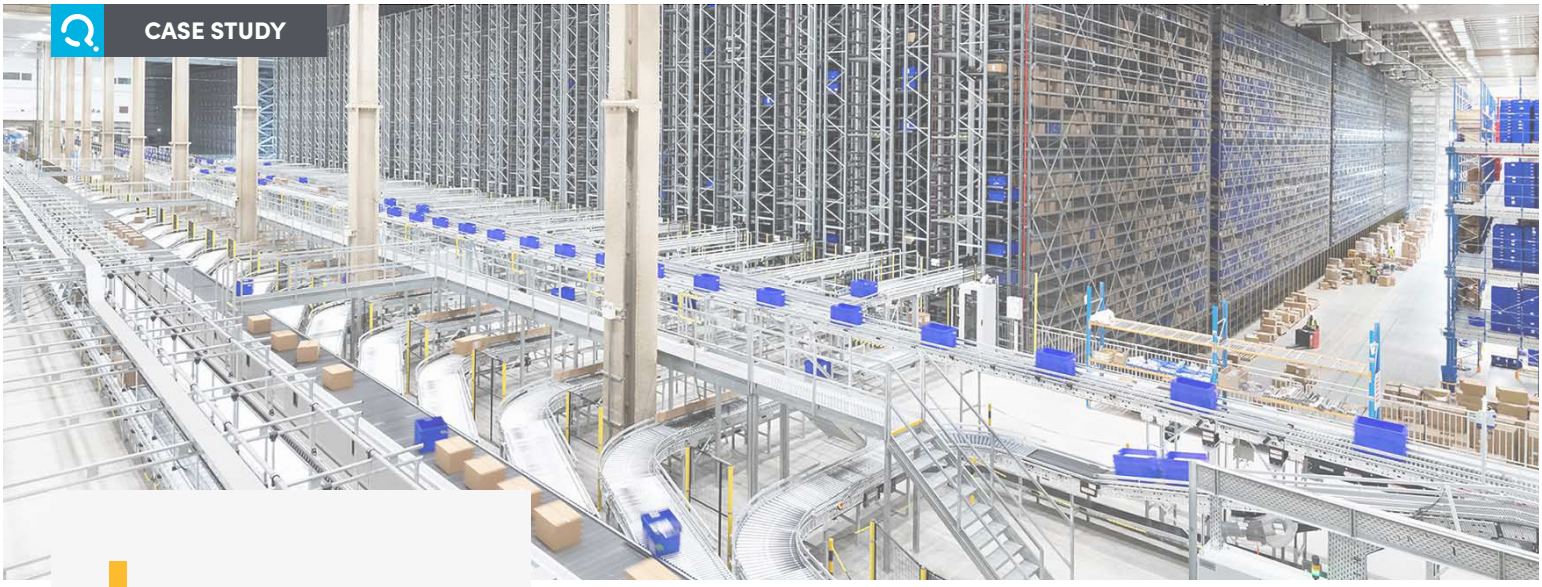
CASE STUDY



DEMATIC

Dematic stregthens its secrity posture with cloud-native Azure network security services

QUISITIVE CLIENT
Dematic

SECTOR
Manufacturing

IN THIS CASE STUDY

- Azure API Management
- Azure DDoS Protection
- Azure Firewall
- Azure Front Door
- Azure Web Application Firewall
- Microsoft Defender for Cloud

Dematic helps keep the world moving. Part of the KION Group, the Atlanta-based company designs, builds, implements, and supports automated system solutions that optimize the supply chain. As it creates these customized solutions to maximize efficiency for customers, Dematic needs a robust, efficient, and flexible security solution to protect sensitive client information and services.

Delivering highly secure supply chain services

Dematic takes pride in its position as a leading supplier of integrated automated technology software and services for warehouses, distribution centers, and production facilities. It has installed more than 6,000 systems of all sizes and levels of complexity, from lower-cost manual options to fully automated systems. It has more than 7,000 employees worldwide and 60 engineering centers in 25 countries.

Since Dematic works with a wide range of customer facilities, from e-commerce and apparel to groceries and healthcare, it constantly creates customized solutions—and the security for those services—to fit customer requirements. The breadth of customization makes it challenging to standardize and scale security services like firewalls, which provide advanced threat protection for sensitive and regulated environments.

Dematic needed a security solution with flexibility, scalability, and cloud-native integration. "We have a responsibility to our customers to protect their data and processes," says Kevin Boutin, Principal Architect at Dematic. "Trust isn't something that happens on its own, so Dematic must proactively demonstrate a variety of mitigation efforts we take to increase security. We need the right tools to effectively demonstrate this."

