AKAMAI 고객 사례

Kaneka Corporation

Secure Internet Access Enterprise를 사용해 보안 체계를 강화하고 인터넷으로 직접 연결되는 트래픽을 보호하는 Kaneka Corporation

그룹 전체에 걸쳐 보안 강화

Kaneka는 화학 제품, 의약품, 식품, 의료 장비, 전자 소재 등 광범위한 재료와 제품을 제조하고 판매하는 종합 화학 제조업체입니다.

도쿄와 오사카에 본사가 있고 직접 채용한 직원 3500명과 그룹사 전체 직원 1만여 명을 두고 있습니다.

Kaneka는 IoT Solutions Center 한 곳에서 회사 전체의 정보 시스템과 보안을 감독하고 있습니다. 이 센터는 비즈니스 솔루션 그룹 책임자인 테츠로 야부키(Tetsuro Yabuki)의 리더십 아래, 2011년 Microsoft 365를 전사적으로 도입했을 때부터 '클라우드 퍼스트(cloud-first)' 정책에 따라 SaaS/PaaS 사용과 가상화된 서버의 중앙 집중화를 적극 추진해 왔습니다. 현재 Windows 기반 서버의 약 90%가 Microsoft Azure 또는 프라이빗 클라우드 환경에 배치되어 있을 뿐 아니라, 핵심 비즈니스 시스템 인프라에 하이브리드 클라우드 설정도 사용되고 있습니다.

IoT Solutions Center는 클라우드 퍼스트 IT 혁신을 추진하면서 구체적인 문제를 해결하고 있으며, 주요 사안은 Kaneka 그룹 전체의 보안을 강화하는 것입니다.

간편하고 빠른 글로벌 배포

야부키는 Kaneka에서 오랫동안 심각한 사이버 보안 인시던트가 발생하지 않았기 때문에 사이버 공격에 대해 별로 염려하지 않았고 전반적으로 보안 의식도 부족했다고 설명합니다.

야부키는 "그런데 2017년에 예상치 못한 보안 인시던트가 잇따라 발생하면서 완전히 달라졌습니다.

각각의 보안 인시던트는 심각하지 않았지만 사이버 리스크가 존재한다는 점이 분명히 드러나면서 IoT Solutions Center에서 최대한 빨리 문제를 해결해야 했습니다. 우리는 Kaneka의 보안 체계를 포괄적으로 강화하기 위한 계획을 마련하고 해외 지사를 포함해 그룹 전체의 보안 거버넌스를 개선하는 정책을 수립했습니다."라고 말합니다.

Kaneka Corporation
일본 도쿄
www.kaneka.co.jp/

업계
리테일 & 소비재

솔루션
Secure Internet Access Enterprise

주요 결과

- 간단한 DNS 변경으로 2개월 만에 글로벌 아웃바운드 웹 트래픽 보안 개선
- 인터넷 직접 연결을 사용하는 지사를 빠르게 보호
- 감염된 엔드포인트 디바이스를 선제적으로 탐지 및 차단

야부키의 포괄적인 사이버 보안 계획은 아웃바운드 및 인바운드 네트워크 트래픽의 위협과 엔드포인트 디바이스에 영향을 줄 수 있는 위협에 대한 보안 체계를 강화하는 것을 포함합니다. 이미 엔드포인트 보안 플랫폼과 엔드포인트 탐지 및 응답 솔루션을 선택한 Kaneka는 아웃바운드 트래픽에 대한 보안 레이어를 추가해 이를 보완할 방법을 찾고 있었고, Akamai의 클라우드 기반 보안 솔루션인 Secure Internet Access Enterprise를 추가 보안 레이어로 구축하기로 결정했습니다.

Secure Internet Access Enterprise 서비스는 Akamai의 광범위한 실시간 위협 인텔리전스를 사용해 악성 DNS 쿼리를 Akamai Intelligent Edge Platform으로 리디렉션하는 간단한 방법을 통해 악성 트래픽을 선제적으로 차단합니다. 이를 통해 회사 디바이스가 악성 웹사이트와 명령 및 제어(C2) 서버에 연결되는 것이 선제적으로 차단되기 때문에 회사 디바이스가 피싱 또는 멀웨어에 감염되어 회사 정보가 유출되는 리스크가 크게 줄어듭니다. 위협 인텔리전스가 지속적으로 자동 업데이트되기 때문에 관리자가 수동으로 개입할 필요가 없습니다.

전반적인 보안 조치를 책임지고 있는 비즈니스 솔루션 그룹의 매니저인 게이지 후지모토(Keiji Fujimoto)는 Secure Internet Access Enterprise를 도입한 이유를 다음과 같이 설명합니다.

"Secure Internet Access Enterprise를 선택하게 된 한 가지 이유는 보안을 유지하는 방법으로 DNS를 사용한다는 것이 혁신적이고 간편하기 때문입니다. 정말 독보적입니다. 세계 최대 DNS 제공업체인 Akamai만이 제공할 수 있는 솔루션이라고 생각합니다. Akamai의 강점을 전문적으로 활용하는 획기적인 클라우드 보안 서비스인 것 같습니다."

또한 후지모토는 Secure Internet Access Enterprise가 Kaneka의 아웃바운드 트래픽 보호 요구사항에 완벽하게 부합되었다고 생각합니다.

"이 사이버 보안 계획의 범위는 Kaneka 그룹 전체에서 보안 조치를 통합하고 보안 거버넌스를 개선하는 것도 포함하는데 쉽고 간편하게 도입할 수 있는 Secure Internet Access Enterprise 덕분에 이러한 보안 조치를 빠르게 배포할 수 있었습니다. 또한 Secure Internet Access Enterprise가 회사 네트워크 구조와 상관없이 악성 통신을 차단하는 것을 보고 놀랐습니다."

