ORACLE

CIO | EXCHANGE

사이버 복원력 확보를 위한 5가지 고려 사항

CIO | EXCHANGE

CIO Exchange Brief

이 CIO Exchange Brief는 Oracle CIO Exchange 이벤트의 주요 논의 사항을 요약한 첫 시리즈입니다. Oracle의 CIO인 Jae Evans가 주최한 이 가상 이벤트에서 글로벌 IT 리더와 동료들은 각계의 저명한 선도적 지식인들과 함께 최신 주제를 논의했습니다.

2021년 9월 CIO Exchange는 사이버 복원력을 주제로 다루었으며 이번에는 이벤트의 주요 논의 사항을 다룹니다.

1. 조직 운영에서 데이터 보안이 차지하는 중요성의 이해
2. 사이버 보안 전략의 강점 및 약점 평가
3. 클라우드 기술을 활용한 심층적인 보안 가시성 확보
4. 워크로드의 클라우드 집결로 방어 태세 강화
5. 고객 중심의 개인 정보 보호

사이버 공격이 발생하는 횟수

11

초마다 한 건

Cybersecurity Ventures[1]에 따르면 사이버 보안은 *2021*년 평균 *11*초마다 한 건이 발생하는 것으로 추정되며 전 세계에서 약 *6*조 달러에 달하는 손실이 발생합니다.

글로벌 사이버 범죄로 인해예상되는 손실 규모

10.5

조 달러

*2025*년까지 글로벌 사이버 범죄로 인해 예상되는 손실은 매년 *10*조 *5*천억 달러입니다.[2] 증가하는 사이버 공격에 선제적으로 대응하기 위해서는 조직의 보안 전략에서 사이버 복원력의 역할을 고려해야 합니다.

1. Cybersecurity Ventures, "5가지 주요 사실, 도표, 예측, 통계로 살펴보는 2020-2021 사이버 보안"
2. Oracle, "사이버 전쟁의 최전선에서"

1 조직 운영에서 데이터 보안이 차지하는 중요성의 이해

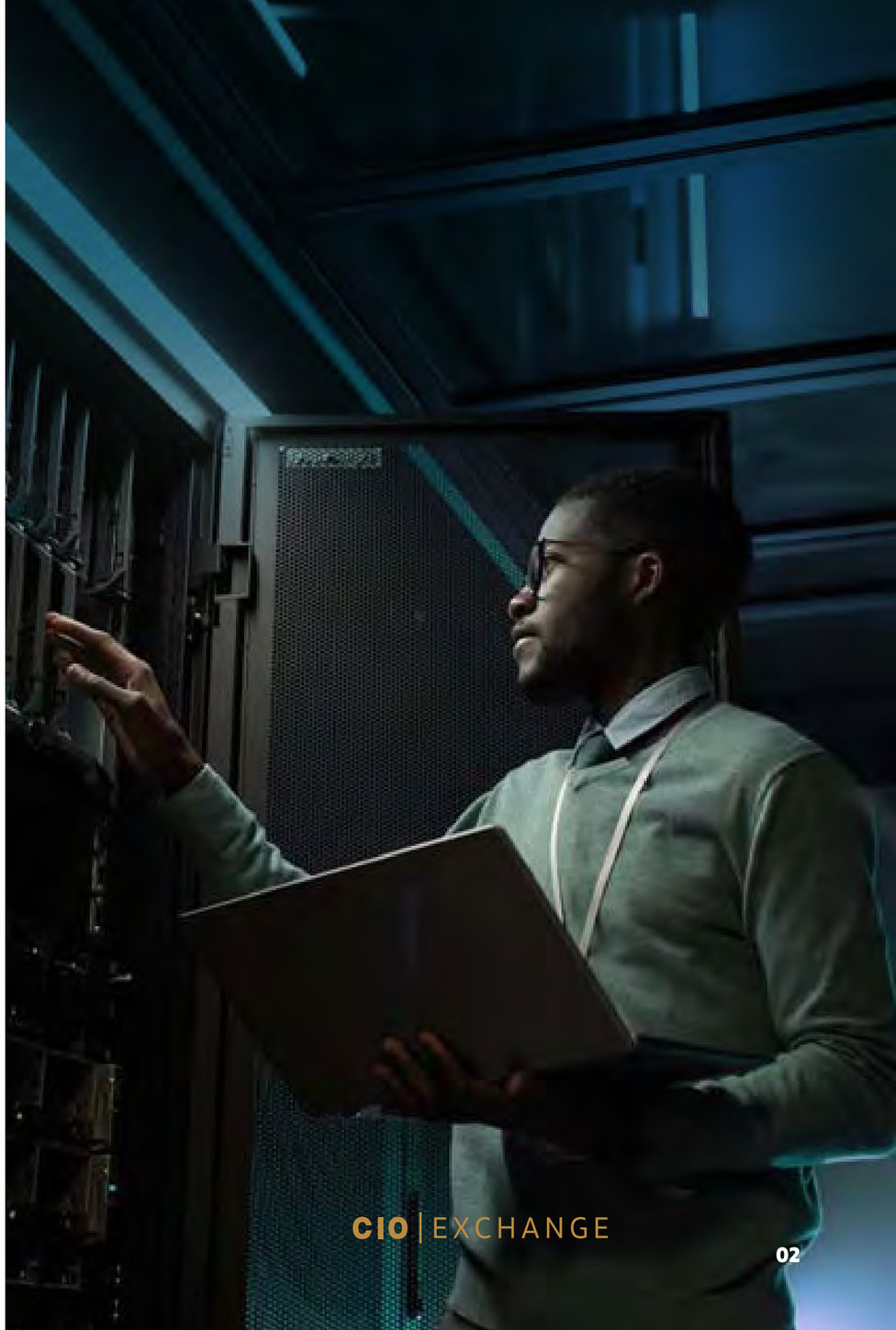
모든 조직은 위치에 관계없이 사이버 공격에 취약합니다. 보안 전략 개발은 사이버 공격 발생 시 데이터를 보호할 수 있는 중요한 단계입니다. 사이버 공격이 더욱 정교해짐에 따라 이를 방지하는 보안 기술의 개발 또한 지속적인 혁신이 필요합니다.