Many Dematic customers work in sectors such as government and healthcare, which require especially rigorous security to protect sensitive information. As you can see, the security stakes are high in the supply chain. A security

incident for a Dematic customer could lead to a mechanical equipment failure that harms people in a warehouse or supply chain delays that cost companies millions of dollars per hour.

Delivering highly secure supply chain services

Dematic knew early on that it wanted to use Microsoft Azure. Since Dematic already used Microsoft cloud-native services internally, the company wanted a cloud-native approach to security for its customer-facing services.

Microsoft created a proof of concept for Dematic, which successfully met the flexibility and scalability requirements for Dematic to deliver highly secure services to customers.

Dematic ultimately selected the Premium tier of Azure Firewall along with the Premium tier of Azure Front Door, the Standard tier of Azure DDoS Protection, Azure API Management, Azure Web Application Firewall, and Microsoft Defender for Cloud.

Dematic partnered with Catapult Systems, a Microsoft Gold partner with specialty certification in cloud security, to deploy the Azure security products, especially Azure Firewall Premium. Dematic also used Microsoft FastTrack in the early stage of its development cycle.

With Azure Firewall Premium features like an intrusion detection and prevention system (IDPS) and transport layer security (TLS) inspection, Dematic can prevent zero-day threats, malware, and viruses from spreading across networks. Dematic uses Azure Firewall Premium for IDPS, TLS inspection, and URL filtering capabilities.

Dematic uses Azure Front Door, a cloud content delivery network service that delivers high performance, scalability, and more secure user experiences. Specifically, Azure Web Application Firewall (WAF), which is attached to Azure Front Door, protects Dematic's customer-facing web applications from web-based attacks and malicious bots. It uses Azure DDoS Protection for network protection and rapid response to denial-of-service attacks. With recommendations from Microsoft Defender for Cloud, Dematic continually strengthens the overall security posture of its environment and protects workloads from evolving threats.

"With Defender for Cloud, we can set security policies and automatically generate compliance reports for the standards that we need to meet for customers," says Brandon Bates, Principal Architect at Dematic. "It gives Dematic and our customers peace of mind when we show that we meet security standards."

> "Cloud-native scaling in Azure Firewall Premium is incredibly important to us. Not only do we remove single points of failure from our architecture, but we also get high availability and uptime of 99.99 percent, which helps us meet service level agreements with our customers."
>
> **KEVIN BOUTIN**
> Principal Architect, Dematic

And with Azure API Management, Dematic has a single place from which to manage APIs for security and more.

"We have centralized where our DevOps, Security Ops, and other users would go to troubleshoot anything related to deployment," Boutin says. "Bringing all these different services into Azure makes our lives easier."

Scalability for meeting customer needs

With Azure Firewall Premium, Dematic can easily and quickly help protect any new data conduits for customers instead of having to seek out the technical expertise needed to do so. It is just one way that Dematic uses cloud-native tools to make security easier.

"Cloud-native scaling in Azure Firewall Premium is incredibly important to us," Boutin says. "Not only do we remove single points of failure from our architecture, but we also get high availability and uptime of 99.99 percent, which helps us meet service level agreements with our customers."

Dematic enjoys on-demand pricing for its security tools, so it only has to pay for what it needs as it creates, tests, and releases products for customers.

"During our production cycles, we offer beta tests for sales groups and decision-makers, but we don't want to be locked into paying for a certain amount of usage," Bates says. "With on-demand pricing in the Azure products that we use, we only pay for what we need at any given time."

Dematic still has the flexibility to use third-party products like Terraform, an open-source infrastructure as code software, for its deployments in Azure. Dematic uses infrastructure as code in the deployment and maintenance of security solutions, so its teams can test applications in production-like environments early in the development cycle.

A more confident security posture

Dematic is confident that its cloud-native Azure network security solutions work around the clock to help prevent and detect any security issues. Now, Dematic can focus on delivering the best services to customers instead of worrying about its security posture and the detailed day-to-day workings of a firewall.

Dematic can use its strong security posture to show new customers the multiple layers of protection in place to help keep their data more secure.

"Our expertise is in developing applications with really easy-to-use interfaces that bring together data, analytics, AI, and other innovative capabilities," Bates says. "Understanding the inner workings of a firewall is not our expertise, and with Azure Firewall Premium, it doesn't have to be. We use Azure Firewall Premium to protect Dematic and our customers around the clock, and we can depend on it."

"Understanding the inner workings of a firewall is not our expertise, and with Azure Firewall Premium, it doesn't have to be. We use Azure Firewall Premium to protect Dematic and our customers around the clock, and we can depend on it."

BRANDON BATES
Principal Architect, Dematic