SOPHOS

CUSTOMER CASE STUDY

Del Monte Foods Chooses Consistent, Flexible, and Scalable Security for Its Cloud-First Strategy

Customer-at-a-Glance

Del Monte Foods, Inc.

Industry
Consumer food products

Number of Users
7,000 employees

Sophos Solutions
Sophos Synchronized Security
Sophos Intercept X Advanced with EDR
Sophos Intercept X Advanced for Server
Sophos Central Web Protection Advanced
Sophos Central Device Encryption
Sophos RED (Remote Ethernet Device)
Sophos XG Firewall
Sophos Technical Account Manager (TAM)

'Ever since we switched to Sophos, we have not experienced any endpoint problems.'

PJ Balsley
Director, IT Technology, Security, and Operations
Del Monte Foods, Inc.

Del Monte Foods, Inc. is a food production company and a household name with a long history in the food industry, promoting recognizable brands like Del Monte®, Contadina®, College Inn®, and S&W®. In 2014, Philippines-based food producer Del Monte Pacific Limited acquired Del Monte's consumer food business. With its state-of-the-art research center and headquarters in the Bay Area, the long-established organization values innovation and stays on top of the latest technology trends to further its business goals. Del Monte takes pride in its brand and its culture, which is driven by a strong work ethic, mutual support, and the spirit of collaboration. Del Monte owns and operates 10 food production facilities, three distribution centers, and multiple offices across the U.S., as well as two production facilities in Mexico.

PJ Balsley, director of IT technology, security, and operations, calls Del Monte "the 100-year-old start-up"—and for good reason. From an IT perspective, as he points out, Del Monte's infrastructure is only a few years old. When the consumer food business was sold, the IT infrastructure had to be built from scratch by its lean IT team of six, as no technology resources were inherited from the parent company. Shortly after the sale, the IT team spent time laying the groundwork. They developed policies and set a standards framework for all systems—workstations, servers, network equipment, and other devices—detailing what access, activities, and applications were permitted and even defining encryption policies at a granular level. After the foundational work was completed internally, the company made a decision to outsource 98% of its IT functions to an extended team of approximately 130 people to a global IT provider.

Challenges

- Provide consistent, flexible, and scalable security to multiple locations, large and small, across North America
- Identify a vendor that could provide compatible and complete protection for a 100% cloud-enabled organization
- Defend valuable intellectual property and other vital corporate data residing in the cloud against ransomware and advanced malware attacks
- Ensure that all users—regardless of location—are productive and safe, while the IT team enjoys continual visibility across the entire technology infrastructure
- Maintain a diligent security strategy while maximizing finite IT resources

What role does security play in a cloud-first corporate environment

At the forefront of technology trends, Del Monte leveraged the cloud and centralized management capabilities to support its business needs and technical requirements. While this strategy has been extremely beneficial for increasing the organization's agility, it has also made the IT team highly security conscious and proactive about protecting endpoints, the network, and sensitive corporate data, such as its valuable intellectual property, which resides on external cloud platforms.

For Balsley and his team, security is always a balancing act. "We're not a technology company, but, similar to most other organizations, we rely heavily on technology to run our core business. Any disruptions that prevent someone from doing their job efficiently is an immense problem," he says. "On the IT side, we evaluate solutions incredibly carefully before we deploy them. We are continually asking ourselves whether those solutions are truly beneficial to the organization or whether they will create problems that interfere with productivity," he says.

Del Monte needed a vendor that would meld seamlessly with its cloud-first strategy, provide transparent protection for its diverse user base across multiple locations, and enable the IT team to fulfill its rigorous security requirements.

How does an organization with multiple offices and mobile workers protect its valuable IP and assets?

The IT team was well aware that Del Monte's valuable research and intellectual property (IP) made it a target of choice for adversaries. They knew that attacks could potentially put Del Monte's vital corporate data at risk and result in business downtime. Balsley and his team made the decision to adopt Sophos when the company was hit with a series of advanced malware and CryptoLocker ransomware attacks, which the legacy endpoint solution was unable to block.

