Deloitte.

A stronger formula for defending against cyber threats

Global chemicals company boosts cybersecurity by elevating attack surface management

Energy, Resources & Industrials

Industry

Attack Surface Management

Solution

Cyber Stories

The starting point

How can you defend something if you don't know what it is? For one sustainable global chemicals company, that question has become increasingly important as the cyber threat landscape has intensified as its business has evolved—with more digital data, processes, systems, and applications.

Despite its digital evolution, the company did not have a proper balance between transformation and business—in particular, its ability to understand and manage its growing organizational attack surface. Merger and Acquisition (M&A) activities exacerbated the problem, as IT was not as involved in all stages of the M&A process. The growing digital footprint of the company—as well as points of on-premises and cloud vulnerabilities and reliance on third-party services and solutions—created an expansive attack surface that was difficult to assess and manage.

That lack of visibility created real and growing risks, providing ample opportunity for attackers to exploit unknown assets vulnerabilities, find a way into the company's systems, and wreak havoc—from stealing sensitive data to launching ransomware attacks.

Though the company had engaged a vendor to assist with their attack surface management (ASM) program, leaders understood that they needed to do more—and do it faster, to keep pace with the evolution of threats and the business. Leaders wanted to do more than identify vulnerabilities. They wanted to ensure they could remediate the associated risks while staying ahead of trends and potential cyberattacks.

Factors in focus

- Digital evolution and expansion of business
- Lack of visibility into a growing attack surface
- Attacker tools, and Tactics, Techniques, and Procedures (TTPs) continue to increase in sophistication, availability, and frequency of use

The way forward

To accelerate its ASM maturity and address needs on a broader scale, the company selected Deloitte and its ASM service to provide a range of services aimed at reducing vulnerabilities and enterprise risk. Working with Deloitte, company leaders began laying out a strategic plan to strengthen attack surface management from end to end—and to make ASM an integral, day-to-day component of cybersecurity.

To begin developing a comprehensive ASM program, Deloitte worked across the client organization to identify and assess the extent of its attack surface and potential vulnerabilities, both externally (Internet facing) and internally. As part of the work, Deloitte leveraged offensive security operations (OSO) specialists and proprietary cyber "cartography" mapping tools to discover previously unknown external assets.

Once the global chemicals company and Deloitte had created a more thorough view of the attack surface, vulnerabilities, and risk exposure, the two organizations collaborated to remediate specific issues. For example, Deloitte played a pivotal role in fortifying the company's cybersecurity by conducting a complete port scan of the company's well known, registered and dynamic ports. This resulted in identifying unknown critical open ports (i.e., network communication endpoints) that were prime targets for potential cyberattacks. This decisive action bolstered the company's defenses against sophisticated threats.

Insights to inspire

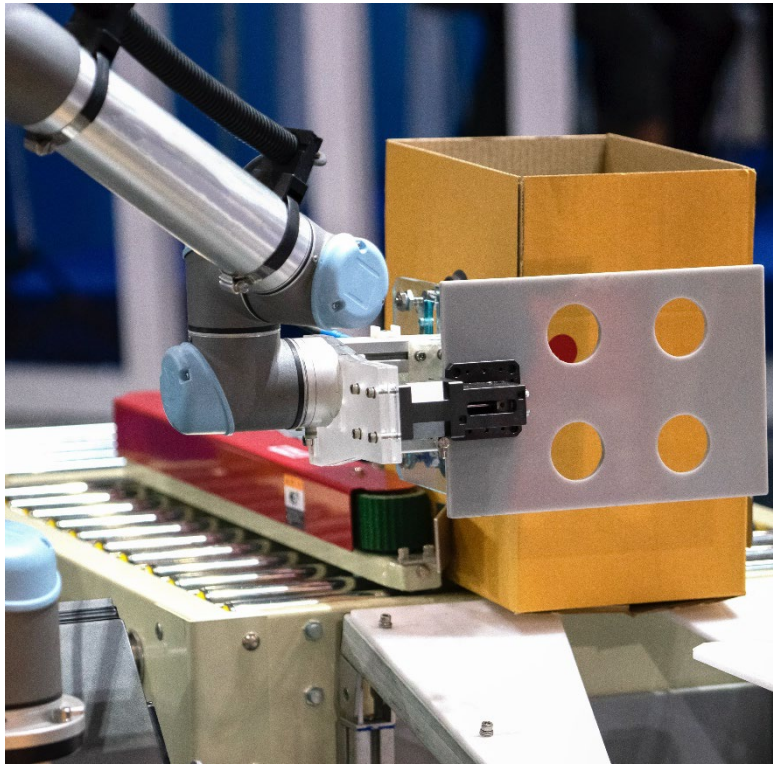
Understand that your attack surface is about more than your enterprise's digital assets. It's about vulnerabilities in your physical and third-party ecosystems too.

Attack surface management should not be a one-time exercise. It should be an ongoing program that evolves as your business and cyber threats evolve.

To enable the company to manage its attack surface on an ongoing basis, Deloitte worked with the company to create foundational governance for the program—covering procedures for vulnerability triaging, remediation, and remediation validation. Developed rapidly using a proprietary Deloitte accelerator, the governance framework and its associated "run book" provided guidance for addressing needs such as triage and escalation of issues, plus detailed steps for remediation.

Analytics have been a key component of the ASM program. Specifically, Deloitte analysts created operational reporting dashboards and deployed other reporting tools that provide insights into ASM-related trends. Those insights have allowed the client to proactively identify and address issues—such as new types of exposure or a growing need for a particular cybersecurity skillset. Deloitte also helped the company increase the efficiency of an existing third-party vulnerability management scanning solution, which has been central to the ongoing ASM program.

With core components of the program in place, the company is looking to build on its new capabilities, with plans to automate reporting and increase integration between attack surface management and other cybersecurity functions. In the meantime, the company is realizing a host of benefits from the ASM transformation—from increased risk visibility to improved business resilience to greater confidence for ongoing innovation.



The achievements

Increased visibility into the organization's external attack surface

Comprehensive risk-reduction program for attack surface management

Detailed governance and procedures for ASM

Proactive insights and detailed reporting to guide ongoing ASM activities and investments

Improved cybersecurity posture and business resilience

Greater confidence in digital enterprise ecosystem, supporting the company's ability to innovate

Let’s talk cyber

How is your organization evolving—and how is it preparing for the new types of cyberattacks that are headed its way? Discover how Deloitte’s worldwide team of industry-focused cyber specialists can help you more effectively manage your organization’s attack surface and stay ahead of new challenges. Contact us to get the conversation started.

deloitte.com/cyber

Contacts

Chuck Littmann
US Attack Surface Management, Managing Director
Deloitte & Touche LLP
clittmann@deloitte.com

Andrew Douglas
US Attack Surface Management Leader
Deloitte & Touche LLP
andouglas@deloitte.com

Lourens Bordewijk
Global Attack Surface Management Leader
Deloitte Netherlands
lbordewijk@deloitte.nl

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte provides industry-leading audit and assurance, tax and legal, consulting, financial advisory, and risk advisory services to nearly 90% of the Fortune Global 500® and thousands of private companies. Our people deliver measurable and lasting results that help reinforce public trust in capital markets, enable clients to transform and thrive, and lead the way toward a stronger economy, a more equitable society, and a sustainable world. Building on its 175-plus year history, Deloitte spans more than 150 countries and territories. Learn how Deloitte’s approximately 457,000 people worldwide make an impact that matters at www.deloitte.com.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (DTTL), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agentsshall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.

© 2025. For information, contact Deloitte Global.

Cyber Stories