2개월 만에 해외 지사에 배포 완료

Kaneka는 이미 Secure Internet Access Enterprise를 사용해 회사 네트워크의 이그레스 포인트를 보호하고 있으며 일본과 해외의 그룹사에 솔루션 구축을 거의 완료했습니다.

Kaneka 해외 지사 및 본사의 정보 시스템은 4개 지역, 즉 북미 및 남미, 유럽 및 아프리카, 말레이시아, 일본 및 아시아에 분산되어 있습니다. 일본에서 보안 거버넌스를 강화하기 위해 시스템을 선도적으로 구현하자 다른 3개 지역을 담당하는 정보 보안 팀이 일본을 따라 Secure Internet Access Enterprise를 전 세계적으로 배포했습니다.

후지모토는 "전 지역에 걸쳐 Secure Internet Access Enterprise를 구축하는 협력 작업은 어렵지 않았습니다. 사실 구현이라고 할 것도 없이 리커시브 DNS 쿼리 대상을 변경하기만 하면 됩니다. 그래서 해외 구현도 순조롭게 진행되어 두 달 만에 완료할 수 있었습니다."라고 회상합니다.

> DNS를 보안 수단으로 사용한다는 개념은 혁신적이면서 논리적입니다. 이는 Akamai 같은 기업만이 제공할 수 있는 솔루션입니다.
>
> **게이지 후지모토(Keiji Fujimoto)**
> Kaneka Corporation IoT 솔루션 센터 비즈니스 솔루션 그룹 매니저

인터넷 직접 연결 보호

일본에 있는 그룹사들의 경우 야부키와 그의 팀이 Kaneka 데이터 센터를 사용하지 않는 (즉, 별도의 환경에서 시스템을 운영하고 별도의 인터넷 직접 연결 이그레스 포인트를 갖고 있음) 회사들을 방문해 협력을 이끌어냈습니다.

Kaneka에 Secure Internet Access Enterprise를 배포하는 것 외에도 이제 Secure Internet Access Enterprise를 사용해 인터넷에 직접 연결하는 지사에서 아웃바운드 트래픽을 보호하고 있습니다.

후지모토는 "Kaneka는 현재 일부 지사에서만 직접 인터넷 연결을 허용하고 있지만 이러한 지사의 아웃바운드 트래픽을 보호할 방법이 필요했습니다. Secure Internet Access Enterprise를 통해 아주 쉽게 보호할 수 있어서 정말 다행입니다."라고 말합니다.

감염된 디바이스를 신속하게 탐지

Kaneka 그룹 전체에 Secure Internet Access Enterprise가 도입되고 Kaneka와 모든 그룹사가 이제 모든 디바이스에서 악성 웹사이트와 C2 서버로의 통신을 선제적으로 차단함에 따라 IoT Solutions Center에서 악성 통신을 하는 모든 디바이스를 신속하게 탐지하고 확인할 수 있습니다. 결과적으로 모든 Kaneka 그룹사의 위험한 디바이스에 대해 즉각적인 조치를 취할 수 있게 되었다고 야부키는 말합니다.

야부키는 "그룹에 위험한 디바이스가 하나만 있어도 잠재적으로 큰 문제로 발전할 수 있습니다. Secure Internet Access Enterprise를 통해 그룹 전체에서 이러한 디바이스를 탐지할 수 있게 된 것은 큰 도움이 되었습니다."라고 말합니다.

가끔 기업의 누군가가 오랫동안 사용하지 않은 디바이스를 사용하기 시작하면 그 디바이스가 위험한 디바이스로 탐지된다고 후지모토는 덧붙입니다.

야부키는 "멀웨어에 감염되어 정보 시스템 부서의 통제를 벗어난 오래된 디바이스를 모르고 사용하는 경우가 있습니다. Secure Internet Access Enterprise 사용 시 또 다른 장점은 이 같은 보안 리스크가 발생할 때 위험한 디바이스를 신속하게 탐지해 디바이스의 통신을 차단하고 디바이스를 중지할 수 있다는 점입니다."라고 설명합니다.

야부키는 또한 "보안 조치는 비즈니스의 핵심 구성요소입니다. 따라서 우리는 매출 규모와 평판에 맞춰 보안에 투자해야 한다고 생각합니다. Kaneka에서 사이버 보안 인시던트들이 갑자기 발생한 이유는 최근 프로모션 활동으로 인지도가 크게 높아진 데 따른 것으로 보입니다. 기업의 가치가 높아질수록 당연히 사이버 리스크도 커집니다. 그렇기 때문에 회사 가치를 보호하기 위한 조치를 지속적으로 개선하면서 Secure Internet Access Enterprise 같은 혁신적인 기술을 집중적으로 활용하는 것이 중요합니다."라고 말합니다.

Kaneka는 1949년 9월 Kanegafuchi Spinning Company, Ltd.에서 분리되면서 설립되었습니다. 창립 당시 회사명은 Kanegafuchi Kagaku Kogyo Co., Ltd.였으며 2004년에 현재 사명으로 변경되었습니다. 폴리염화비닐인 카네비닐(Kanevinyl)을 개발하며 화학 제품 제조업체로 시작했으며, 현재 광범위한 화학 제품, 기능성 수지, 발포 수지, 식품, 의약품, 의료 장비, 전자 소재, 태양 전지, 합성 섬유를 제공합니다. 최근에는 환원형 코엔자임 Q10 같은 건강 보조 제품을 제공하고 제빵용 우유 같은 유제품을 제조하고 판매하는 등 세상을 건강하게 만드는 기업이라는 비전을 확대하여 100% 해수에서 생분해되는 생분해성 고분자 PHBH를 개발하는 등 지구 환경 보존에도 기여하고 있습니다. https://www.kaneka.co.jp/.