Balsley and his team first deployed Sophos Central Endpoint Protection. The solution provides Del Monte with a broad spectrum of endpoint protection: signatureless malware detection, host intrusion prevention, category-based web filtering—enforced both on and off the corporate network—application control, peripheral control to manage access to removable media and mobile devices, and data loss prevention to restrict unauthorized data flow. The centralized cloud-based management console is intuitive, easy to use, and a perfect fit for Del Monte's cloud infrastructure.

"Ever since we switched to Sophos, we have not experienced any endpoint problems. We take an aggressive approach and turn on all the features and capabilities for that extra measure of protection. Our team no longer spends the entire day monitoring endpoints, or continuously examining log files. With Sophos, we know our endpoints are healthy and operating as they should. I feel very comfortable that our endpoints are well protected," asserts Balsley.

The team also added Sophos Intercept X Advanced to block and remove residual ransomware from previous attacks and prevent future attacks. Sophos Intercept X Advanced safeguards endpoints against known and unknown threats through its signatureless exploit prevention, deep learning malware detection, and advanced ransomware protection.

"We haven't had any CryptoLocker issues since our Sophos deployment. Intercept X excellently blocked infected files and reverted those files back to their previously known good state. We've seen it first-hand - Intercept X does an impressive job at cleaning up previous threats," relates Balsley.

Another facet of Del Monte's uncompromising data protection plan was to prevent users from saving and sharing vital company data on USB drives that were not encrypted. Sophos Intercept X Advanced provides them with a level of control that enables them to permit only approved, encrypted storage devices. The team took it a step further with Sophos Central Device Encryption, which they deployed over the air with just a few clicks. Now all of Del Monte's systems, even remote laptops, have full-disk encryption.

As a result, Balsley now knows that encryption requirements for protecting sensitive data are being completely met. An established company with brand

'Sophos XG Firewall provides the next generation protection the team and I needed, especially when you deploy the Sophos Firewall with Intercept X Advanced.'

PJ Balsley
Director, IT Technology, Security, and Operations
Del Monte Foods, Inc.

equity like Del Monte is especially concerned about maintaining compliance to preserve the reputation it has worked so hard to build over the years.

"We're an extremely dispersed and mobile organization, with approximately 40 locations—ranging from large production facilities to remote small offices or home offices—so it's imperative we encrypt everything. Sophos Central Device Encryption is an exceptional product for us. It was easy to roll out full-disk encryption to all devices and then monitor, audit, and enforce policies to ensure that all users, even those with administrative access, weren't disabling hardware encryption on their computers," declares Balsley.

With Del Monte's departments handling sensitive data, users needed secure access, something the legacy solution was unable to provide. Sophos Central Web Protection Advanced allows users to safely access authorized Internet-based locations so they can do their jobs while preventing them from going to unapproved sites.

Rounding out Del Monte's security posture is Sophos Intercept X Advanced for Server. Del Monte's data center consists of a mixture of Linux and Windows servers, which house business-critical applications. The IT team exercises strict change control over the servers, which are locked down and regulated by complex firewall rule sets. Even though they are at incredibly low risk of infection, Sophos security is nevertheless mandatory. Sophos Intercept X Advanced for Server secures these systems from attacks using a combination of traditional and next-generation techniques, including CryptoGuard anti-ransomware, WipeGuard for MBR, exploit prevention, deep-learning, malicious traffic detection, and server lockdown for application whitelisting.

How do you choose the right, next-generation firewall for your organization?

To safeguard the network, Balsley and his team are currently in the process of deploying Sophos XG Firewalls and Synchronized Security. Prior to signing on with Sophos, Del Monte relied on an MPLS provider for Internet connectivity at its branch and remote locations. The IT team had no visibility at all into network activity, and reporting was non-existent. "I didn't have the proper visibility into our network security at the time, and that was certainly terrifying because we had no perspective or holistic understanding on what was going on," recalls Balsley.

When evaluating firewalls, the IT team was looking for a cost-effective solution that could handle the moderate volume of network traffic while offering next-generation capabilities for the best possible level of security. In comparison, competitive firewalls tended to be overly and unnecessarily complex, while other firewalls were costly and were much more than Del Monte needed, especially when associated with proposed benefits.