Deloitte가 정리한 사이버 방어의 기본 방어 조치에는 응답 계획, 자기 방어 계획, 사이버 인식 교육 및 위생이 포함됩니다. Deloitte 설문 조사 결과에 따르면 응답자의 9%만이 네 가지 조치를 모두 구현했습니다. 응답자의 53%가 자체 방어 계획을 완벽히 구현했으며 응답 계획, 사이버 위생 관행 혹은 정기적 사이버 인식 교육을 모두 구현한 응답자는 절반에도 못 미쳤습니다[3].

가상 세계의 영역이 점점 더 확대되면서 이제 기업들은 지능적 위협(advanced threat)으로부터 스스로를 방어해야 하는 위치에 있습니다. 또한 원격 근무로 전환하는 기업이 계속 증가하면서 피싱과 랜섬웨어 같은 사이버 공격이 전례 없는 속도로 증가하고 있습니다.

Ponemon이 조사한 바에 따르면 2021년을 기준으로 두 번째로 많이 시도되며 큰 피해를 입히는 데이터 침해 공격은 피싱입니다[4].

3. Cybersecurity Ventures, "2025년까지 글로벌 사이버 범죄로 인해 예상되는 손실은 매년 10조 5천억 달러"
4. Deloitte, "사이버 금융 조사 2021년 55월"



2 사이버 보안 전략의 강점 및 약점 평가

디지털 정보의 비중이 커짐에 따라
기업에서 디지털 인벤토리와 시스템의 보안 상태를 파악해야 할 필요성이 커지고 있습니다.

**사이버 보안 전략을 평가한다면
다음 질문에서 출발하는 것이 좋습니다.**

- ☑ **우리의 취약점은 어디인가요?**
- ☑ **이용 중인 벤더는 어떤 방법으로 소프트웨어 보안을 유지하나요?**
- ☑ **온프레미스 설비의 보안 수준은 어떤가요?**
- ☑ **인증 절차, 구획화, 무신뢰 원칙을 실천하고 있나요?**
- ☑ **직원들은 피싱 공격과 기타 사이버보안 위협에 대비한 교육을 마쳤나요?**

각 지역의 자치 단체와 기타 공공 기관의 경우 민간 부문 파트너십의 역할도 평가해야 합니다. 사이버 공격 방식이 계속 발전 및 진화함에 따라 자치단체와 기타 공공 기관을 대상으로 더 많은 공격이 이루어집니다. 공공기관의 경우 대규모 보안 자동화에 도움이 되는 전문 클라우드 제공 업체와 협력하여 신속한 공격 억제 능력을 갖춘다면 장기적인 복원력을 확보할 뿐 아니라 미래를 위한 최고의 기술에 투자할 수 있습니다.

3 클라우드 기술을 활용한 심층적인 보안 가시성 확보

분석에 따르면 랜섬웨어 비용을 지불하는 피해자의 일부는 동일한 집단의 2차 공격에 피해를 입을 가능성이 거의 80%에 달합니다. 랜섬웨어 공격에 피해를 입은 회사 가운데 66% 이상은 급격하고 심각한 수익 손실을 보고합니다[5].

