자료 및 세션을 이용할 수 있도록 직원 훈련 세션 일정을 수립합니다.
- 훈련 프로그램의 효과를 모니터링 및 평가합니다.
- 프로그램이 항상 최신 위협 환경을 반영하도록 주기적으로 콘텐츠 및 훈련 자료를 업데이트합니다.

## 커넥티드 디바이스에 대한 계획의 이행



- 조직의 프린터 및 커넥티드 디바이스 목록을 최신으로 유지합니다.
- 프린터 및 커넥티드 디바이스에 대한 사용자 인증을 실시하여 권한이 있는 사용자만 해당 장치에 접근할 수 있도록 합니다.
- 모든 프린터 및 커넥티드 디바이스의 소프트웨어를 최신 버전으로 유지합니다.
- 각 장치의 보안 기능을 검토합니다. 보안 인쇄 출력과 보안 모바일 인쇄와 같이 중요한 인쇄 보안 기능을 제공하는 솔루션을 이용합니다.
- 변화하는 인쇄 보안 위협에 대비한 최신 보안 기능을 제공하는 관리형 인쇄 서비스를 이용합니다.
- 조직의 사이버 보안 인식 훈련 프로그램에 프린터 및 커넥티드 디바이스의 보호에 관한 정보가 포함되도록 합니다.

# 최우선 비즈니스 과제인 IT 네트워크 보안

아태 지역의 기업들은 역내 증가하는 글로벌 보안 공격에 대비하기 위해 IT 보안을 최우선 과제로 삼아야 합니다. 위협이 증가하면서 네트워크, 데이터 및 프린터를 포함한 장치를 보호하는 것에 대한 기업들의 관심이 높아지고 있습니다.

역동적인 위협 환경에 효과적으로 대응하기 위해서는 IT 보안에 관한 최신 트렌드와 과제를 지속적으로 파악하고 안정적인 보안 솔루션을 구현하기 위한 유연한 계획을 운영해야 합니다. 이러한 전략적 접근법을 바탕으로 기업은 진행 중인 프로세스와 강력한 IT 파트너십을 통해 자사의 보안을 강화할 수 있습니다.


**신뢰할 수 있고 경험이 풍부한 IT 보안 파트너로서 귀사의 IT팀에 적합한 솔루션 및 지원을 제공하는 후지필름비즈니스 이노베이션과 함께 하세요.**





# 후지필름비즈니스이노베이션과 함께 성공하기


후지필름비즈니스이노베이션의 강력하고 안정적인 디지털 기술 및 자동화 솔루션은 귀사의 디지털 트랜스포메이션을 지원합니다.



 **AppGuard**는 차세대 사이버보안 소프트웨어입니다. 고유의 전매 특허 기술을 기반으로 멀웨어 탐지 및 식별 외에도 모든 무단 사용을 전면 차단할 수 있습니다. 이를 통해 알려지거나 알려지지 않은 멀웨어의 위협으로부터 귀사의 엔드포인트 및 서버를 효과적으로 보호하여 보다 안정적인 IT 보안 환경을 구축할 수 있습니다.

 **ApeosWare Management Suite 2**는 원활한 장치 관리, 통합 인증, 보안 인쇄 출력, 로그 회계, 문서 배포 및 정보 유출 추적을 지원하는 인쇄 관리 소프트웨어입니다. 종합 문서 관리 기능을 간소화하여 기업에 상당한 가치를 제공합니다.

 **IT 전문가 서비스**는 중소기업을 대상으로 한 종합적인 관리형 IT 지원 서비스입니다. IT 전문가 서비스를 통해 중소기업은 실력 있는 IT 전문가의 도움을 받으면서 보다 중요한 비즈니스 업무를 추진하는 데 집중할 수 있습니다.