Sophos XG Firewalls and RED devices were the logical choice. Sophos XG Firewalls provide Balsley and his team with visibility they never had before—

into the network, users, and applications—directly from the control center. Now the team can resolve any potential issues before they become problems. Sophos XG Firewalls check all the boxes on the team's wishlist—and then some—with intrusion prevention system (IPS), advanced threat protection (ATP), sandboxing, dual antivirus, web and application control and visibility, antiphishing, and a full-featured web application firewall. "Sophos XG Firewall provides the next generation protection the team and I needed, especially when you deploy the Sophos Firewall with Sophos Intercept X Advanced," summarizes Balsley.

How does Synchronized Security coordinate and enhance incident response and remediation?

Synchronized Security, which leverages unique Sophos Security Heartbeat™ technology to enable endpoints and firewalls to communicate and share threat intelligence, is a unique capability of Sophos XG Firewall that Balsley did not necessarily seek out but was impressed with when he saw it in action. Synchronized Security immediately identifies the source of a potential threat and automatically isolates compromised systems. The goal of isolating compromised systems is to ensure the spreading of the infection is eliminated, while allowing the team to focus on proper processes with decreased incident response time. "When I learned more about Synchronized Security, I was definitely impressed. It's truly a cutting-edge solution. My first reaction was, 'We need this'," he remarks.

Synchronized Security alerts his team whenever there is an issue for any number of reasons. "Sophos Synchronized Security lets us know when there is a threat at the endpoint or the edge and if any compromise has taken place. Our team can then proactively monitor and remediate issues more quickly," indicates Balsley.

While Balsley feels confident that corporate workstations are well-secured with Sophos endpoint technology, he is concerned about potential risks introduced by unmanaged devices, such as printers, personal devices, tablets, smart TVs, and switches. "My biggest fears revolve around systems we don't know about. With Synchronized Security, we have more control over these devices than we ever had before. It gives us unprecedented visibility across our entire environment. The firewalls monitor devices I don't know about, and the endpoint protection controls devices I do know about. Now I can keep an eye on everything cohesively and receive notifications about potential issues so that we can research them and get to the bottom of them immediately," he explains.

The IT team at Del Monte continues to fine-tune their security architecture and looks for ways to make their team more efficient and effective. Balsley has extended his existing Sophos Premium Support service to include a technical account manager (TAM). Having access to a Sophos expert helps provide insights, assist with faster problem resolution and case escalation, and free up his staff to work on more strategic projects.

"The greatest benefit of working with a Sophos TAM is that it allows us to continually tune the environment and turn it into a well-oiled machine, where everything runs smoothly and even the small issues are addressed," states Balsley.

He also sees the value in the intelligent enterprise detection and response (EDR) technology built into the latest version of Sophos Intercept X Advanced. EDR provides guided investigation tools, allowing security teams of any skill level to gain a better understanding of their organization's security postures. This means the IT team can focus on the business of IT instead of chasing false positives and dealing with overwhelming volumes of alerts. It's another way for Del Monte to add this capability with a limited headcount.

As Balsley points out, Sophos is the ideal fit for a cloud-based organization like Del Monte that wants to use the best possible tools to advance their aggressive and broad-ranging security strategy and fully protect its users, devices, and most importantly, its data and IP.

According to Balsley, "We wanted to deploy the same technology across the board, so that it's consistent, flexible, and scalable for all our locations, large and small. Sophos makes that possible. The cloud-managed platform and centralized management console gives us complete visibility over the entire organization. It's especially advantageous for us because we have a small staff. Our team can easily monitor all the alerts and resolve them efficiently, regardless of where users work."

At the end of the day, Balsley knows he and his team made the right choice for Del Monte. "We wanted a security vendor that understood our needs between multiple sites as they all have different requirements. Sophos made sense from a price perspective but more importantly we were looking for best of breed products – security solutions on the market that could fit our needs most completely and scale with us. We wanted strong security that was invisible to the user – and we were able to get that Sophos. We've seen it work well for us as we have Sophos on both our endpoints and network. Having the endpoints and firewall speak to each other is an added bonus, and that is something no other vendor provides."

'We wanted to deploy the same technology across the board, so that it's consistent, flexible, and scalable for all our locations, large and small. Sophos makes that possible.'

PJ Balsley
Director, IT Technology, Security, and Operations
Del Monte Foods, Inc.

Start your free trial of Sophos Central today to get started with Synchronized Security.

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North America Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

SOPHOS

2019-05-01 CSNA (RP)