사이버 보안의 핵심 전략은 행동 분석을 바탕으로 교육, 파트너십, 위협 감지에 대한 통제 능력과 가시성을 확보하는 것입니다. 조직은 이 정보를 이용해 위협으로 의심되는 활동을 감지함으로써 클라우드 보안을 통합하고 데이터 침해와 랜섬웨어 공격에 대비할 수 있습니다. 이러한 가시성 확보를 위해 일부 회사는 연구원을 고용해 사이버 범죄자의 행동을 분석합니다. 수많은 대규모 조직에서는 이를 위해 막대한 양의 IT와 보안 관련 리소스를 보안 부서의 채용, 구성, 유지에 투입하며 때로 이를 위해 과도한 비용이 비효율적으로 낭비되기까지 합니다.

> "세상에서 가장 중요한 데이터를 Oracle Cloud와 같은 클라우드에 집중시키는 일은 수만의 고객을 대신해 방대한 양의 자원을 데이터 보호에 투입할 수 있다는 것을 의미합니다. 또한 경제의 기본적인 관점에서 … 클라우드는 보안이라는 면에 있어 놀라울 정도로 당연한 선택입니다."
>
> **- Edward Screven, Oracle's chief corporate architect**

비즈니스 리더에게 사이버 위협의 실체가 더욱 명확해지면서 클라우드와 보안에 대한 기업의 생각이 달라지기 시작했습니다.

5. UpGuard, "2021년 데이터 유출로 비용 손실"

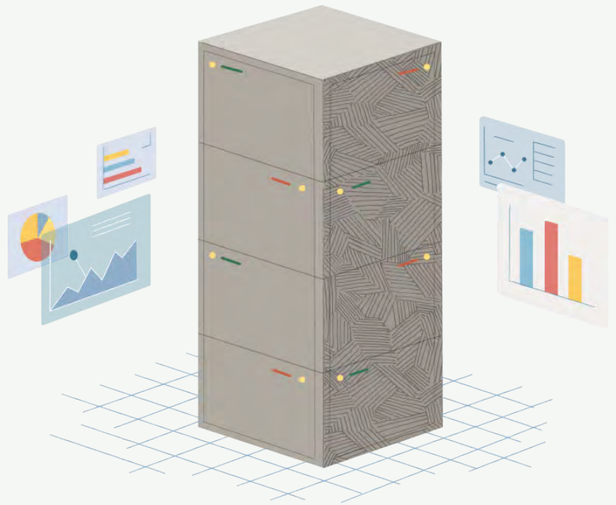
3 클라우드 기술을 활용한 심층적인 보안 가시성 확보

확장 및 자동화가 가능해지면서 공격이 더욱 정교해졌으며 때로 여러 위치에서 복수의 공격 시도가 발생합니다. 대부분의 클라우드 서비스 제공업체(cloud service provider, CSP)는 개별 조직보다 더 많은 자원을 보안에 투입할 수 있으며 궁극적으로 여러 고객을 보호하기 위해 보다 진보적이고 경제적인 기술을 제공합니다. Oracle과 같은 CSP는 보안 기능을 이미 내장하고 있기 때문에 조직에서는 CSP가 이미 투자한 보안을 활용해 비용을 절감할 수 있습니다.

세계에서 가장 규모가 크고 정교한 조직의 신뢰를 얻고 있는 Tanium은 사이버 보안 분야의 선도 주자로서 클라우드가 제공하는 효율성을 잘 보여줍니다. Tanium은 Oracle Cloud Infrastructure를 이용해 자사의 엔드포인트 관리 및 보안 제품인 Tanium as a Service(TaaS)에 보안을 기본 탑재하고 고가용성 및 검증된 가격 대비 성능을 제공합니다. 이는 결과적으로 더욱 폭넓은 고객 확보에 도움을 줍니다.

> "Oracle과 함께라면 고객 기반 확장이 가능합니다. 엔드포인트 제어를 원하는 중소기업 고객을 상대로 우수한 가격 경쟁력을 갖춘 제로 인프라(zero infrastructure) 기반의 솔루션을 서비스할 수 있기 때문입니다."
>
> **– Orion Hindawi, CEO, Tanium 공동창업자**

TaaS 고객은 Oracle Cloud Infrastructure의 정교한 인공지능 및 머신러닝 기능을 활용하여 Tanium의 실시간 데이터, 가시성, 제어는 물론 사이버 공격에 자동 대응하는 혜택을 누릴 수 있습니다.



