FORTINET
361SECURITY
2017 한국, 서울

# 디지털 전환의 시대, 기업 사이버보안 해법




BylineNetwork
SPECIAL REPORT


# 디지털 전환의 시대, 기업 사이버보안 해법

전세계 기업들의 디지털 전환(Digital Transformation)이 가속화되면서 클라우드, 빅데이터, 사물인터넷, 인공지능 같은 새로운 기술이 적극 도입되고 있다. 디지털화가 가속화되는 환경에서는 사이버보안은 간과할 수 없는 필수불가결한 요소다.

더욱이 보안위협은 갈수록 정교하게 진화되고 다양화되고 있어 보안방식도 전통적인 방식보다는 새로운 접근법이 필요하다는 지적이 보안업계에서 대두되고 있다.

포티넷코리아는 10월25일 '2017 포티넷 361° 시큐리티' 컨퍼런스를 개최하고, 기업들이 빠르게 변화하는 사이버위협을 효과적으로 관리할 수 있는 보안 해법을 제시했다.

이번 행사에 연사로 참가하기 위해 방한한 매튜 콴(Mattew Kwan) 포티넷 아시아태평양지역 솔루션 마케팅 담당 이사는 "경계 방화벽, 기기 보안, 애플리케이션 보안 등 동종업계 최고의 보안 솔루션을 갖추는 것만으로는 보안공백을 메우기에 충분치 않다"고 지적했다.

콴 이사는 "서로 고립돼 운영되는 보안 솔루션을 서로 긴밀하게 통합해 최신 사이버위협 인텔리전스 정보를 공유해야 하며, 포괄적인 가시성을 확보해야 한다"라면서 "보안 프로세스를 자동화하는 것도 중요하고, 파트너십을 바탕으로 부족한 부분은 서로 협력해야 한다"고 강조했다.

앤써니 지안도메니코(Anthony Giandomenico) 포티넷 선임 보안전략가는 "자동화되는 사이버공격에 맞서 싸우려면 자동화된 보안방식으로 대응해야 한다"라면서 "포티넷은 자동화된 방어를 위해 인공지능, 머신러닝, 딥러닝을 활용해 실행가능한 위협 인텔리전스 정보를 파악해 보안 패브릭(Security Fabric)에 녹여낸다. 각 보안 제품들은 서로 커뮤니케이션해 자동화된 결정으로 자동 방어할 수 있도록 제공한다"고 밝혔다.

FORTINET


# 블록체인은 안전한가? 보안위협은 존재한다

이날 행사 기조연설자로 나선 매튜 콴 포티넷 아시아태평양지역 솔루션 마케팅 담당 이사는 "과연 블록체인은 안전한가?"라는 화두를 꺼내며 "블록체인도 네트워크 등의 기본 인프라 기반 서비스이기 때문에 보안위협 요소를 갖고 있다"고 지적했다.

그는 먼저 분산원장기술(Distributed Ledger Technology, DLT), 즉 블록체인이 전세계적으로 크게 각광을 받고 있는 이유로 데이터 품질이 높고 탈중앙화 된 모델이어서 신뢰성이 높고 안전하다는 점을 꼽았다.

또 컨센선스(합의)를 기반으로 프로세스를 운영하기 때문에 무결성이 높다. 블록체인으로 거래(transaction)가 이뤄진 데이터는 변경할 수가 없기 때문에 사기범죄에 이용될 위험성도 떨어지고 거래 투명성이 높아진다는 것도 이점으로 제시했다.

현재 거래 환경에 비해 생태계가 단순화되고 거래 속도도 빨라지고 비용도 크게 절감할 수 있기 때문에 다양한 산업군에서 개발과 도입을 적극 추진하고 있다.





콴 이사는 "블록체인은 아직 초기단계로, 많은 전문가들은 현재 블록체인을 월드와이드웹(WWW) 1.5세대에 비유한다"라며 "인터넷도 초창기부터 바이러스, 피싱, 랜섬웨어 등 많은 보안문제가 있었던 것처럼 블록체인 환경에서도 이같은 일이 반복될 수 있다. 앞으로 어떠한 일이 벌어질지 모른다"고 설명했다.

이어 그는 "많은 사람들이 블록체인은 신뢰성이 높으며, 암호화돼 있고 변경이 불가능해 안전하다고 믿지만 그 이상도 그 이하도 아니다. 블록체인 역시 네트워크와 서버 등 인프라가 필요하고 애플리케이션에서 월렛을 관리하기 때문에 보안이 반드시 필요하다"고 강조했다.

보안성과 신뢰성이 뛰어난 기술로 여겨지는 블록체인의 보안위협은 존재한다.

콴 이사가 제시한 블록체인의 취약성과 보안위협은 4가지다.

# 01

## 합의 가로채기 (Consensus HIJACK)

분산 모델인 블록체인은 참여자 다수의 합의를 도출해 거래가 무결하다는 것을 검증하는 과정을 거친다. 만일 공격자가 과반수 이상을 장악하면 거래 유효성 검증 프로세스를 조작할 수 있다.

높은 연산능력을 갖춘 컴퓨팅 파워를 이용해 공격자가 과반 이상을 점유하게 되면 노드 통제가 가능하다.

비트코인은 이를 '51% 공격'이라고 부른다. 51% 공격에 성공한 공격자는 자신이 점유한 비율을 뺀 나머지 블록체인 네트워크 부분보다 더 빠른 속도로 새 블록을 만들 수 있다. 다른 참가자들은 공격자가 조작한 체인이 유효하다고 간주하게 된다.

물론 블록체인 규모가 커지면 과반 이상을 점유하는 것 자체가 현실적으로 어렵다.

# 02

## 디도스(DDoS) 공격

공격자가 가짜 e월렛(전자지갑)을 만들어 블록체인 노드에 참여하거나 월렛이 침투당해 네트워크에 많은 수의 스팸 거래를 발생시키면 네트워크가 정상 작동하지 않게 만들 수 있다. 생성되는 수많은 거래의 사기 여부를 검증하느라 블록체인 처리속도가 느려져 서비스거부가 발생할 수 있다. 블록체인판 디도스 공격이다.

2016년 3월 비트코인 네트워크 속도가 느려져 중단에 가까워진 적이 있었다. 이 사태의 원인은 평균 거래 수수료보다 높은 스팸 거래를 대량 유발하는 비트코인 월렛에 있었다.

# 03

## 사이드체인 (Sidechains)

사이드체인 취약성은 두 불록체인이 연결되는 지점에서 발생한다. 하나의 블록체인을 사용하는 곳이 또 다른 블록체인을 사용하는 곳과 협력하기 위해 두 불록체인을 연동할 때 연결지점을 견고하게 만들기 위해 양방향 페깅(pegging)을 수행한다.

하지만 이 연결지점이 취약하면 공격을 받을 수 있고 자칫 큰 보안 문제로 이어질 수 있다.

# 04

## 스마트계약 (Smart Contract)

스마트계약은 블록체인에서 거래나 계약이 이뤄질 때 사용되는 프로그램이다. 때문에 코딩 작업 과정에서 오류나 결함으로 인한 취약점이 발생할 가능성이 충분하다.

지난해 실제로 스마트계약 취약점이 악용된 사례가 발생했다. 피해를 입은 기관은 '다오(The DAO)'라는 탈중앙화 자율조직이다. 다오는 크라우드펀딩으로 28일이라는 단기간 내에 1억5000만달러에 상당하는 이더(Ether)를 모금했다. 크라우드펀딩 역사상 최대 규모다. 그런데 2016년 6월 17일, 신원이 밝혀지지 않은 공격자가 스마트계약 코드 취약점을 악용해 다오 펀드를 공격, 이더리움에서 총 5000만달러 상당의 가상화폐를 탈취했다. 다행히 사건이 발생한 뒤 이더리움은 '하드포크(hard fork)/메트로폴리스(Metropolis)' 업데이트를 실시해 도난당한 이더를 복구했다.

