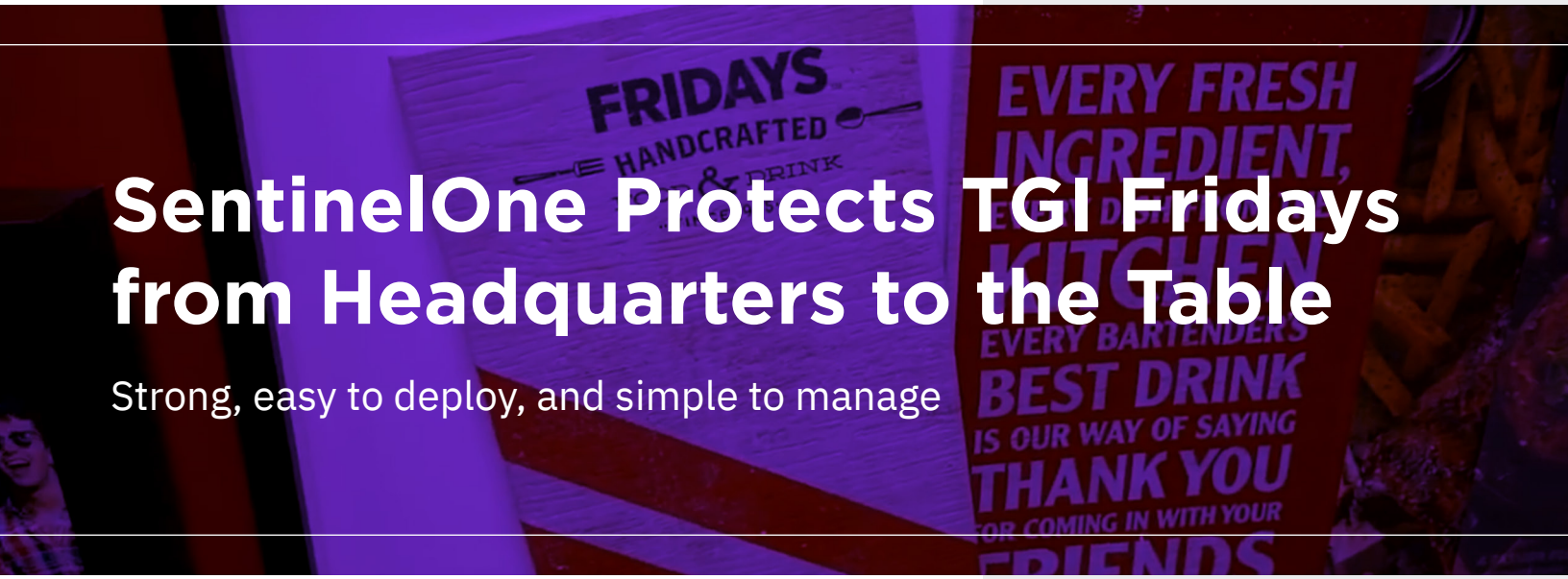
CASE STUDY

SentinelOne



SentinelOne Protects TGI Fridays from Headquarters to the Table

Strong, easy to deploy, and simple to manage

The Challenge: Eliminating Exposure To Internal And External Threats

"Our users are constantly under threat of attack—whether they're in this building or outside of these four walls," states Sam Langley, VP of Information Technology, at TGI Fridays' headquarters in Dallas, Texas. "We needed strong endpoint protection that traveled with the users."

Opening its first location in New York City in 1965, TGI Fridays now encompasses more than 900 restaurants in 60 countries employing nearly 74,000 staff members. Using a franchise model, it serves high-quality, authentic American food and handcrafted cocktails to over 50 million guests each year. Celebrating "Fridays" by bringing people together to socialize is at the core of TGI Fridays' legendary promise: "In Here, It's Always Friday®.

Driving business growth and increasing profitability, TGI Fridays has focused on digital technology innovation to enhance the guest experience. Using applications powered by artificial intelligence (AI), they've increased client engagement, improved internal operations, and boosted the skills of their team members to deliver exceptional experiences.

"My responsibilities include all restaurant facing technology," explains Langley, "from the point-of-sale system to the back of the house infrastructure to the corporate office and corporate infrastructure software development and information security."

TGI FRIDAYS

CHALLENGES

- Strong, company-wide protection for all endpoints against malicious threats
- Fast, easy deployment with minimal user impact
- Simple management of endpoint security leaving staff to concentrate on critical projects

SOLUTION

- SentinelOne Endpoint Protection Platform

BENEFITS

- Accelerated threat detection, prioritization, and response
- Lightweight agents with built-in autonomy for real-time security
- Simple, deploy-and-forget with minimal management

Competing With The Best Of The Best

Designed for rapid deployment and simple manageability across both on-premise and cloud environments, SentinelOne blocks threats at the endpoint, utilizing multiple AI engines to automatically quarantine and eliminate risks in real-time.

"For us, our typical evaluation process consists of running multiple side-by-side proof of concepts for around 30 days," states Langley, commenting on TGI Fridays' approach to purchasing new technologies. "After the 30 days, we evaluate each of the vendors against our critical success factors, which—in our case—are strong protection and the ease of deployment and management."

SentinelOne's light-weight agent is deployed on each endpoint to deliver autonomous protection. It successfully detects and responds to both internal and external threats before they traverse the network. The independent and dynamic nature of SentinelOne agents minimizes the need for continual monitoring and management at the Security Operations Center (SOC), reducing management costs and increasing innovation targeted at driving business growth.

Leveraging AI For Protection Against All Threat Vectors

"SentinelOne met all of our critical success factors," explains Langley, "with the most important being strong protection."

SentinelOne's next-generation, single-agent technology utilizes AI to protect devices against all threat vectors: pre-execution, on-execution, and post-execution.

Pre-execution: Replacing traditional signatures, SentinelOne's Static AI engine provides protection at the agent level before the attack occurs, obviating the need for recurring scans that impact user productivity.

Sam Langley
VP of Information Technology at TGI Fridays

"SentinelOne's autonomous endpoint model helps free up my team to focus on other critical projects, and frees me up to focus on other aspects of information security."

On-execution: Tracking all processes and their interactions at the agent level, the vector-agnostic Behavioral AI engine detects malicious activities, triggering a response at machine speed to protect the entire network.

Post-execution: Providing rich forensic data, SentinelOne's Automated Endpoint Detection and Response (EDR) technology automatically mitigates threats, performs network isolation, auto-immunizes endpoints against newly discovered threats. It also rolls back endpoints to their pre-infected state if required.

"We had a report of malware being delivered to a user," highlights Langley. "We captured the malware on disk—which our current AV (antivirus) solution didn't capture. We installed it on the pilot desktop running SentinelOne. SentinelOne caught it immediately and prevented it from being saved to disk. The traditional AV solution didn't catch that malware until the next day."

Focusing On Your Business While SentinelOne Secures Your Network

"As I imagine the scenario across the enterprise, it was an obvious decision to select SentinelOne," states Langley. "SentinelOne's autonomous endpoint model helps free up my team to focus on other critical projects, and frees me up to focus on other aspects of information security."