GRUPO BIMBO®

NOURISHING A BETTER WORLD

Grupo Bimbo protects its global connected supply chain with Palo Alto Networks

RESULTS

Twice the insurance coverage

Company's insurance coverage doubled without insurers raising the premium

Days to one hour

reduction in mean time to resolution

$100,000

in monthly connectivity cost savings in one country alone

paloalto® NETWORKS

Grupo Bimbo, the world's largest baker, boasts an impressive portfolio of brands consumed by billions of people each day. Brands including Grupo Bimbo, Sara Lee, Sun-Maid, and Oroweat, which generate $20 billion in revenue. Simple, connected Palo Alto Networks platforms safeguard food production worldwide, ensuring the uninterrupted supply of baked products to millions of consumers every day.

Grupo Bimbo chose to consolidate its security footprint with a suite of Palo Alto Networks platforms. As a result, they are driving down risk, reducing complexity, and automating multiple security processes.

An innovative Zero Trust security strategy for OT devices is being rolled out to support uninterrupted baking in more than 200 bakery plants worldwide. Direct-to-app connectivity is saving $100,000 in monthly savings in Grupo Bimbo's Colombian operation, and the mean time to detect and respond has been reduced from weeks to minutes. This forward-thinking cyber strategy is so resilient that Grupo Bimbo's insurers have doubled the company's insurance coverage without increasing the premium.

IN BRIEF

Challenge

- Modernize legacy security infrastructure. Disconnected, siloed platforms increased risk, reduced productivity, and led to rising operational costs.
- Reduce attack surface without negatively impacting performance or hybrid-user experience. Legacy VPN was complex to use and sapped performance.
- Prevent cyberthreats from impacting IoT networks and causing food production downtime or failure.

Solution

Platformization with Palo Alto Networks®:

- Next-Generation Firewalls powered by Precision AI™ with IoT/OT security for multiple environments, including their OT
- Cloud-Delivered Security Services:
  - DNS Security
  - WildFire®
  - Threat Prevention
  - URL Filtering
- Prisma® SASE
- Prisma® Cloud
- Cortex XDR®
- Cortex XSOAR®
- Cortex Xpanse®
- Unit 42® Incident Response
- Unit 42® Retainer

Results

- Reduction in mean time to resolution from days to one hour.
- Protects OT and uninterrupted bakery supply.
- Reduced monthly connectivity costs by $100,000 in one country.
- Insurers doubled company's insurance coverage without raising premium.
- BlackCat incident stopped within hours through Cortex XDR.

CHALLENGE

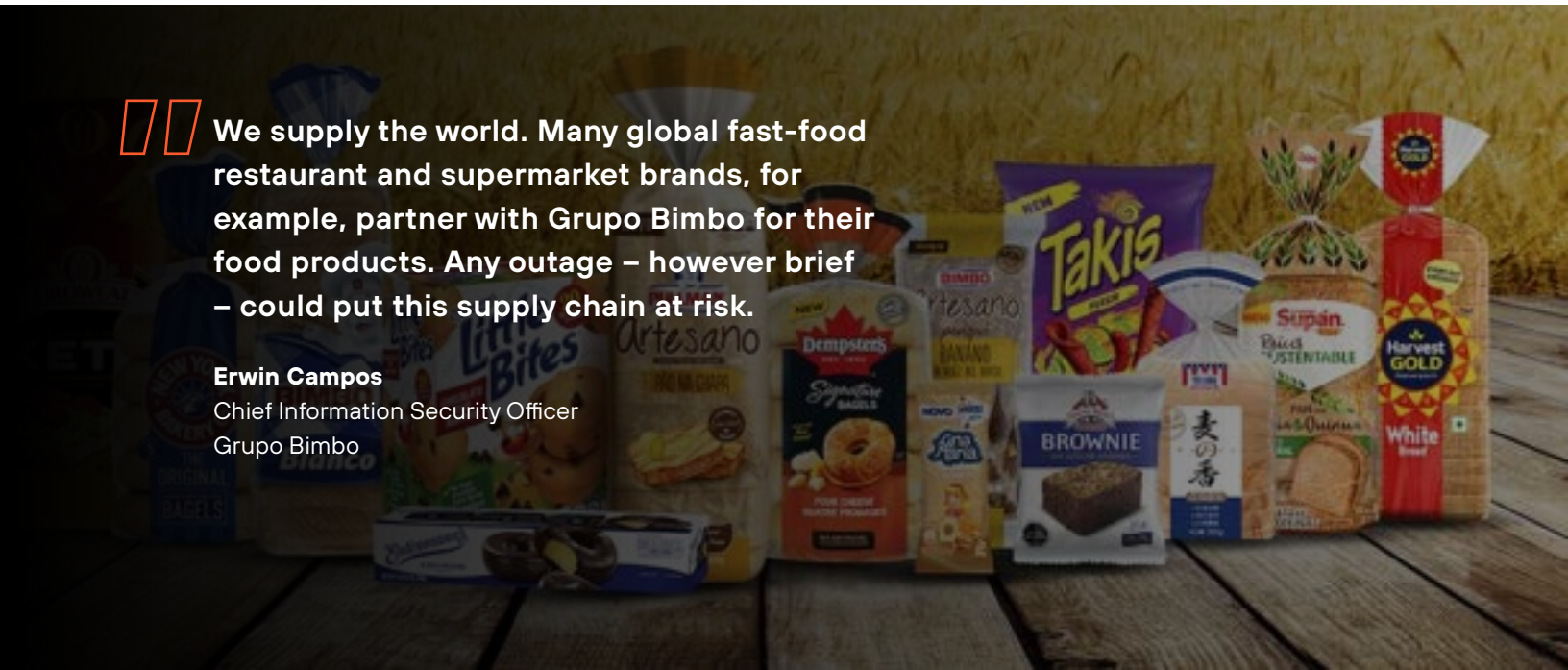
Nourishing the world with bread, buns, and bagels