콴 이사는 "블록체인은 아직 초기단계이기 때문에 잠재 리스크가 있다. 그리고 스마트계약 취약점을 악용한 공격이 발생한 것처럼 실제 위협도 존재한다"라면서 "블록체인을 도입할 경우 이같은 취약성을 고려해야 한다"고 강조했다. By

# "GDPR 시대, 대규모 개인정보 침해사고 발생시 기업 파산 수준 영향"

콴 이사는 유럽연합(EU) 개인정보보호법(GDPR) 시행이 기업에 미치는 영향을 시나리오를 바탕으로 설명하기도 했다.

GDPR은 EU의 법규정이지만 유럽 지역에서 사업을 하고 있는 기업, 그리고 유럽 내 거주하는 정부주체의 개인정보를 저장·사용해 서비스를 제공하거나 모니터링하는 기업까지 전세계 모든 기업에 적용된다.

콴 이사는 "GDPR을 위반하게 되면 조직이 도산하는 수준의 악영향을 미칠 정도로 산정될 수 있다"고 말했다.

GDPR을 위반하면 벌금이 부과된다. 데이터 침해 정도에 따라 두 가지 구조를 갖고 있다.

연간 매출액의 2% 또는 최대 1000만 유로 가운데 높은 금액으로 벌금이 부과된다.

데이터 침해 수준이 심각한 경우 연간 매출액의 4% 또는 2000만유로 가운데 높은 금액으로 부과된다.

이와는 별도로 피해자(정보주체)들로부터 손해배상 소송을 당할 수도 있다.

그는 작년 11월 영국의 테스코뱅크(Tesco Bank)에서 9000개 계정이 탈취된 대규모 개인정보 침해사고 사례를 들면서 "이 사고로 테스코뱅크는 2500만파운드의 벌금이 부과됐지만, 만일 GDPR이 발효된 이후 이 사고가 났다면 19억파운드의 벌금을 내게 됐을 수도 있다. 이같은 금액은 기업이 파산할 수 있는 높은 금액"이라고 강조했다.

GDPR은 데이터 침해 사고가 발생해 이를 탐지한 경우 감독당국에 지체 없이 그 사실을 알리도록 의무화하고 있다. 72시간 내에 통지해야 한다.

콴 이사는 "만일 GDPR이 발효된 후인 2018년 8월 20일에 최초 침입이 발생한 뒤 146일이 지난 후인 2019년 1월13일 해당기업에서 침해사실을 발견한 경우엔 72시간 이내에 감독당국인 EU에 통지해야 한다. 만일 1월16일에 통지했을 경우 손해액 산정은 탐지한 날부터 사실을 알린 3일을 기준으로 하지 않는다. 최초 침입이 발생한 날부터 146일 동안 입은 손해를 산정하게 된다"고 설명하기도 했다.

GDPR 시대에는 기업에 사이버침해를 예방하고 탐지하는 것이 더욱 중요해진다는 얘기다.

콴 이사는 "GDPR을 준수하려면 많은 정보와 시간, 그리고 비용이 필요하다. 하지만 GDPR은 기업 조직에 미치는 영향이 매우 크다. 기업의 제품과 서비스, 프로세스, 직원 등 관계자까지 조직 전체가 영향을 받는다"라며 "해킹과 침해사고를 예방하는 것도 중요하지만 예방조치가 실패하는 경우도 있기 때문에 빠르게 탐지해 어떻게 위험을 줄일 지 고민해야 한다"고 제안했다. By

# "자동화된 사이버공격, 자동화된 보안방식으로 대응해야"

"사이버범죄자들은 자동화된 툴을 사용한다. 자동화된 공격에 맞서 싸우려면 자동화된 보안방식으로 대응해야 한다."

앤써니 지안도메니코 포티넷 선임 보안전략가는 "사이버범죄 생태계가 정교하게 발전하면서 이제는 보안에 대한 경험이 많지 않아도 쉽게 악성코드를 생성하고 유포할 수 있게 됐다"라면서 이같이 강조했다.

그에 따르면, 악성코드는 점점 정교해지고 있다. 악성코드(malware)가 자동화되고 점점 더 '사람같은(Human-like) 행동'을 나타내는 수준에 근접하고 있다. 때문에 이에 맞서 자동화된 방식의 보다 정교한 침입 방어·보안시스템이 필요하다.

지안도메니코 보안전략가는 "악성코드가 네트워크 환경에 침입해 주변 환경을 식별해 원하는 정보를 찾고 취약한 시스템을 식별한다. 원하는 공격 대상과 목표를 찾아 액션을 취한다. 현재는 사람이 뒤에서 악성코드를 가이드 하지만, 점점 악성코드 스스로 행동하면서 미션 달성을 위한 액션을 취하는 방향으로 발전하고 있다"고 설명했다.

이어 그는 "악성코드가 점점 더 스마트해지고 있다는 흔적과 공격 성향이 나타나고 있다"라면서 "이제는 단일 플랫폼이 아니라 다중 플랫폼을 공격하고 있다"고 덧붙였다.

또한 "해킹 공격이 이제는 매우 쉬워졌다. 프로세스가 자동화돼 원하는 악성코드를 쉽게 확산시킬 수 있다"라며 "위협의 양이 계속 늘어나는 결과를 나타내기 때문에 이제는 자동화된 방어책이 필요하다. 기계(머신)가 사람을 위해 악성공격을 식별하고 서로 통신해 의사결정을 스스로 내려 공격을 막거나 영향을 최소화시킬 수 있도록 해야 한다"고 제안했다.

지안도메니코 보안 전략가는 두드러진 보안위협으로 취약한 사물인터넷(IoT) 기기를 활용한 공격을 꼽기도 했다.

그는 "IoT 위협은 실제 일어나고 있다"라면서 "IoT 기기가 클라우드에 접속하는데 있어 가장 약한 링크로 작용하고 있는데, 홈 라우터와 DVR, NAS, IP카메라, 프린터 순으로 공격을 많이 당하고 있다"고 소개하기도 했다.

대표적인 지능형 IoT 익스플로잇 공격으로는 '하지메(Hajime)' 봇넷과 미라이(Mirai)가 있다. 그중에서도 하지메 봇넷은 분산된 다중 플랫폼을 사용하는 취약한 IoT 기기를 공격하는데, 웜의 특징을 나타낸다. 중앙집중화된 명령제어(C&C)가 아니라 P2P 안에서 이뤄져 방어가 힘들다.

'하지메' 봇넷은 지난 2016년 10월25일 처음 공격을 탐지했는데, 9개 플랫폼과 x86 시스템을 공격했다. 포티넷은 하루에 3만여건의 '하지메' 봇넷 공격을 탐지하고 있다.

그럼에도 지안도메니코 보안전략가는 "보안연구자들은 '하지메' 봇넷을 좋은 봇넷, '미라이'는 나쁜 봇넷으로 간주한다"라면서 "하지메는 IoT 기기에 영향을 미치고 공격을 확산하고 있긴 하지만 악성 공격을 벌이지는 않는다. 하지메는 미라이 봇넷과 경쟁관계로 서로 영향을 미치고 있다"고 설명했다.

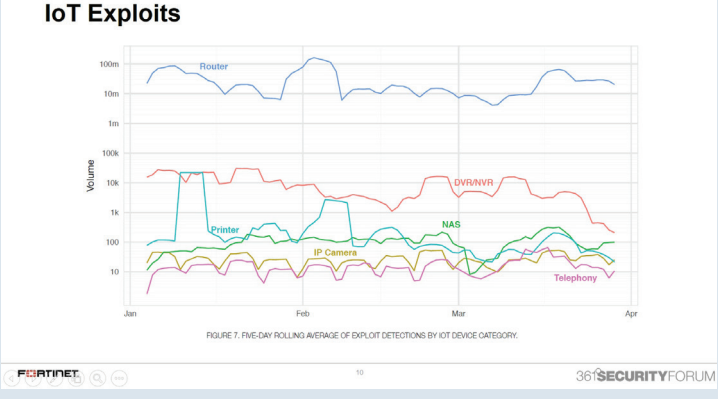
랜섬웨어 위협과 관련해서도 그는 IoT 기기를 대상으로 한 랜섬웨어 공격을 경고했다. 사이버범죄 생태계가 규모의 경제를 표방하고 있기 때문에 랜섬웨어 피해대상은 점점 증가하지만, 기기를 사용하지 못하도록 한 뒤 이를 풀어주는 대가로 요구하는 몸값은 상대적으로 낮아질 것으로 전망했다.