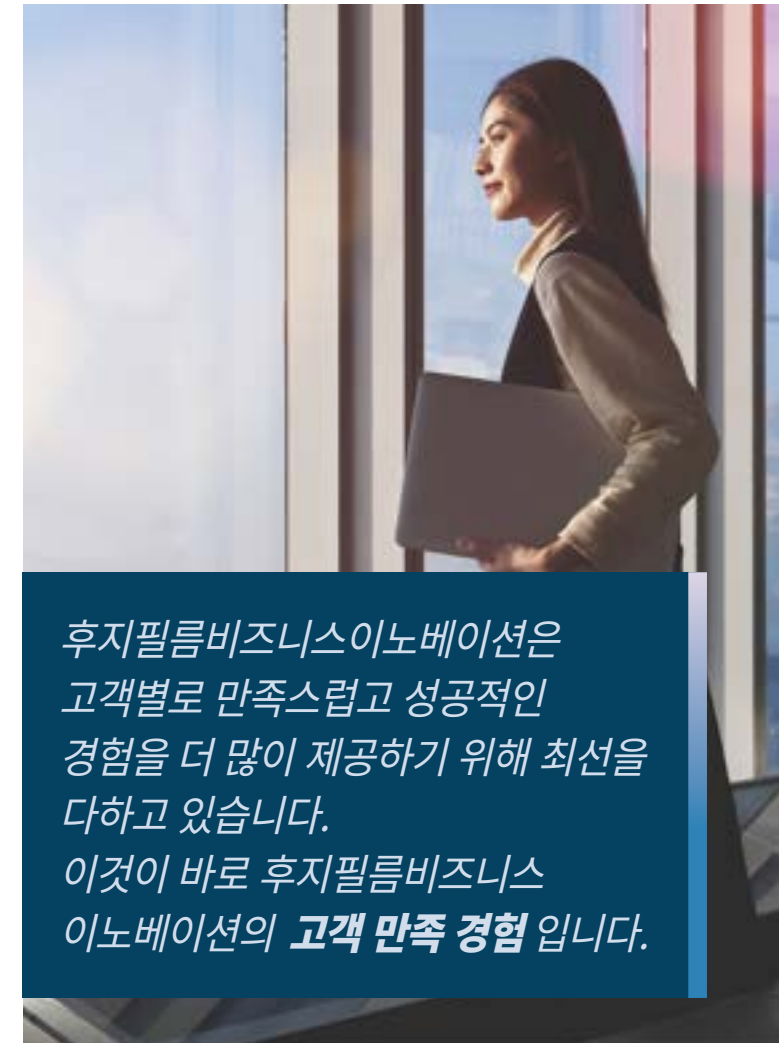
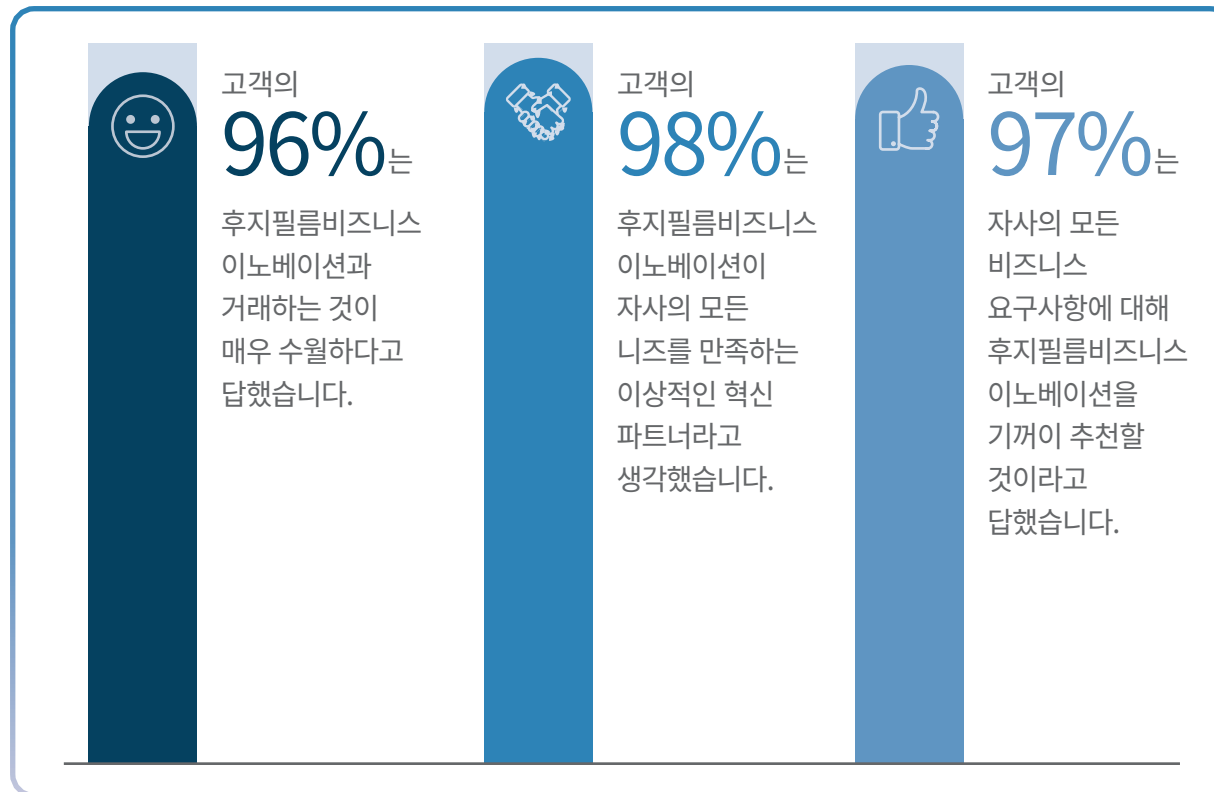
 **MPS(Managed Print Services) Guardia**는 비용 초과, 데이터 침해 및 생산성 손실 등으로부터 조직을 보호해주는 후지필름비즈니스이노베이션이 제공하는 차세대 관리형 인쇄 서비스입니다.



