Oerlikon Reduces Patch Time and Improves Management-Level Cyber Risk Visibility With Balbix

oerlikon

About Oerlikon

Oerlikon Group is a global manufacturing powerhouse for surface engineering, polymer processing, and additive manufacturing. Their high-tech solutions are designed for applications in growth markets such as the automotive industry, aerospace, energy, the tooling industry, and manufacturing. Headquartered in Pfäffikon, Switzerland, Oerlikon has a global footprint.

Daniel Gisler, the Chief Information Security Officer (CISO), is a security veteran who is a respected thought leader in the industry. He is responsible for the cybersecurity of Oerlikon and over 10,000 employees at 179 locations in 37 countries.

The Challenge

Oerlikon's IT infrastructure and users are spread across a global base of operations, comprising production plants and other locations. Daniel and his team are tasked with monitoring and securing this large workforce and associated IT assets across sites and geographies.

When new vulnerabilities and security issues emerge at a very rapid rate as is the case today, it is very hard for infosec teams to keep up. Daniel and his team were looking for a risk-based approach to identify and remediate critical vulnerabilities efficiently. To achieve this, they had three questions top of mind:

- How to get a comprehensive inventory of all network-connected assets, categorized by asset types and sites
- How to detect vulnerabilities and other risk issues including poor password hygiene and missing/weak encryption and assign owners to fix them
- How to reduce the mean time to resolve newly discovered security issues from months to days

> "To succeed in cybersecurity, time is of the essence, so we invest in tools and architectures that give us a speed advantage. Balbix provides us with real-time security posture visibility, vulnerability prioritization, and reduces our MTTR for issues."
>
> **— Daniel Gisler, CISO, Oerlikon**

Enter Balbix

Oerlikon deployed Balbix in data centers in North America, Europe, and Asia covering tens of thousands of assets, and multiple asset types. They immediately saw results. Oerlikon was able to:

- Get an accurate inventory of all assets, including devices, apps, and services in near real time. The assets were categorized into managed and unmanaged assets, on-premises and cloud assets, fixed and mobile etc.
- Analyze and categorize usage, network traffic, and other attributes for each asset
- Continuously monitor each asset across 100+ attack vectors, including missing encryption, weak and reused passwords, obsolete software, OS requiring upgrades and more
- Assign risk owners to dynamic groups of assets based on their location, hostname, and other custom attributes

"To succeed in cybersecurity, time is of the essence, so we invest in tools and architectures that give us a speed advantage. Balbix provides us with real-time security posture visibility, vulnerability prioritization, and reduces our MTTR for issues," says Daniel. They have seen spectacular results with Balbix.

- ☑ Three times more assets have been identified compared to the previous inventory process.
- ☑ Mean time to patch has been reduced by 50% and counting
- ☑ Communicating about security to management is made a lot easier with the trend lines from the Balbix CISO Dashboard

Prioritization of Risk Items

At Oerlikon, Balbix continuously discovers and prioritizes emerging vulnerabilities based on risk, incorporating information about vulnerabilities, threat levels, asset exposure, security controls and business criticality. Dashboards with powerful filtered search capabilities enable the security team to identify risk areas quickly.

3X
more assets identified

50%
reduction in mean time to patch

EASY
reporting to the management

> "Balbix provides each IT administrator with a customized dashboard containing dozens of operational and analytical widgets specific to their area of responsibility."

— Daniel Gisler, CISO, Oerlikon

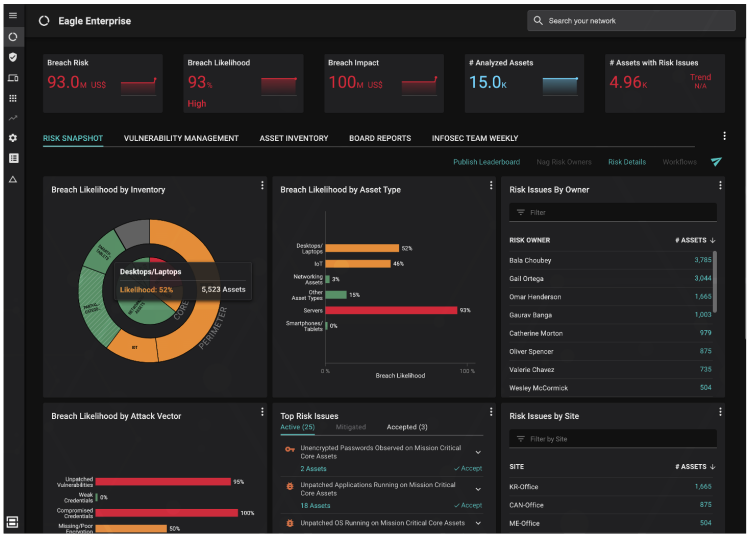
Communicating Security to Stakeholders

As the CISO, communicating about Oerlikon's security posture to various stakeholders is a big part of Daniel's responsibilities.

"Snapshots are emotional. Trendlines, on the other hand, are factual. For far too long, we have based our cybersecurity decisions on emotions and chasing the next shiny new object. And we have been reactive to what's going on in the news. Balbix allows me to be completely data-driven and use facts to make my decisions. With dashboards and reports that give me a bird's eye view of my enterprise, I am also empowered to defend my decisions in front of the management and show the continued value we are extracting from our cybersecurity investments."

His security team also needed a way to quantify what cyber risk meant in a business sense: "All the typical indicators such as indicators of compromise and CVSS scores do not mean much to line of business owners," says Daniel. "We needed to talk about our security posture with context and relevance, so application owners understood what cyber risk meant to their business, and Balbix allowed us to do that."

> "Snapshots are emotional. Trendlines, on the other hand, are factual. For far too long, we have based our cybersecurity decisions on emotions. Balbix allows me to be completely data-driven and use facts to make my decisions. With dashboards and reports that give me a bird's eye view of my enterprise, I am also empowered to defend my decisions in front of the management..."
>
> **— Daniel Gisler, CISO, Oerlikon**



Example Dashboard in the Balbix Platform

To learn more about the Balbix platform and to see a 30-minute demo, get in touch.