CUSTOMER SUCCESS STORY

Fortune 1000 Manufacturer

TECHNOLOGY

Industry
- Fortune 1000 Manufacturer

Environment
- 900+ Windows workstations, both mfg. floor and office environment
- 400+ ICS Machines

Challenges
- Identified spear phishing and drive-by-download attacks as persistent threats
- Concern that even with employee training risk existed due to volume of attacks
- Lightly managed workstations on mfg. floor shared by multiple workers
- Lean InfoSec and IT operations unable to dedicate time to a labor intensive solution
- Existing whitelisting solution overly complex, slow to propagate changes across network

Results
- Contained spear phishing attack to single machine; prevented spread to other machines
- Rapid, and local exception handling process allowed executive to update local whitelist, in real time, to allow conferencing application for prospect conversation
- Established controls to prevent liabilities from unlicensed software installs
- Documented audit log of exception acknowledged by the end user

DIGITAL GUARDIAN®
Formerly VERDASYS

Application Control Secures Manufacturing Floor and Back Office - While Maintaining Business Velocity

Managing desktops can be a challenge given the rise of spear phishing attacks, couple that with multiple users on a single machine and you have a potential for rapid system drift. This drift opens the door to malware, or unapproved applications on these machines, putting your data and your organization at risk.

The company had proactively identified this gap and sought to alleviate it with an application whitelisting solution but ran into problems once deployed to a small portion of the business. Overly complex management requirements were taking valuable time from the InfoSec team, centralized and rigid exception handling delayed approvals for whitelist additions. They were looking for a way to control applications without the complexity. Digital Guardian Application Whitelisting (formerly Savant Protection), solved all these problems and delivered a unique whitelisting architecture that can scale to achieve their goal of 100% deployment.

THE BUSINESS CHALLENGE

The company maintains a blend of traditional desktops in both a single machine, single user model as well as machines on the manufacturing floor shared by different users with each shift. This environment resulted in endpoints deviating, often rapidly, from the standard and approved corporate configuration. These machines, as deployed on the manufacturing floor interfaced with the ICS environment to power their manufacturing processes where any incompatibilities or downtime could impact the production schedule or worker safety.

A secure desktop environment is the ideal goal, but there needs to be a way to make changes when new applications are required. The organization demanded a way to be flexible when new applications are needed at the endpoint, but this flexibility could not be at the expense of productivity.

CRITICAL SUCCESS FACTORS

- Streamlined usability for the InfoSec team
- Flexible management options
- Enhance desktop/end user security without negative impact on productivity
- Robust whitelist not subject to single point of failure

DIGITAL GUARDIAN FACTS

Customers
- Over 250 customers
- 130 of the Global 2000
- Government Agencies
- Used by 7 of the top 10 US Patent Holders
- Over 2,100,000 endpoints protected
- Only solution to scale to 250K+ agents

Information Discovery and Classification
- Context-based data awareness
- Content Inspection
- User Classification
- All content is tagged with permissions
- Permissions persist through reuse, renaming
- Over 300 data types
- 90 languages

Response Options
- Monitor, log, report
- Prompt, justify, and report
- Block and report

Supported Platforms
- Desktop/Laptop
- Server
- Network
- Virtual
- Supports devices on network and off network

Supported OS
- Windows
- Linux
- Mac OS

Deployment Models
- On Premise
- Managed Service
- Hybrid

DIGITAL GUARDIAN®
Formerly VERDASYS

www.digitalguardian.com

THE SOLUTION

> It gives me a unique perspective that I can't get from other tools.
>
> *- Manager, IT Security*

Digital Guardian Application Whitelisting was deployed across a subset of the user base, mainly on the high risk machines to re-establish to the leadership that application whitelisting can be an effective tool without excess overhead. Based on its initial success, including containing a spear phishing attack to just one user, the company intends to expand deployment of Digital Guardian across the entire pool of endpoints, with over 1/3 being on the manufacturing floor, and then include the ICS network for an end to end application whitelisted environment.

Digital Guardian Application Whitelisting delivers the easiest to manage and most secure application whitelisting solution:

- **Rapid deployment:** Installs in minutes with no pre-determination of which applications and libraries are required. Once installed the agent automatically creates a unique whitelist that determines what executables are permitted to run on that device.
- **Blocks unknown and unauthorized executables:** Protects workstations, servers, and fixed function devices such as POS terminals and ICS devices.
- **Stops malware before it can spread:** Using a device specific whitelist, malicious processes cannot propagate throughout the environment, even if an infected external machine connects to your network.
- **Flexible management options:** Local GUI and centralized console facilitates usability for both InfoSec and end user.

THE RESULTS

> I trust it so much; I feel like a have a real weapon to stop the bad guys.
>
> *- Manager, IT Security*

Being able to manage the whitelist both at the endpoint through a local GUI and via a centralized management console gave the InfoSec team the ability to respond more quickly to change requests, and empower the end user to manage their own without potentially compromising the corporate environment. Because each machine maintains its own, unique whitelist malware cannot propagate across the network and is contained at the individual endpoint. Moreover, the ability to add applications instantly delivers the business speed required to maintain their edge in the competitive environment they operate. With Digital Guardian in place the organization can protect their endpoints, their network, and ultimately their business.