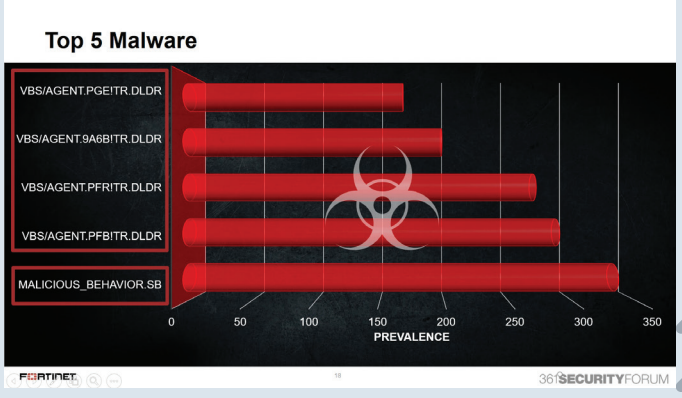
랜섬웨어는 대부분 이메일을 통해 확산되지만 취약점을 활용해 공격하면서 웜처럼 빠르게 확산되는 '랜섬 웜'의 형태로 바뀌고 있다는 것도 주요 동향으로 꼽았다.

'랜섬웜' 형태의 공격은 올해 워너크라이, 페트야(낫페트야) 사례에서 이미 발견됐다.

그는 "RaaS(Ransomware as a Service) 제공으로 랜섬웨어 공격이 매우 쉽게 이뤄지며, 서비스가 맞춤화되고 있다. 멀웨어를 생성한 사람과 수익을 공유하고 심지어 한 달에 10만건의 랜섬웨어를 설치하면 인센티브를 주는 체계도 운영하기도 한다"고 전하기도 했다.

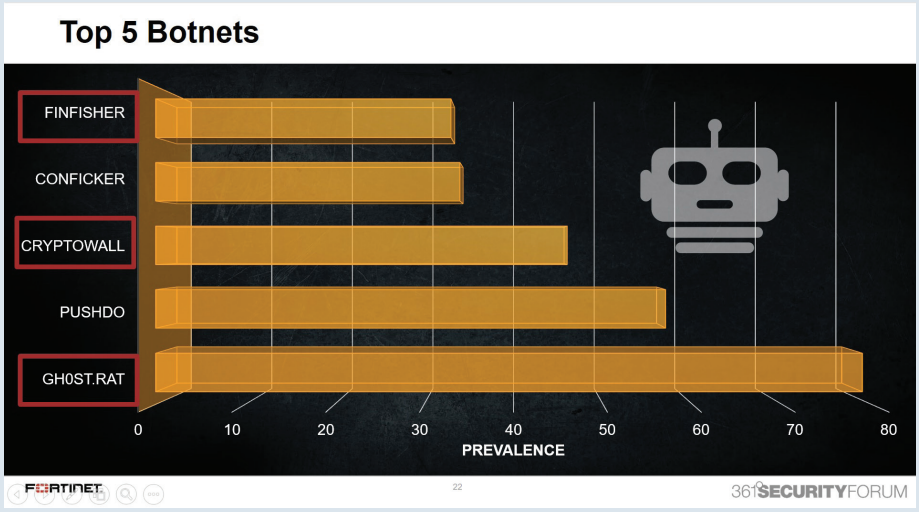
한편, 그는 한국을 포함해 아시아태평양지역에서 올해 3분기까지 가장 많은 활동을 나타낸 보안위협을 소개하기도 했다. 포티넷 포티가드랩에서 전세계 300만개의 센서를 통해 수집한 실제 공격 정보를 기반으로 분석한 결과다.



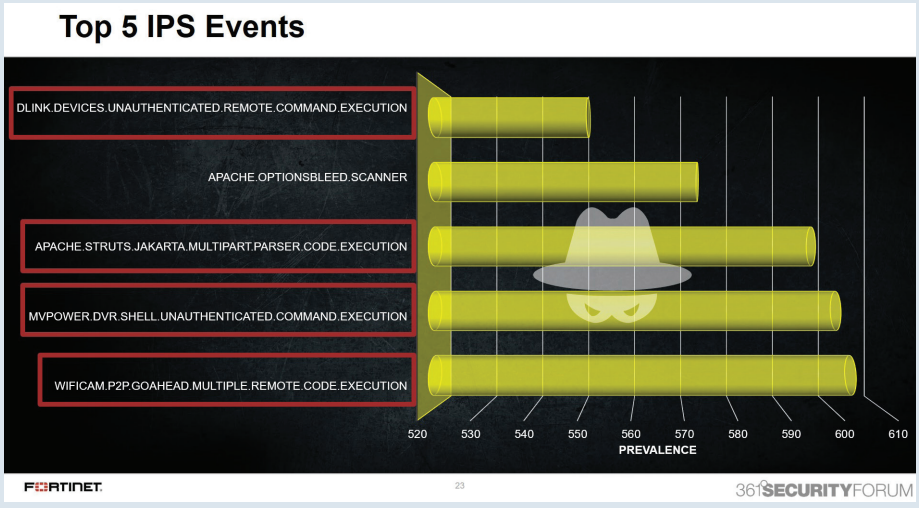
상위 5대 악성코드는 알려지지 않은 위협인 'Malicious_Behavior.SB'와 멀웨어를 다운로드하는 에이전트들(VBS/Agent.PFBITR.DLDR 등)로 대부분 이메일 첨부파일 내 악성매크로 등을 이용해 감염시킨다.

상위 5대 랜섬웨어는 크립토월(CrytoWall, 74%), 버록(Virlock, 10%), 토런트로커(8%), 케르베르(6%), 크립토쉴드(2%)다.




상위 5대 봇넷은 '고스트랫(Gh0st.RAT)', '푸시두(PushDo)', '크립토월', '컨피커(Conficker)', '핀피셔(Finfisher)' 등이다.

침입방지시스템(IPS) 이벤트로 분석한 상위 5개 익스플로잇 가운데 3개는 IoT 디바이스 관련 취약점 공격이다.




포티넷은 기존의 보안 장비들이 서로 연결돼 정보를 서로 공유하고 대응하는 '포티넷 보안 패브릭'을 제공하고 있다. 보안 패브릭 지능적 운영시스템인 '포티OS 5.6'과 새로운 보안운영(Security Operation) 솔루션을 기반으로 별도의 인적 개입 없이도 비즈니스 요구사항이 네트워크 보안 조치로 자동 연결되는 인텐트(Intent) 기반 네트워크 보안을 구현한다.

인텐트 기반 네트워크 보안은 궁극적으로 자체 긴급 대응이 가능한(self-sufficient) 기술을 고객에게 제공함으로써 고객들이 전체 공격 면에 대해 최적의 보안 태세를 지속적으로 유지할 수 있도록 해준다.

지안도메니코 보안전략가는 "자동화된 대응의 목표는 네트워크 위협이 발생하면 탐지했다는 수준의 경고가 아니라 위협을 탐지해 의사결정을 내려 대응 조치, 즉 실제 행동이 이뤄졌다는 보고를 받는 것"이라고 말했다. By


# "보안, 이거 실화다"

보안 현장에서는 분명 얘기치 못한 일이 많이 일어나고, 또 그에 대응하는 현장 경험이 넘쳐나기 마련이다. '2017 포티넷 361° 시큐리티' 컨퍼런스에 참여한 이 회사 직원들이 현장에서 느낀 생생한 고객사 체험기 말, 말, 말을 정리했다. 대기업, 중소기업, 금융권 등 각 산업군 보안 담당자들은 지금 어떤 이슈에 가장 관심이 있을까.

