ScottsMiracle-Gro Selects Xage to Secure Remote Access Across North American Manufacturing Plants

Overview

The ScottsMiracle-Gro Company is the leading marketer of branded consumer lawn and garden products in North America.With more than 80 manufacturing and distribution facilities across its supply chain, ScottsMiracle-Gro relies on critical operational technology (OT) systems and production capabilities to ensure safe, efficient, and reliable operations at scale. As ScottsMiracle-Gro has continued to transform its supply chain, the cybersecurity team prioritized modernizing remote access to the diverse OT systems throughout its large and matrixed footprint.

A critical business requirement was **securing third-party remote access** to manufacturing and distribution facilities. Vendors and contractors are essential to supporting OT systems, yet the traditional remote access approaches introduced unnecessary security risks and operational friction that the company wanted to eliminate.

The team also recognized that **visibility alone was not enough** to protect its operations. Without the ability to granularly control and isolate access, the organization remained exposed to security risks that could disrupt supply chain operations.

To address these challenges, ScottsMiracle-Gro adopted a protection-first approach to securing its facilities and partnered with Xage Security. By deploying Xage secure remote access (SRA) across all sites, ScottsMiracle-Gro was able to modernize how access is secured for both internal teams and third-party vendors—without relying on agents, VPNs, or jump servers. The following case study explores how Xage's Zero Trust approach helped ScottsMiracle-Gro strengthen security, streamline operations, and reduce downtime across its North American supply chain.

ScottsMiracle-Gro®

With Xage, ScottsMiracle-Gro is able to:

- **Provide browser-based remote access without VPNs, agents, or jump servers**
- **Enforce granular, identity-based access down to specific plants and assets**
- **Centrally manage third-party identities and Zero Trust-based access policies**
- **Apply consistent security controls across all North American sites**
- **Deliver a simple, intuitive experience for plant operators and third-party users, enabling secure access without added complexity**
- **Meet latency requirements for remote operational tasks**

> ***"We knew visibility alone isn't enough—especially given the diverse systems that we manage. We chose Xage because we wanted to take a protection-first approach to securing our supply chain facilities. Xage delivered a scalable way to isolate risk and securely enable third-party access across our operations."***
>
> **— Dane Durbin, CISO, The ScottsMiracle-Gro Company**

Protection-First Approach to OT Security

ScottsMiracle-Gro's cybersecurity team initially attempted to improve security posture through OT asset discovery and vulnerability management initiatives. However, achieving complete visibility across all sites proved difficult to scale. Additionally, some of the critical systems were difficult to continuously patch and protect against software vulnerabilities.

To address business needs, ScottsMiracle-Gro adopted a **protection-first security strategy.**

Rather than waiting for "complete" asset inventory or relying on slow and incomplete vulnerability remediation, the security team prioritized reducing risk immediately by securing access paths into manufacturing and distribution environments. **Secure remote access (SRA) was identified as the top initiative** to modernize cybersecurity.

Key requirements included:

- Secure, consistent third-party access across all plants and facilities
- Support for both legacy and modern OT systems
- Agentless access for vendors and contractors
- Elimination of jump servers and VPN complexity
- Centralized policy enforcement at scale

xage SECURITY

Why ScottsMiracle-Gro Chose Xage

ScottsMiracle-Gro evaluated several IT-centric and OT-focused SRA solutions. Many required installing endpoint agents on third-party laptops or the deployment of jump servers at each plant—approaches that it deemed **costly, complex, and operationally impractical.**

Xage was selected for its ability to deliver **agentless, Zero Trust SRA** purpose-built for OT environments.

With Xage SRA, ScottsMiracle-Gro is able to:

- Provide browser-based remote access without VPNs, agents, or jump servers
- Enforce granular, identity-based access down to specific plants and assets
- Centrally manage third-party identities and Zero Trust-based access policies
- Apply consistent security controls across all North American sites
- Deliver a simple, intuitive experience for plant operators and third-party users, enabling secure access without added complexity
- Meet latency requirements for remote operational tasks

Xage's scalable architecture and protection-first approach aligned directly with ScottsMiracle-Gro's cybersecurity and operational objectives.

Business Results

Reduced Risk and Improved Resilience

By securing remote access with granular, standardized policies, ScottsMiracle-Gro significantly reduced the potential blast radius of security incidents and strengthened resilience across critical operations. With the deployment of the Xage SRA solution, ScottsMiracle-Gro eliminated traditional approaches to remote operations.

Faster Issue Resolution and Less Downtime

Previously, contractors often had to travel on site to resolve equipment issues, delaying resolution by days. With Xage, secure access can be provisioned within minutes, enabling faster troubleshooting and mitigating potential production downtime.

Improved Visibility and Auditability

Xage provides compliance-ready audit logs, session visibility, and recording capabilities. Furthermore, the detailed, tamper-proof audit logs can easily be ingested into ScottsMiracle-Gro's SIEM. This improves security monitoring, supports compliance requirements, and demonstrates increased cybersecurity maturity for cyber insurance assessments.

Positive Adoption Across Teams

The deployment of Xage SRA has received positive feedback from cybersecurity teams, OT teams, and third-party vendors, streamlining remote access while strengthening security posture. Users have reported significantly improved ease of access to critical systems needed to do their jobs.

xage SECURITY