CASE STUDY

HOW AMERICA'S FAVORITE BEAN COMPANY CONTINUES TO SECURE A 129-YEAR LEGACY ON A UNIFIED MICROSOFT PLATFORM

SINCE 1908 BUSH'S BEST

BUSH BROTHERS & COMPANY

WEBSITE
www.bushbeans.com

INDUSTRY
Food & Beverage

GEOGRAPHY
United States

SIZE
800+ employees

Bush Brothers & Company has been a family-operated business since 1897, when a Chestnut Hill, Tennessee schoolteacher named Andrew Jackson "A.J." Bush opened a general store and then a cannery with his sons. Today, Bush's Best produces roughly 80 percent of the canned baked beans consumed in the United States.[1] It's a nationally recognized household brand, one associated with a beloved golden retriever mascot and a legacy built on quality, community, and doing things the right way.

That legacy is the business. The proprietary family recipes, the iconic "roll that beautiful bean footage" slogan, and the brand's intellectual property (IP) behind it, as well as the manufacturing processes and operational know-how that have kept Bush's Best the market leader in its category for generations. These are all foundational assets that have aided Bush in building this trusted reputation that's lasted more than a century. Which is why keeping all of it safe — the trade secrets, the sensitive data, the systems that house it, and the operations that sustain and grow the business — is a big deal.

When you have around 800 employees, two manufacturing plants, and hundreds of endpoints, identities, and systems spanning corporate IT, plant operations, and cloud applications, a continuous security program is essential to ensuring everything stays protected and operational.

Like many manufacturers balancing legacy systems with modern cloud services, Bush Brothers needed security that could keep pace without adding unnecessary complexity. The team wanted stronger end-to-end visibility, clearer advisory guidance on security practices and benchmarks, and a way to reduce overlap across tools, especially as costs and operational effort increased with a security information and event management (SIEM) platform and endpoint stack that didn't fully integrate.

> *"Working with the team at Avertium was fantastic. The team was very knowledgeable, implementation was fast and easy, and we saw more value and greater coverage with Avertium than we did in the whole first year with our previous MSSP."*
>
> – Ron Grohman, Infrastructure and Security Manager, Bush Brothers & Company

ASSESSING THE FOUNDATION BEFORE MAKING BIGGER BETS

Infrastructure and Security Manager Ron Grohman has spent more than 12 years at Bush Brothers, shaping the company's security program to preserve the brand's legacy and keep operations running smoothly. For much of that time, Avertium has worked alongside him — serving as a trusted security advisor and services partner.

Over the years, the Bush Brothers and Avertium teams have worked together to close foundational gaps across Bush's security program. Avertium helped the company adopt the CIS Controls framework that Bush had selected, giving them a structured set of best-practice benchmarks to prioritize against. Together, they built out security policies, ran tabletop exercises to pressure-test response readiness, and documented incident response procedures.

When it came time again to revisit security investments amid rising infrastructure complexity and accumulating licensing costs, Grohman turned to a partner he already trusted. Working together for years had given him confidence in how Avertium operates. That work followed Avertium's Assess, Design, Protect (ADP) approach, a programmatic method that keeps security and compliance woven into a broader, evolving strategy.

The partnership has spanned many different areas of Bush Brothers' security program:

- Governance, risk, and compliance (GRC)
- State-by-state privacy breach notification requirements
- Operational technology (OT) vulnerability management
- Secure, ethical use of AI across the organization

So when the next set of decisions came into view, Avertium was the natural partner to help Grohman and his team think them through.

GETTING THE MOST OUT OF MICROSOFT SECURITY INVESTMENTS

Bush Brothers had already invested in Microsoft 365 E5, which gave the team access to a deep bench of advanced security capabilities, including Microsoft Defender for Endpoint, Defender for Identity, Defender for Cloud Apps, and data governance tools through Microsoft Purview. But many of those capabilities were being underutilized, and E5 on its own didn't cover the SIEM and managed detection layers the business needed.

At the same time, the company was paying separately for CrowdStrike for endpoint protection and Splunk as its SIEM. The tools didn't integrate natively, the all-up cost was climbing, and the operational effort to manage and tune three disconnected platforms was taking time away from higher-value work. Grohman knew Avertium had built deep expertise in the Microsoft Security stack, and he asked them to validate his team's assumptions, map out options, and help chart a path forward that fit Bush Brothers' goals.

THE END GOAL

An integrated, streamlined Microsoft Security environment built to flex with Bush Brothers, today and tomorrow.

As a Microsoft Security Solutions Partner with deep expertise across the Microsoft Security portfolio, Avertium was the right advisor to help Grohman expand and mature their security practice over time. The teams evaluated what Bush Brothers already owned to find where untapped value was hiding.

For instance, Microsoft Defender XDR could take on the endpoint and identity protection Bush Brothers was paying CrowdStrike to deliver, and Purview's data governance capabilities were sitting largely untouched. Avertium's recommendation was to optimize those existing investments while simultaneously extending the platform by adding Microsoft Sentinel to the product stack.