고우성 토크아이티 PD의 진행 아래 포티넷코리아 SE 이상훈 부장, 윤대영 차장, 안경진 차장이 패널로 참석해 고객사례를 발표했다. 이 부장은 공공·중견기업 기술지원을, 안 차장과 윤 차장은 각각 대기업군과 병원, 통신사를 담당하고 있다.

TOPIC 1

보안 트렌드

# Q. 각자 생각하는 요즘 보안 트렌드는.

**이상훈** 부장 — 데브옵스

"데브옵스의 개념이 시큐리티로 확장되고 있다. 스타트업은 아예 인프라 설계부터, 큰 인터넷 기업은 오퍼레이션 단순화를 위해 데브옵스를 도입한다. 오퍼레이션 단순화가 중요한 이유는 대부분의 회사가 이미 인프라를 구축하고 있는 상황에서 자동화를 위해 조직과 사람 제품을 모두 완벽하게 바꾸기 어렵기 때문이다. 자동화를 하는 이유는 휴먼 에러를 줄이기 위한 것인데, 그런 이유에서 무리 없이 장애 없고 안정적인 네트워크를 꾸릴 수 있게 하려면 오퍼레이션 단순화가 우선돼야 한다."

**안경진** 차장 — 솔루션 간 유기적 통합

"하나는 클라우드, 다른 하나는 솔루션 간 유기적 통합이다. 이를 포티넷은 '패브릭'이라는 개념으로 표현한다. 포티넷이 각 장비 간 유기적 통합이나 연결을 제공하는 개념을 최초로 제시했다. 대기업이나 해외 기업에선 통상 약 40개 정도 보안 제품을 쓴다고 한다. 각 제품군이 우수한 성능을 내지만 따로 동작하고, 심지어 다른 포맷을 가진 결과물을 보여주므로 이원화된 조직으로 보안 이벤트에 대응해야하는 어려움이 있다. 이렇게 되면 많은 인력과 노력이 필요한데, 그럼에도 불구하고 보안사고는 결국 발생한다. 우수한 제품의 성능을 통합, 단순화해서 사용할 수 있는 콘셉트가 제공되지 않아서다. 패브릭은 보안사고에 대응하는 시간을 획기적으로 줄일 수 있다. 보안 피해 발생 자체를 피할 순 없으나 그걸 최소화하는 데는 매우 큰 도움이 된다고 본다."

**윤대영** 차장 — SDN & NFV

"많은 통신사 고객들이 소프트웨어정의네트워킹(SDN)과 네트워크기능가상화(NFV)로 가고 있다. 이를 통한 가상화와 애플리케이션프로그래밍인터페이스(API)를 제공하고 있다. 조금 더 성능이 좋고 편하게 쓸 수 있는 통신 서비스를 제공해야 하므로 고민하고 있다. 그래서 매일 성능검증시험(BMT)와 개념검증(POC)을 한다. 포털은 기반 자체가 서버이다 보니 서버 가상화나 네트워크 가상화와 연계해 어떻게 보다 쉽게 적용하는지를 고민한다.

**이상훈** 부장
포티넷코리아

**안경진** 차장
포티넷코리아

**윤대영** 차장
포티넷코리아

TOPIC 2

## 고객 사례

# Q. 각자 맡은 영역에서 각 산업군의 특징과 고민, 구축 사례를 얘기해 달라.

### 이상훈 부장 — 공공기관, 인터넷 기업

"인터넷 기업은 일단 자유로운 분위기다. 그렇다보니 통제가 필요한 보안에선 힘든 부분도 있다. 최근 국내 인터넷 기업의 추세가 하나의 기업이 독자 생존하는 것이 아니라 몇 개 업체가 연합하는 경우가 생긴다. 그러다보니 보안 관리가 더욱 어려워진다. 수익을 내는 사업에 우선 투자하기 때문에 보안 투자는 뒤로 밀린다. 그래서 관리자의 부하를 줄여야 한다. 대기업처럼 무조건 '통제'하는 정책을 인터넷 기업이 도입하긴 어렵겠지만 명확하게 공격인 것만 막겠다고 하는 것에 대해선 누구도 뭐라 할 수 없다. 이 경우 관리자의 부하도 줄어든다."

"학교의 경우엔 인터넷 기업보다 인력이 더 없다. 대학은 대부분 네트워크 담당자가 정보보호책임을 겸직한다. 혼자하기 어려우니 외주 업체를 많이 쓰고, 그래서 운영도 더 어려워진다. 대학은 수강신청을 하는 서버, 내부 인터넷, 교직원 업무 등의 세 가지 다른 패턴의 트래픽 트렌드가 있는데 이를 모두 하려다 보니 투자비용이 크다. 그래서 패브릭 개념을 도입한다. 네트워크 장비와 스위치, 방화벽 등 보안장비를 '보안 패브릭'으로 연동했더니 한 화면에서 이를 한꺼번에 관리할 수 있는 형태가 됐다. 모두 좋아하더라."

(패브릭 연동 시스템 구축이 비용이 많이 들지 않느냐는 질문에) "예산이 새로 생길 때마다 단계별로 차근차근 하나씩 붙여가는 형태를 추천한다. 기존 솔루션이라도 연동이 가능한 부분이 있다면 직접 API 연동을 하지 않더라도 운영을 단순화할 수 있는 방법이 있다. 이를 추천한다.

### 안경진 차장 — 대기업, 병원

"그룹사의 경우 내부 근무자도 많고, 계열사도 많다. 때문에 여러 가지 부가적 기능을 요구 했다. 사용하고 있던 벤더사가 차세대 방화벽뿐만 아니라 지능형지속위협(APT) 공격에 대응할 솔루션이 없었으므로 다른 회사와 포티넷의 BMT를 통해서 시험을 해보고 채택했다. 모바일 환경이라든지 이동성이 잦은 근무자를 위해서 IP 상관없이 상자를 제어할 수 있도록 연동을 통해서 차세대 방화벽 모든 기능을 사용해 보완했다."

"대학과 마찬가지로 보안에 취약한 곳이 헬스케어다. 대학은 공격 대상이 일부 학생이나 관련 기록인데, 헬스케어 쪽은 환자 진료 기록, 병원 진료와 관련된 중요한 논문이나 서적이 대상이라 사람 목숨과 관련돼 있으므로 갈취 가능성이 가장 높은 대상이다. 대학과 마찬가지로 IT 인력, 특히 보안 인프라가 제대로 갖춰져 있지 않고, 사고 발생할 때 대응팀이 전무하다. 랜섬웨어나 APT 공격 대상이 되거나 피해 입는 사례가 많았다. 따라서 한 고객사도 레거시 방화벽만 운영해오다 실제 속도 저하라든지 이벤트 발생했을 때 로그 검색 속도나 샌드박스 연동 기술의 부재 등으로 인해 확장성이나 보안 향상을 이뤄내기가 굉장히 어려워 차세대 방화벽을 도입했다."

(병원 등에서는 BMT나 POC를 어떻게 진행하느냐는 질문에) "여러 제조사가 상호 연동되는지를 POC 하는데, 대부분 콘셉트가 솔루션 A와 B를 연결하는 것이다. 포티넷처럼 A를 중심으로 B, C, D, E, F가 연동돼 상호 정보 공유되는 콘셉트는 그 당시만 해도 보기 어려웠다. 지금도 찾아볼 순 있다 해도 각각 솔루션 포인트가 포티넷의 콘셉트를 따라 오기 급급한 정도다. 포티넷은 전체 솔루션을 하나로 묶어서 특정 이벤트가 다양한 곳으로 들어왔을 때 어떻게 정보를 공유하고 고객사에 대응방안 제공할 수 있는지에 중점을 두고 있다."