Grupo Bimbo is thriving. The Group is Latin America's most popular food brand and one of the fastest-growing food companies in the US. Cybersecurity is an essential ingredient for this growth. "We need to keep the bad guys out of our network," explains Erwin Campos, Chief Information Security Officer (CISO), Grupo Bimbo.

At first sight, their cybersecurity goals appear almost impossible: protecting manufacturing sites and 139,000 people in 35 countries, rapidly securing newly acquired businesses, supporting a hybrid working model, safeguarding thousands of internet of things (IoT) devices, and providing operational technology (OT) security for multiple environments—including OT that monitors food production equipment. Complexity and change have been major barriers.

Grupo Bimbo previously relied on a disconnected suite of cybersecurity tools throughout the Americas, Europe, Asia, and Africa. "There was overlap between each, no connected view of our security posture, and significant manual administration. With each business acquisition, we accumulated more tools," says Erwin.

"We supply the world," Erwin continues. "Many global fast-food restaurant and supermarket brands, for example, partner with Grupo Bimbo for their food products. Any outage – however brief – could put this supply chain at risk. We have a 4% share of the US$560 billion global baking industry, and, as we grow, we need to be continually vigilant, using complete network visibility to safeguard the business from every threat."



> **We supply the world. Many global fast-food restaurant and supermarket brands, for example, partner with Grupo Bimbo for their food products. Any outage – however brief – could put this supply chain at risk.**

Erwin Campos
Chief Information Security Officer
Grupo Bimbo

SOLUTION

Simple, connected platforms

Grupo Bimbo standardized on simple, comprehensive, scalable Palo Alto Networks platforms to unite its cloud-centric future. This integrated platform approach seizes breakthroughs in artificial intelligence, analytics, automation, and orchestration to protect the organization worldwide across clouds, networks, and mobile devices.

"Our focus is on bread, not security. Palo Alto Networks helps preserve Grupo Bimbo's financial advantage by making the business more agile, flexible, and reliable. Protecting the global infrastructure with one common, simple platform means we can focus more resources on our sales, customers, and growth," says Erwin.

40,000

endpoints protected with full visibility and analytics

AI-driven security operations

The legacy endpoint technology lacked the flexibility and depth of functionality to detect and prevent unknown malware. By contrast, Cortex XDR provides full visibility, protection, and analytics across 40,000 endpoints, pinpointing threats, uncovering vulnerabilities, blocking attacks, and supercharging investigations. It also helps Grupo Bimbo accelerate its securing of new acquisitions. For example, during a recent international bakery acquisition, the Cortex XDR AI/ML engine detected and isolated a vulnerability in the legacy infrastructure, allowing the acquisition to proceed at pace, free of threats. Cortex XDR also increases its zero-day malware protection by sending unknown samples to WildFire for in-depth analysis.