As Microsoft's cloud-native SIEM, Sentinel is designed to build on E5 telemetry and unify signals across Bush Brothers' environment. This could effectively replace what Splunk had been doing and establish a foundation for managed detection and response through Avertium's Fusion MXDR for Microsoft.

The end goal was an integrated, streamlined Microsoft Security environment designed to flex with Bush Brothers, meeting today's needs while leaving room for tomorrow's priorities, like AI security and data governance. Avertium could then extend, configure, and operationalize capabilities over time in close partnership with Grohman and his team.

MAKING THE CASE FOR AVERTIUM FUSION MXDR FOR MICROSOFT

Before retiring any existing technologies, Avertium walked the Bush Brothers team through what a unified Defender XDR and Sentinel security operations (SecOps) platform could look like, particularly when configured to their specific business needs and operationalized through Avertium Fusion MXDR for Microsoft.

Fusion MXDR is Avertium's managed extended detection and response solution, purpose-built for the Microsoft Security platform.

During a hands-on technical demonstration, Avertium walked the team through several capabilities that stood out. For example, Avertium showcased Microsoft Sentinel's Fusion correlation capabilities, which revealed a level of advanced alert correlation that Bush Brothers hadn't experienced before, automatically connecting related signals across their environment into high-confidence incidents and a more coherent threat picture.

Avertium further demonstrated how log ingestion and tiering strategies could be optimized so that full analytics was reserved for prioritized high-value data, helping keep Azure spend manageable. The Bush Brothers team was also drawn to the advanced hunting queries that Avertium builds on top of Sentinel's native capabilities, demonstrating a depth of threat detection that was novel and exciting to Grohman and his team.

Configuring the platform was only part of what Avertium brought to the table. On top of Defender XDR and Sentinel's native capabilities, Avertium layers its own detection logic, custom correlation rules, and advanced hunting queries. This turns a powerful Microsoft platform into operationalized security tailored to Bush Brothers' specific environment and risk profile.

For a lean security team that had been managing complex infrastructure and paying for various point solutions, this was a turning point.

A unified XDR environment, with Avertium's proprietary detection layers built on top and Fusion MXDR providing continuous coverage, would give Grohman and his team a way to simplify operations and reduce costs. It would also deliver a complete, contextualized picture of Bush Brothers' security posture around the clock without requiring an in-house security operations center (SOC).

"Simplicity and cost. It was a huge benefit to have everything in one place and naturally work together. Simplified configuration, management, and reduced cost. Those were the biggest reasons why we moved to a unified Microsoft Security platform."

– Ron Grohman, Infrastructure and Security Manager, Bush Brothers & Company

SIMPLICITY, SAVINGS, AND SECURITY THAT ACTUALLY WORK TOGETHER

Today, Bush Brothers has transitioned off CrowdStrike and Splunk, and Avertium runs Defender XDR and Sentinel through Fusion MXDR for Microsoft. This provides continuous managed threat detection and response across Bush Brothers' corporate and manufacturing environments — all on a single, unified platform.

The results speak for themselves. By consolidating onto the Microsoft Security stack and operationalizing it through Avertium's managed services, Bush Brothers simplified its security operations workflows, improved threat visibility across the business, and delivered approximately 20 percent in cost savings over the previous combination of tools and providers. Budget and effort that used to go toward maintaining and tuning disconnected platforms are now going toward higher-value work, including data governance.

> *"Top of mind is always how to stay ahead of the ever-accelerating technology curve. Data security is baked into everything we do. Our next move is likely making more precise and targeted decisions using analytics and AI instead of broad, company-wide solutions."*
>
> – Ron Grohman, Infrastructure and Security Manager, Bush Brothers & Company

PROTECTING THE NEXT CHAPTER

With the security operations foundation in place, Grohman and his team have turned their attention to what comes next: being a good steward of their security investments and utilizing the vast capabilities included in their Microsoft 365 E5 licensing. To achieve these goals, the team is utilizing Avertium's Envisioning Workshops to get hands-on, expert-led experience with the tools they already own.

Bush Brothers continues to mature best practices across the organization, focusing next on strengthening data governance and policy enforcement. The company is also progressing penetration testing maturity with advanced exercises and additional tabletop scenarios to validate that their security environment is not only deployed, but effective. These strategic initiatives are helping Grohman and his team turn security into a real business enabler, giving Bush Brothers the confidence to scale, integrate, and recover with agility.

Avertium remains both the operator running Fusion MXDR and Bush Brothers' long-term security partner.

GET HANDS-ON GUIDANCE FROM MICROSOFT EXPERTS

For organizations looking to get more from their Microsoft Security investments, Avertium's Microsoft-funded Envisioning Workshops offer a practical starting point. Discover workshops spanning data security, cloud security, modern SecOps, and threat protection.

EXPLORE WORKSHOPS

[1] Bush's Beans cooks up 117-year-old business in East Tennessee | Main Street Media, 2025

AVERTIUM®

ASSESS. DESIGN. PROTECT.