### 윤대영 차장 — 통신사

"많은 통신사 고객들이 소프트웨어정의네트워킹(SDN)과 네트워크기능가상화(NFV)로 가고 있다. 이를 통한 가상화와 애플리케이션프로그래밍인터페이스(API)를 제공하고 있다. 조금 더 성능이 좋고 편하게 쓸 수 있는 통신 서비스를 제공해야 하므로 고민하고 있다. 그래서 매일 성능검증시험(BMT)와 개념검증(POC)을 한다. 포털은 기반 자체가 서버이다 보니 서버 가상화나 네트워크 가상화와 연계해 어떻게 보다 쉽게 적용하는지를 고민한다. By



# "복잡한 보안 인프라, 한 눈에 모니터링 해야"

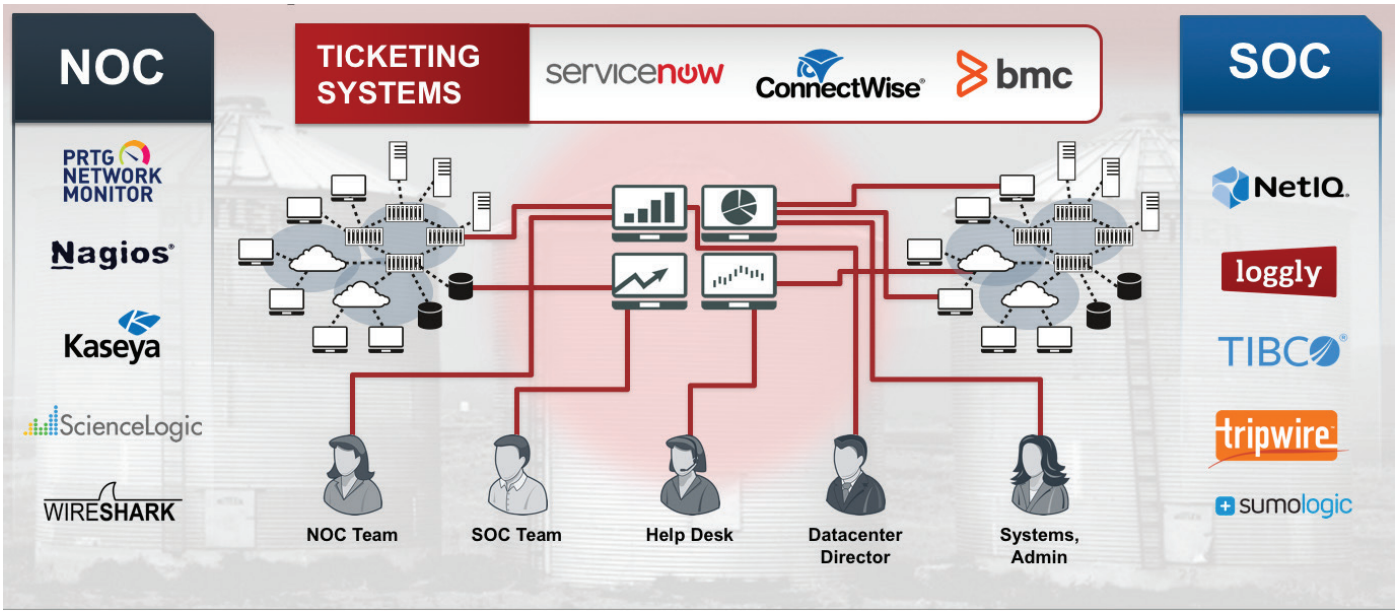
요즘 기업들은 매우 다양한 보안 인프라를 운영하고 있다. 엔드포인트, 네트워크, 서버 단에서 모두 보안 시스템을 운영한다. 한 기업에서 40가지의 서로 다른 보안 솔루션이 구동되기도 한다. 보안 사고가 나면 관련 솔루션 담당자들이 모여서 문제의 원인을 찾아야 하는데, 전체를 바라보는 뷰가 없어 원인을 찾는 것도 쉽지 않다.

이처럼 보안 환경이 복잡할수록 관리도 복잡해진다. 현재 대부분의 기업들은 인프라 전반을 모니터링 하지 못하고 각 부문별, 영역별로 별도로 모니터링 툴을 이용하고 있다. 이 때문에 보안 솔루션과 제품, 기술이 발전해 갈수록 이를 위한 관리도 복잡해지고 관리 비용도 점점 늘어난다.

기업 문화와 조직논리도 관리의 어려움을 더한다. IT환경은 물리 머신부터 가상 머신, 클라우드까지 다양해지고 있지만, 기업의 IT운영 조직은 네트워크, 서버, 엔드포인트 등으로 나뉘어져 있다. 보안운영센터(SOC)와 네트워크운영센터(NOC)도 별도로 돌아간다.

포티넷은 이런 문제를 해결하기 위해 '포티SIEM(보안정보이벤트관리)' 솔루션으로 통합운영환경을 제안한다. '포티SIEM'은 포티넷 뿐 아니라 다른 벤더의 보안 솔루션, 비보안 장비까지 하나의 관점으로 관리할 수 있는 모니터링 시스템이다.

보안과 네트워크 운영센터(Security and Network Operations Center)에 단일 모니터링 방식을 지원하는 솔루션으로, 가트너가 정의한 기존의 모든 SIEM 기능에 특허 받은 실시간 자산 디스커버리·분석, 신속한 통합, 멀티터넌트 아키텍처, 용이한 아키텍처 스케일아웃(scale-out) 등을 추가적으로 지원한다.




오경 포티넷코리아 이사는 '2017 포티넷 361° 시큐리티' 컨퍼런스에서 '가시성과 제어 능력 향상을 위한 SOC와 NOC 컨버전스 솔루션'이라는 주제로 '포티SIEM'을 소개했다.

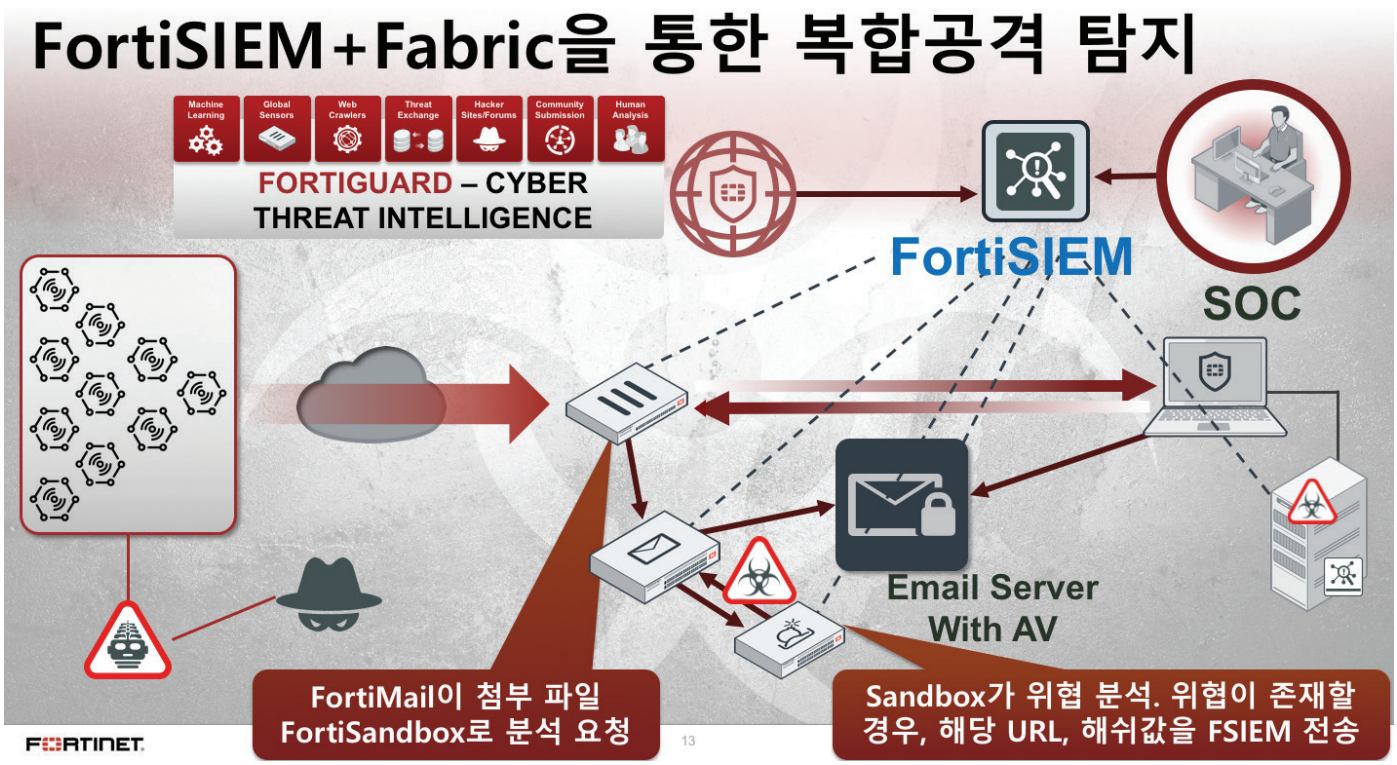
오 이사는 "기업의 IT 환경에는 포티넷의 솔루션 이외에도 다른 회사의 방화벽을 비롯한 보안 장비, 스위치 등 네트워크 장비, 서버 등 다양하게 운영하고 있다"라면서 "이를 한 눈에 보면서 관리할 수 있는 솔루션이 필요하다"고 말했다.