BlackCat incident

stopped within hours through Cortex XDR

Cortex XSOAR is integrated with Grupo Bimbo's security operations center to automate incident response workflows; reduce alert noise; and eliminate repetitive, manual tasks. Cortex Xpanse is also deployed to identify unexpected and unknown services, helping Grupo Bimbo control and reduce its attack surface.

Erwin comments, "We recently had an incident involving BlackCat. The Cortex XDR Forensics module gave us instant access to threat intelligence and all the forensic artifacts and events. We stopped the incident within a couple of hours. Now, every one of our operations is eager to get their hands on Cortex."

AI-Powered secure access service edge (SASE)

Prisma Access, the cloud-delivered security component of Prisma SASE, is being rolled out worldwide to replace an expensive legacy multiprotocol label switching (MPLS) network. As Grupo Bimbo moves to a hybrid working model, Prisma Access protects its remote locations from even the most sophisticated threats, providing a full spectrum of security services, including Advanced Threat Prevention, Advanced URL Filtering, DNS Security, sandboxing, and more. And it's all delivered through a simple, intuitive user experience with significantly better performance.

Industrial OT Security

Grupo Bimbo is deploying a suite of ruggedized ML-Powered Next-Generation Firewalls (NGFWs) with IoT/OT security for multiple environments to provide continuous analysis of OT network behavior in its global bakery network. The internet of things (IoT) monitoring devices integrate seamlessly with Cortex XDR to provide security event management and orchestrated response. OT security insights are gained via user and device behavior analysis, and threat assessments ensure continuous protection.

"Our food manufacturing process is an intersection of technology, full of sensors, electronic controls, and automated equipment. These dedicated appliances sit at the center of Grupo Bimbo's OT networks for better visibility and control of IoT traffic, enabling fast detection and remediation of malicious activity," says Erwin.

The OT devices, including heat sensors, scanners, cameras, and digital machinery, are exposed to huge cooking temperature variations. The devices also face other harsh conditions, coming into contact with steam and bakery ingredients such as flour. "The growing interconnectivity of our OT and IT network creates new cybersecurity challenges," says Erwin. "We needed a purpose-built OT network security platform that would reliably cope with the demanding conditions in the bakeries, reduce complexity, and close OT security gaps."

Security management

Through a Unit 42 Retainer, incident response and security consulting experts are engaged with Grupo Bimbo to guide the organization before, during, and after an incident. "We recently used the Unit 42 expert services for threat hunting during a threat at one of our subsidiaries. The team immediately identified the artifacts and eliminated the exposed endpoints," says Erwin.

BENEFITS

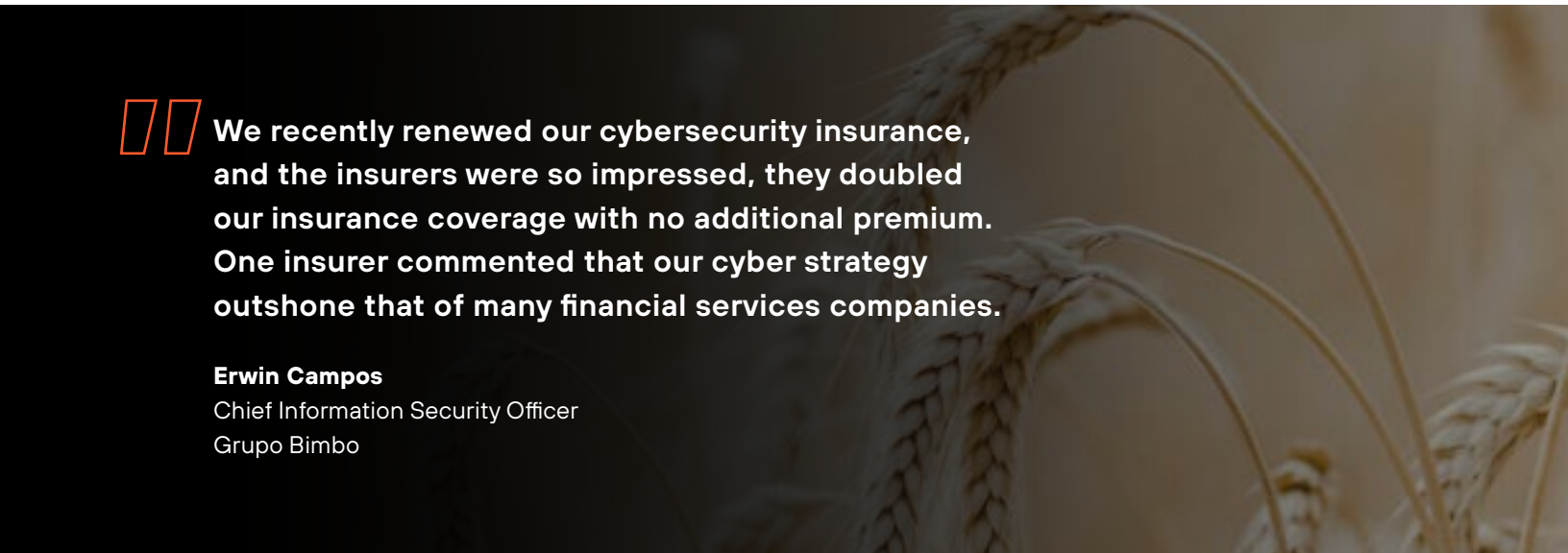
A masterclass in connected, global cybersecurity

