MILLIKEN & COMPANY

CASE STUDY

CYBERARK®

Milliken™

Company: Milliken & Company

Milliken & Company enhances security protocol through least privilege with default deny application control to protect global end users.

Industry: Manufacturing

Employees: 7,000+

CyberArk Product & Services:
Endpoint Privilege Manager

"CyberArk gave us the visibility and granular control needed to implement both least privilege and 'default deny' application control with minimal disruption to the organization. "

Ken Brown, Chief Information Security Officer
Milliken & Company

Global manufacturer deploys CyberArk Endpoint Privilege Manager to reduce risk on endpoints across 50 sites worldwide.

Milliken & Company, a diversified global manufacturer, has a long-standing heritage of exploring, discovering, and creating ways to enhance people's lives. For more than 150 years, innovation has led the way combining science with meaningful design and insights. With a knowledge-based investment approach, Milliken employs more than 100 PhDs and has accumulated more than 5,000 worldwide patents. Across more than 35 manufacturing plants located in the U.S., U.K., Belgium, France, China, India, and Australia, and sales and service operations throughout the Americas, Europe, and Asia, more than 7,000 Milliken associates required a security solution that could scale and mitigate risk to enable them to continue to deliver on the Milliken promise to add true value to people's lives, improve health and safety, and make this world more sustainable.

THE CHALLENGE

Growing both organically and through acquisition since 1865, Milliken amassed unprecedented intellectual property, which has powered much of the company's success. It has also presented challenges to protect that information and mitigate risks presented by the modern IT environment. Privacy and data security were a top priority. With the company operating more than 50 locations around the world, they needed a solution that could cover every endpoint and scale with the growing company. Amidst a current landscape of large breaches occurring at other companies, Milliken's desire to protect its associates and its intellectual property led them to perform an internal security assessment, which included hiring a third-party security consultant to independently evaluate their environment. The assessment's outcome demonstrated to the Milliken security team that changes were needed, leading to new security policies for managing this global IT environment. At Milliken, end users were running with full administrative rights on their company devices. A goal was established to eliminate this high risk and only allow certain individuals to have elevated privileges and only for specific applications and functionality. Along with establishing least privilege, the company sought better capabilities to govern application control.

To ensure that users continued to have the freedom needed to do their jobs effectively, the right solution needed to balance the needs of the business around innovation but also minimize risk to the company and brand.

THE SOLUTION

Milliken chose CyberArk Endpoint Privilege Manager to deliver a global solution across every endpoint in the company. According to Ken Brown, Chief Information Security Officer for Milliken, "We needed to critically address three security requirements from a global perspective: least privilege, patch management and application control; CyberArk Endpoint Privilege Manager covers two of these for us very nicely".

CyberArk Endpoint Privilege Manager enables the company to detect and apply granular-level control to all policies and establish standard users without administrative privileges – a key requirement for selecting the privilege management product because it eliminates a large portion of the risk they were currently facing." CyberArk Endpoint Privilege Manager gave us that visibility to plan and prepare the organization to move to standard user. Furthermore, running Endpoint Privilege Manager in monitor mode allowed us to capture the applications in use today. With this visibility, CyberArk Endpoint Privilege Manager allowed us to create policies for reputable applications needed for business while blocking all unknown and unauthorized software.

With these policies in place, we were able to switch to blocking mode with a high degree of confidence" Ken continued. Rolling out CyberArk in a phased approach also ensured Ken and his team that these security controls were accepted by the company and enabled a complete global rollout in under six months. To enable end users to have creative freedom, Milliken leveraged a feature in CyberArk Endpoint Privilege Manager which defined permitted applications through a trusted-sources model that ensured only known applications were entering onto workstations and laptops. CyberArk Endpoint Privilege Manager has a capability to manage assets on and off the network as well as determine reputation scores for every application and its related files. With Cyberark, allowing only authorized changes to the environment was now a reality regardless of where the end user was operating.

THE RESULTS

The CyberArk Endpoint Privilege Manager solution helps secure and control the IT environment at Milliken more efficiently and cost effectively worldwide. All application control and privilege management policies propagate immediately, regardless of the worker's location, ensuring that all end user machines are equally secure, even as they travel from facility to facility. Ken added that the results experienced speak for themselves "CyberArk Endpoint Privilege Manager gave us the visibility and granular control needed to implement both least privilege and 'default deny' application control with minimal disruption to the organization. We are also happy to say that since we have enabled 'default deny', our instances of malware have dropped substantially. In fact through sandbox testing we successfully blocked Wannacry giving us a high degree of confidence for the effectiveness of 'default deny'.

From a forensics and incident response perspective, CyberArk provides visibility through the application catalog to see all applications installed in the environment, when these items were installed, and their respective execution timelines. "Help with incident response was a benefit that Milliken was not expecting to get with CyberArk Endpoint Privilege Manager and filled a gap we had at the endpoint" adds Ken. The benefits extend beyond security too with a reduction in help desk calls because CyberArk ensures that only known applications are installed. By eliminating unauthorized applications, the entire endpoint environment has a higher degree of stability which helps to drive down the support required and helps Milliken to control costs.

With the level of control offered and instant notifications of any policy infringement, both the IT administrator and the company are able to proactively tackle issues as they arise. Today, Milliken is leveraging CyberArk Endpoint Privilege Manager on over 5,000 endpoints implementing least privilege and application control policies with minimal impact to end-user experience.

Endpoint Privilege Manager runs on Amazon Web Services (AWS), which delivers a scalable cloud computing platform with high availability and dependability, protecting the confidentiality, integrity, and availability of our customers' systems and data.

Challenge

- Allow freedom to innovate across 50 sites globally with a flexible and scalable solution to address data privacy concerns and protect intellectual property

Environment

- 7,000 end users spread across 50+ sites worldwide
- Every user running as local admin
- Many applications in use

Results & Key Benefits

- Multi-phased rollout fully deployed in six months
  - Phase 1: Successfully removed admin credentials on every endpoint
  - Phase 2: Application control using 'default deny' with trusted sources
- Instances of malware outbreaks dropped substantially
- Dramatic reduction of risk and ability to infiltrate windows environment
- Closed visibility gap at endpoint for incident response processes
- With application control, endpoint stability increased resulting in fewer desk calls