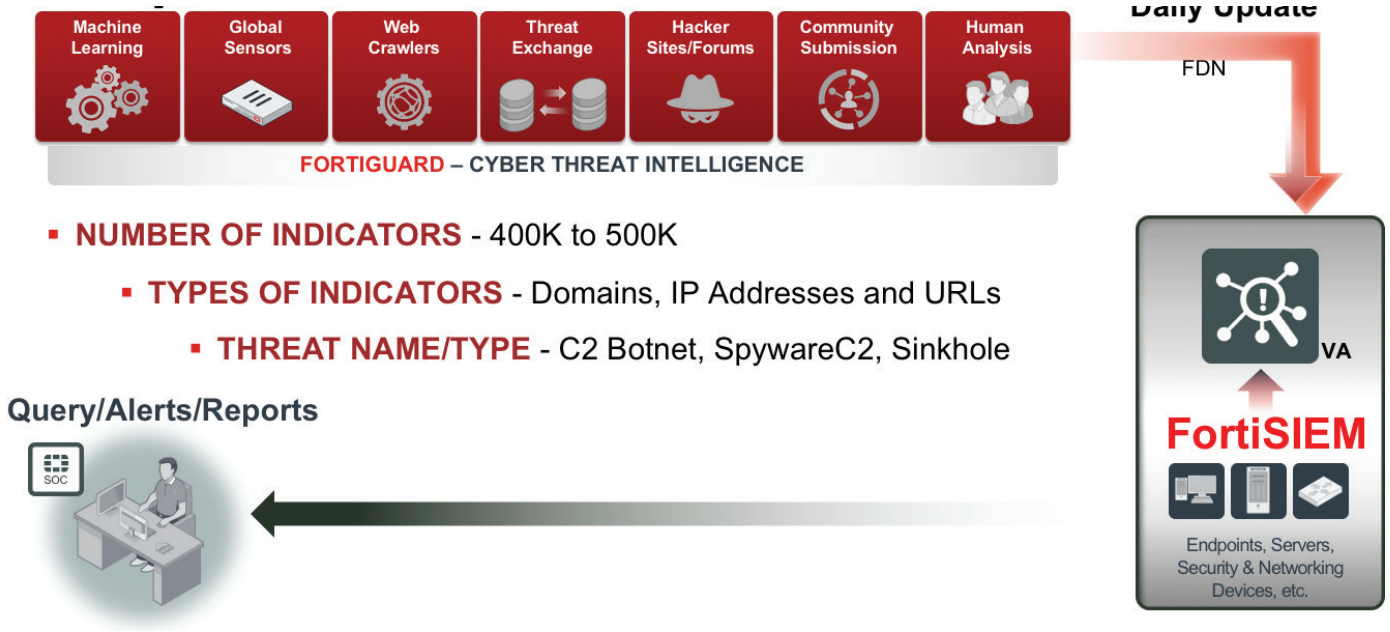
이어 오 이사는 "'포티SIEM'은 포티넷 보안 제품이든 경쟁사 제품이든 모두 한 눈에 모니터링 할 수 있고, 보안 장비가 아닌 소스로부터도 정보를 수집해 성능이나 가용성을 모니터링 할 수 있다"고 강조했다.

오 이사는 복합 공격(Blended Attack)이 들어왔을 때 '포티SIEM'이 어떻게 대응하는지 시나리오를 예시했다.

일단 공격자가 디도스(DDoS) 공격으로 시작한다고 가정하자. 공격자는 디도스 공격을 통해 정신없게 만들어 놓고 피싱 이메일을 보내거나 멀웨어를 심고 서버를 공격한다. 이처럼 네트워크, 이메일, 서버가 복합적으로 공격을 받는 경우는 흔하다. 이를 막기 위한 각각의 장비들이 있지만, 이 장비들을 각각 모니터링 솔루션으로 보는 방식으로 공격을 관리하긴 힘들다.

그에 따르면, '포티SIEM'은 방화벽, 모든 보안 장비, 네트워크 및 서버 장비까지 연동해 놓으면 각각의 장비들이 공격을 막았는지 샌드박스로 빠졌는지 인트라넷 내부로 들어왔는지 한 눈에 볼 수 있다.






## 디도스 탐지

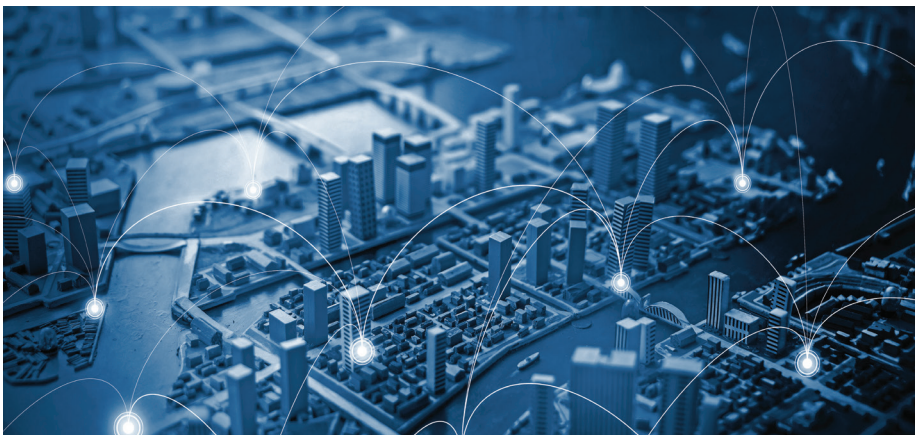
우선 '포티SIEM'은 레이어7(L7)을 모니터링하면서 디도스 공격을 탐지한다. 웹페이지가 얼마나 느려졌는지 '포티SIEM'에서 직접 체크할 수 있고, 인터페이스에서 트래픽이 얼마나 들어오는지 서버의 메모리는 얼마나 늘었는지, 네트워크 트래픽 정보가 다 보인다. 디바이스 성능을 모니터링 하면서 디바이스 공격도 감지할 수 있다.

이처럼 서비스와 디바이스의 성능을 모니터링 하면서 그 결과를 보안과 연관해 분석 결과를 제공한다. '포티SIEM'의 네트워크 대시보드에서 캐치할 수 있다. 기존에는 애플리케이션성능관리(APM) 솔루션에서 하던 일까지 '포티SIEM'이 하는 것이다.