Grupo Bimbo's approach to cybersecurity is being transformed by this innovative, connected platform approach, which:

+ **Powers cyber transformation:** The connected network and endpoint security platforms enable secure digital transformation—even as Grupo Bimbo's pace of change accelerates. Erwin explains: "First, Palo Alto Networks has the flexibility to support any legacy environment—and the most modern cloud ones. Second, while many cyber solutions only monitor environments, Palo Alto Networks fights back with unbeatable protection. Third, the platforms are continually innovating, most recently, for example, with the rugged firewalls in the OT environment."
+ **Ensures uninterrupted baking:** With Palo Alto Networks, Grupo Bimbo can safely capitalize on the benefits of Industry 4.0 (for example, using the firewalls for OT monitoring), protect the integrated supply chain, maintain business continuity, and achieve disaster recovery.
+ **Drives people productivity:** Grupo Bimbo's people can now concentrate more on baking and the strategy behind it, and less on security configurations and poor connectivity performance. They also have the flexibility to work anytime, anywhere with high-performance, best-in-class security and direct-to-app connectivity.
+ **Reduces risk:** Erwin's insurers in London recently evaluated Grupo Bimbo's modern cyber strategy. They were so impressed that they doubled Grupo Bimbo's insurance coverage with no additional premium.

+ **Increases security agility:** Grupo Bimbo can react faster to threats using the streamlined platform approach. "Thanks to Cortex XDR, our MTTR and MTTD have been reduced from days to one hour, and we have successfully stopped three critical incidents. That can be the difference between keeping and losing a business," says Erwin.
+ **Underpins M&A strategy:** As Grupo Bimbo grows through acquisition, the Palo Alto Networks platforms are used to quickly monitor and secure the acquired infrastructure, eliminate threats, and streamline business integration. "We love the flexibility of the cyber architecture. We can replicate it from bakery to bakery quickly and without complexity," says Erwin.
+ **Simplifies security:** The platform approach to security is not only simple, comprehensive, and scalable but also more effective. Automation drives agility, shared intelligence reduces risk, and scalable cyber infrastructure doesn't require additional resources.
+ **Lowers cost of operation:** The connected platforms are less expensive to deploy and maintain than multiple disconnected point cyber solutions. Erwin explains one example: "Prisma Access is live in our Colombian operation and already saving the business approximately $100,000 per month." In another example, Xpanse has eliminated the cost of redundant hardware and software.

Erwin's insurers explored this modern cyber strategy and came away pleased. Erwin explains, "We recently renewed our cybersecurity insurance, and I visited brokers in London to explain how we are using Palo Alto Networks and other technologies to safeguard our global operations. The insurers were so impressed, they doubled our insurance coverage with no additional premium. One insurer commented that our cyber strategy outshone that of many financial services companies."



> **We recently renewed our cybersecurity insurance, and the insurers were so impressed, they doubled our insurance coverage with no additional premium. One insurer commented that our cyber strategy outshone that of many financial services companies.**

Erwin Campos
Chief Information Security Officer
Grupo Bimbo