4 워크로드의 클라우드 집결로 방어 태세 강화

사이버 공격이 더욱 정교해지고 빈도가 잦아지더라도 사이버 보안 전쟁에서 승리할 수 있습니다. 데이터 분석 같은 클라우드 서비스를 이용해 데이터 위험을 평가하고 이상 활동을 모니터링하면 보안 태세를 강화할 수 있습니다. 이는 사이버 복원력을 향상할 뿐 아니라 공격을 예측해 이에 대응하는 방법을 더욱 강화합니다.

온프레미스 시설의 보안 수준이 높다고 생각했지만 대부분의 조직에서 생각을 달리하기 시작했습니다. 실제로 75%의 조직은 이제 퍼블릭 클라우드가 온프레미스 시스템보다 더 안전하다고 판단합니다. 퍼블릭 클라우드 인프라에 탑재된 보안 서비스를 활용하면 클라우드상에서 애플리케이션을 구축하는 기업은 자체 리소스를 구비하지 않고도 클라우드에 탑재된 보안 기능을 활용할 수 있습니다.

또한 클라우드에서 제공하는 데이터 집계 기능으로 공격자에 대한 인사이트를 확보해 공격에 미리 대비할 수 있도록 도와줍니다.

기본 제공되는 보안 혜택에도 불구하고 클라우드에서 워크로드를 관리하면 복잡성이 증가할 수 있습니다. 이러한 과제는 프로비저닝 및 구성, 암호화, 패치 적용 및 업데이트, 확장 및 성능 튜닝을 자동화함으로써 바로 대응할 수 있습니다. Oracle의 자율운영 서비스는 수동 프로세스로 인한 조직의 위험을 낮추고 클라우드 규모의 데이터 관리에 소모되는 시간을 절약할 수 있습니다.

75% **의 조직에서 온프레미스 시스템보다 퍼블릭 클라우드가 더욱 안전함을 확인**

5 고객 중심의 개인정보 보호

기업에게 사이버 공격은 더 이상 간과할 수 없는 위협입니다. 이에 더해 모든 산업 전반의 디지털 전환에서 가장 잘 알려진 이슈가 데이터 유출과 사이버 복원성이라는 점은 흥미로운 혁신 기회를 보여줍니다.

PayPal은 2020년 한 해에만 9000억 건의 거래를 처리한 세계 최대 규모의 결제 서비스 업체 가운데 하나로서 고객 중심의 보안 접근 방식을 취하고 있습니다. 이 기업은 사이버 보안을 고객에 대한 약속으로 간주하며 기업의 모든 프로세스는 개인 정보 보호를 위해 설계되었습니다. PayPal의 부사장이자 CTO인 Sri Shivananda는 기업과 고객의 관계가 신뢰를 바탕으로 해야 한다고 말합니다. 그 신뢰의 가장 중요한 측면 가운데 하나는 안전입니다.

PayPal은 세계 최대 규모의 결제 서비스 업체 가운데 하나로서 2020년 한 해에만

900 **처리억 건 이상의 거래를**

"과거에는 재해 복구가 복원 기술의 첨단이라고 우리들 대부분이 생각했지만 지금은 사이버 복원이 이를 대체하고 있습니다."

– Sri Shivananda, EVP & CTO, PayPal

남은 일은 쾌속 전진

기술 업계의 미신 가운데 하나는 보안 분야의 발전이 느리다는 것입니다. 그러나 만족스러운 수준의 신속한 보안 경험을 고객에게 제공하는 일은 불가능한 미션이 아닙니다. 이는 플랫폼 중심의 사고방식으로 실현할 수 있습니다. 전사적 활용이 가능한 공통 보안 플랫폼을 구축하면 견고한 보안을 바탕으로 고객이 만족하는 제품과 경험을 신속하게 창출할 수 있습니다.

조직 전체가 보안 전략을 확립해 실행에 옮길 때 기업은 최선의 성과를 발휘할 수 있습니다. Oracle의 보안 우선 접근 방식은 인프라, 애플리케이션, 사용자의 모든 측면에서 최고 수준의 보안으로 데이터를 보호하기에 고객은 혁신에 더욱 집중할 수 있습니다.

"기술 분야의 여러 리더와 만나 사이버 위협으로부터 고객과 기업 환경을 보호하기 위한 의견과 통찰력을 확인할 수 있었습니다.

우리 모두는 보안의 중요성은 물론 기밀성과 무결성 유지의 중요성에도 동의했습니다. 직원과 제휴사를 비롯해 소비자와 고객사에게 제공되는 데이터와 서비스의 가용성 또한 마찬가지입니다."

– Jae Evans, CIO, Oracle

Oracle Cloud Security 시작하기

oracle.com/security

CIO Exchange 이벤트 자세히 알아보기

oracle.com/events/cio-exchange

ORACLE