## 피싱 이메일, 악성코드 탐지

악성코드나 피싱 이메일이 들어오는 것도 '포티SIEM'으로 모니터링 할 수 있다. '포티SIEM'은 자체적으로 파일 무결성 체크를 하는 기능이 있다. 또 보안 장비 없이도 '포티SIEM' 세션 트래픽을 분석할 수 있고, 보안 장비에서 보내는 것도 분석할 수 있다.

서버를 비롯한 사내 장비 목록을 하나의 대시보드에서 다 볼 수 있고, 각 장비의 가용성도 한 눈에 확인할 수 있다. 보안 장비만 하는 것이 아니다. 서버 장비의 건강상태, 하드웨어 버전, 인터페이스 상태 등까지 보인다. 윈도우 서비스의 상태도 볼 수 있다. 윈도우 서비스 중에 멈춘 게 있는지, 무언가 새로 설치한 것이 있는지 볼 수 있다. 기존에는 이런 정보는 윈도우 서버에 들어가야 확인할 수 있었다. 그러나 '포티SIEM'은 원격으로 확인할 수 있다.



## 침해위협 정보 연동

많은 벤더들이 침해위협 정보를 제공한다. 그러나 이 정보만으로 할 수 있는 일이 별로 없다. 이런 정보가 제대로 소비되기 위해서는 내 환경에 맞는 분석이 필요하다. '포티SIEM'은 침해위협 정보를 현재 기업의 보안 시스템 현황과 맞춰 구체적으로 어디가 약한 고리인지, 어떤 위협을 대비해야 하는지 알려준다.

'포티SIEM'은 당연히 포티넷 보안제품과의 궁합도 최적화 돼 있다. 예를 들어 '포티SIEM'은 '포티게이트'가 문제의 IP를 차단하거나, URL 또는 DNS 조회를 차단하도록 대응 조치를 수행한다. '포티샌드박스'가 위협을 분석해서 위협이 존재한다면 악성 URL 및 해시값을 '포티SIEM'으로 전송한다. '포티SIEM' 침해지표(IOC) 서비스에서는 로그값과 매치해 위험 수준에 대해 경고한다. '포티SIEM'은 관련 프로세스 정지, 네트워크에서 해당 디바이스 격리, 스캔 수행 등의 다양한 액션을 수행 가능하다.

오경 이사는 "고객이 원하는 것은 결국 공격이 들어오면 빨리 발견하고, 침해가 들어오면 그에 대한 대응력을 높이는 것"이라며 "이를 위해서는 전체 인프라 운영에 대한 단일 뷰 보안 관리가 필요하고 '포티SIEM'만이 할 수 있다"고 강조했다. By

# 포티넷, 2018년 어떤 신제품 내놓나


포티넷의 2018년 신제품 로드맵이 모두 공개됐다. 배준호 포티넷코리아 이사는 '2017 포티넷 361° 시큐리티' 컨퍼런스에서 자사 차세대 운영체제인 '포티OS 6.0'을 비롯한 신제품군을 소개했다.

배 이사가 이날 강조한 단어는 '패브릭'이다. 패브릭의 사전적 의미는 섬유다. 체크무늬로 된 섬유는 양방향 어디로 잡아당겨도 잘 찢어지지 않는다. '보호'라는 측면에서 보안업계에서 자주 사용하는 단어기도 하지만, 포티넷의 보안 기술 비전을 총괄해 부르는 용어가 '보안 패브릭'이기도 하기 때문이다.

보안 패브릭은 취약점 분석 작업 단순화, 신속한 측정 수단 등 현재 보안 상태 분석 기술을 제공하고 보안 모델 표준 준수, 고객 업무 프로세스와 연동 지원 등 주요 비즈니스 서비스와 연계하는 등으로 진화하고 있다.

그는 "결국 가장 중요한 것은 사람"이라며 "보안을 강화하기 위해 보안 솔루션을 구매하는 사람들이 이를 잘 쓰기 위해서는 직관적으로 이해가 빠르게 제품이 구성돼야 한다. 거기에 맞춰서 패브릭도 진화한 것"이라며 내년 신제품과 서비스가 지향하는 바를 짚었다.

포티넷은 내년 패브릭 신제품의 개선점을 크게 세 가지 카테고리로 잡았다. 첫째는 '인지·보호', 둘째는 '탐지·대응' 마지막으로 '복구·분석 보고'다. 이 셋은 미국 국립표준기술연구소(NIST)의 사이버보안 프레임워크 권고에 따른 것이다.

'인지·보호'는 이용자들이 우선 소유 자산을 파악하도록 지원한다는 점에 초점 맞췄다. 아울러 운영 자산별 우선순위와 잠재 위협을 각각 파악하고 비즈니스 서비스에 영향을 주는 위협을 인지토록 한다. 우선순위에 따라 각 자산의 위험을 평가하고 사고 대응 계획을 수립하는 위험 관리계획을 세운 다음 알려진 보안 위협으로부터 보호 시스템을 구현하는 형태로 진행된다.

이와 관련해 내년 새로 선보이게 될 포티OS 6.0은 '가시성 확장' '보호 강화' '감사(Audit) 개선' '추적과 비교'에 중점을 뒀다.

업데이트된 OS에는 사용자 장비가 안드로이드인지 넥서스인지 삼성 갤럭시인지 등 디바이스를 인지할 수 있는 핑거프린트 기술과, 물리적 토폴로지와 논리적 토폴로지를 구분해 전체 네트워크 중 어디가 문제가 있고 어디를 차단시켜야 하는지를 알게 하는 프레임워크가 함께 들어갔다.

아울러 망분리 이슈에 맞춰 악성코드 확산을 막는 보호 기능과 지금까지 '포티게이트' 이용자들이 가장 많이 요청해온 포렌식 기술이 포함됐다. 이는 악성코드를 탐지하는 것에서 끝나는 것이 아닌, 해당 코드가 어떤 기술로 만들어졌는지를 알게 하는 위협정보 추출기능을 뜻한다.

감사 개선 부문에선, '포티가드' 서비스가 데이트된다. 운영자가 원하는 벌크테스트를 할 수 있도록 해당 기능을 템플릿에 녹였다. 각 기업 보안 담당자가 템플릿 기반으로 사이버 공격 시연과 시뮬레이션을 할 수 있게 한 것이다.

자동화된 감사보고서는 포티넷이 가장 역점을 둔 부분이기도 하다. 배 이사는 "특히 갑자기 감사를 시작해서 보고서를 제출하라는 말이 나왔을 때 자동화된 컴플라이언스 감사 보고서가 나오게 만드는게 포티넷이 2018년에 내놓을 '포티OS 6.0'에서 가장 많이 바뀔 키 포인트"라고 강조했다.

"탐지·대응' 부문에서는 로깅, 모니터링, 보고 활성화 등이 포함되는 사전준비와 경계선 탐지, 증거 분석 및 수집과 봉쇄 격리, 복구와 지식 공유 등이 요구된다. 패브릭은 여기에서 시스템 최적화와 범위 확대, 간소화된 절차, 자동화 등이 포함된 '사고 관리' 기능을 제공한다.

이 과정에서 강조되는 부분은 자동화다. 배이사는 "결론적으로는 자동화다. 사람이기 때문에 아침 8시에 출근하고 6시에 퇴근해서 개인 생활을 해야 하기 때문에 어차피 일할 수 있는 시간은 한정돼 있다"며 "모든 것을 자동화 할 수 있는 기능이 템플릿 형태로 6.0에서 제공될 예정"이라고 설명했다.

예를 들어 사내 누군가 갑자기 악성코드를 다운로드했을 경우, 네트워크에서 격리시키는 기능을 기존에는 운영자가 매뉴얼로 클릭해 진행했다면 새 OS에서는 이 과정이 자동화된다. 휴대폰의 트위터 등에서 수신 경보 등을 받아볼 수 있게도 했다.

마지막 '복구·분석'은 보안사고 사후의 문제를 다룬다. 책임의 원천을 찾기 위한 사후 분석 시스템도 자동화된다. 보고서의 경우 보고를 받는 사람이 보기 좋게 파일을 정리해야 하는데 이 부분도 자동화 돼 C레벨 리포트가 작성돼 나온다.