# 후지필름비즈니스이노베이션과 함께 디지털 트랜스포메이션 여정을 위한 역량 강화하기

기업들은 후지필름비즈니스이노베이션의 솔루션과 전문성을 활용하여 지속적인 디지털 트랜스포메이션을 위한 다음 단계로 나아갈 수 있습니다. 후지필름비즈니스이노베이션의 소중한 고객들이 전하는 후지필름비즈니스이노베이션과의 파트너십에 대한 이야기를 들어보세요.

당사 고객 설문 조사를 통해 다음과 같은 놀라운 인사이트를 얻을 수 있었습니다.



후지필름비즈니스이노베이션은 고객별로 만족스럽고 성공적인 경험을 더 많이 제공하기 위해 최선을 다하고 있습니다. 이것이 바로 후지필름비즈니스이노베이션의 **고객 만족 경험**입니다.

## 후지필름비즈니스 이노베이션과 함께 귀사의 IT 보안 역량 강화하기

사이버 위협이 나날이 증가하고  
정교해지면서 기업들은 IT 보안을  
최우선 과제로 삼아야 합니다.  
후지필름비즈니스이노베이션과 함께  
하면 귀사의 사이버 보안 태세를  
구축하도록 도와주는 안정적이고  
강력한 솔루션을 갖출 수 있습니다.

고객 중심 기업인 후지필름비즈니스이노베이션은 당사 파트너를 위해 탁월한 경험을 구축하는 데 있어서 큰 자부심을 느낍니다. 당사는 고객에게 효과적으로 작동할 수 있는 올바른 솔루션을 구현하기 위해 고객과 긴밀하게 소통합니다.

빠르게 변화하는 IT 보안 환경에 대응하기 위한 파트너로서 후지필름비즈니스 이노베이션은 항상 귀사와 함께 하겠습니다.

귀사가 디지털 트랜스포메이션의 잠재력을 최대한 실현하고 보안 위협으로부터 조직을 안전하게 지킬 수 있도록 돕겠습니다.



지금 문의하여  
후지필름비즈니스  
이노베이션과 함께 미래를  
준비하고 관리하세요.

# 참고 자료

12. Accenture, Scaling Enterprise Digital Transformation, 2021년 8월
3. IBM, IBM Security X-Force Threat Intelligence Index 2023, 2023년 3월
4. Check Point Research, Global Cyberattacks Continue to Rise with Africa and APAC Suffering Most, 2023년 4월
- 5, 6, 7. Kroll, State of Incident Response: APAC, 2022년 10월
8. IBM, IBM Security X-Force Threat Intelligence Index 2023, 2023년 3월
910. Kroll, State of Incident Response: APAC, 2022년 10월
11. EY, Global Information Security Survey, 2021년 7월
12. Thales, 2023 Thales Global Data Threat Report, 2023년 6월
13. Usecure, The Role of Human Error in Successful Cyber Security Breaches, 2022년 6월
- 14, 15. ISC2, Revealing New Opportunities for the Cybersecurity Workforce, 2022년 10월
16. Deloitte, Finding cybersecurity talent in an altered world, 2023년 2월
17. Advantis Global, The Cybersecurity Talent Shortage: Understanding the Urgency and Impact, 2023년 7월
18. Boston Consulting Group and Cisco, The Future of Cloud in Asia Pacific, 2021년 8월
19. Alibaba Cloud, A Majority of Asia Businesses Expect to Increase Cloud Investment in 2023, 2023년 3월
20. Thales, 2023 Thales Global Data Threat Report, 2023년 6월
21. Tech Target, Top 4 mobile security threats and challenges for businesses, 2021년 5월
22. CNBC, Palo Alto Networks CEO warns companies need modern, integrated cybersecurity: 'The bad actors are moving faster', 2023년 8월
23. IDC, Leadership in a Changing Digital World: Five Mandates, 2023년 4월
24. Frost & Sullivan, Asia-Pacific (APAC) Managed and Professional Security Services Market: The Shortage of Cybersecurity Professionals is Driving MSS and PSS' Future Growth Potential, 2022년 11월

FUJIFILM 및 FUJIFILM 로고는 FUJIFILM Corporation의 등록 상표 또는 상표입니다.