예컨대 "어느 건물 몇 층 사무실의 PC가 잘못되어 보안사고가 난다", "악성코드가 왜 퍼졌는지", "이 PC의 악성코드가 같은 층에서 다른 층으로 퍼졌는지" "어떻게 트래픽이 왔다갔는지"등에 대한 보고도 연간, 일간, 시간당 통계 데이터를 자동화해 보고서에 담는다.

클라우드 부문에선 '포티OS'가 x86/64 서버 하드웨어와 하이퍼바이저를 모두 지원한다. 주요 가상화 플랫폼과 연동 모듈, 커넥터를 지원하는데 VM웨어의 NSX, 시스코 ACI, 오픈스택, 누아지네트웍스 같은 가상화·프라이빗 클라우드와 아마존웹서비스, 마이크로소프트 애저와 애저스택, 구글, 오라클 등이 만드는 퍼블릭 클라우드가 모두 포함된다.


포티넷 클라우드와 가상화 로드맵을 보면 지금까지는 '서비스로서의 보안'을 필두로 원격 관리 서비스인 '포티클라우드 포티게이트', '포티클라우드 액세스 포인트'가 있고, 보안 서비스로서 '포티클라우드 샌드박스' '포티메일 클라우드'가 있다.

그러나 내년에는 기존 솔루션 외에도 원격 관리 서비스로서 '포티클라우드 포티익스텐더&포티스위치'가 추가된다. 보안 서비스로 '포티웹 클라우드', '포티CASB(Cloud Access Security Broker) 클라우드', '포티넷 인증(Authentication)' 등이 더해진다. By

# "방화벽-스위치-무선AP를 한 방에 제어하고 관리하자"

"기업들은 사내 이용자들은 유선과 무선을 자유롭게 액세스하면서도 관리자들은 네트워크상에서 전체적이고 네트워크 보안 정책 집행을 원합니다. 이것이 가능하려면 간편한 네트워크가 필요한데, 현재 기업의 실상은 그렇지 않습니다."

이창운 포티넷코리아 이사는 "기업들은 유무선에 따라 다른 보안 솔루션과 정책을 운영하고 있고 중복투자, 비용 증가의 문제점을 안고 있다"고 이같이 말했다.

실제로 기업들은 임직원 및 파트너에게 유무선 액세스 서비스를 제공하면서 적지 않은 고민을 안고 있다. 얼마나 많은 장비들이 네트워크에 연결돼 있는지, 접속된 장비들이 무엇을 하고 있는지 실시간으로 파악하고 있어야 하기 때문에 유선, 무선 및 보안 관리를 효율적으로 하는 것이 중요하다. 현재는 독립된 개별적인 관리·제어 시스템을 운영 중인데 이는 관리의 복잡성을 야기하곤 했다. 이 때문에 효율적인 방법을 찾을 필요가 있다.

가트너 설문조사에 따르면, 기업들은 네트워크 전반에 걸쳐 공통된 보안, 정책 집행 및 관리를 선호한다. 특히 70% 이상의 응답자들은 액세스 레이어는 단일 벤더를 통해 액세스 레이어 솔루션이 배포되는 것을 선호한다고 답했다.

이창운 이사는 포티넷의 포티게이트와 포티스위치, 포티AP 등 네트워크 장비를 활용하면 '유무선 시큐어 액세스'를 구현할 수 있다고 설명했다.

포티게이트-포티스위치-포티AP를 연결하는 아키텍처를 통해 간단하고 쉽게 네트워크를 확장하면서 보안을 유지할 수 있다는 것이다. 하나의 포티게이트에서 다수의 포티게이트, 스위치, AP에 이르기까지 광범위하게 네트워크 확장성을 제공한다고 이 이사는 강조했다.

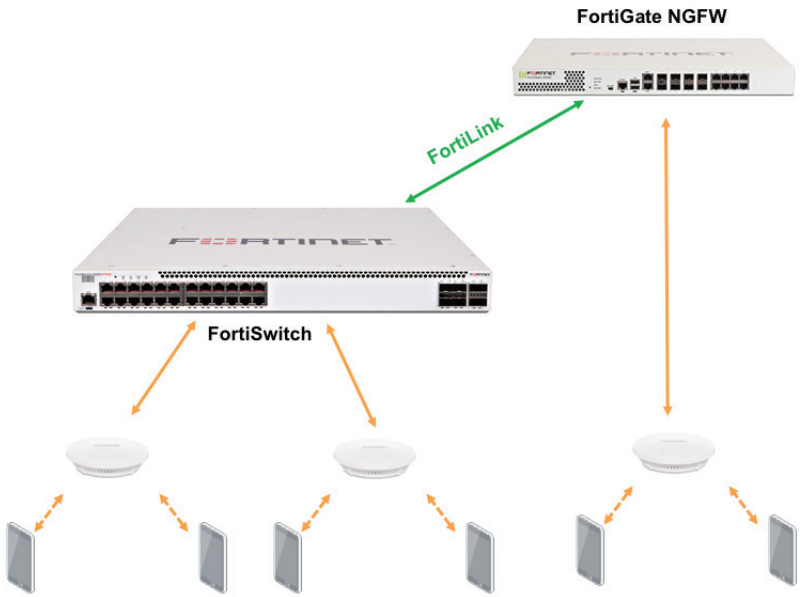
특히 하나의 화면에서 유무선 네트워크에 엑세스한 장비와 사용자를 관리할 수 있다. 이를 위해서는 포티게이트와 포티스위치를 포티링크로 연결한다. 그리고 PoE 스위치 포트에 AP를 연결한다. 이렇게 하면 하나의 대시보드에서 방화벽과 스위치, 무선AP를 모두 관리할 수 있다.

이와 같은 아키텍처를 구성하면 ▲보안 서비스 세트 완성(차세대 방화벽를 중심으로 네트워크·서비스 확장) ▲스위치 구성 및 제어(포티링크 프로토콜로 통합된 통합 스위치 관리) ▲AP 구성 및 제어(최고의 성능과 간편한 구축) ▲단일창을 통한 관리(무선, 유선 및 보안 통합 관리와 사용자 제어) 등의 장점을 누릴 수 있다.

이 이사는 "고성능 무선은 필수적으로 필요하지만 무선랜 서비스를 위해서는 이것만으로 충분하지 않고, 강력한 스위치도 필수적으로 필요하지만 통합 액세스를 위해서는 그것만 있어서도 안된다"면서 "포티넷 유무선 시큐어 액세스는 모든 네트워크 서비스 구현 및 배치에 대한 최소 요구사항"이라고 말했다.

그는 "모든 포티게이트 제품에서 추가 비용없이 엔터프라이즈 무선랜 및 스위치를 관리할 수 있고, 단일 플랫폼에서 무선, 스위칭, 보안, 사용자 제어 서비스 제공하면서 포티넷의 보안 패브릭 통합을 통한 가시성을 제공한다"면서 "포티게이트 통합 솔루션은 다중 플랫폼과 다중 관리 애플리케이션 구축을 통해 복잡성 및 보안 위협을 제거한다"고 강조했다. By

[그림 1] 포티넷의 유무선 시큐어 액세스의 차별점



FORTINET®

# 디지털 전환의 시대, 기업 사이버보안 해법


By BylineNetwork

**발행** | 바이라인네트워크
**배포** | https://byline.network/
**취재/글** | 이유지 기자 yjlee@byline.network
심재석 기자 shimsky@byline.network
남혜현 기자 smilla@byline.network
**문의** | byline@byline.network



FORTINET®

**솔루션 문의처**

**포티넷코리아**
**주소** | 서울특별시 강남구 영동대로 325(대치동, 해암빌딩 14/15층)
**전화** | 080-559-8989
**이메일** | kr-callcenter@fortinet.com
**홈페이지** | http://kr.fortinet.com
**페이스북** | https://www.facebook.com/fortinetkorea