FORESCOUT
See it. Secure it. Assure it.

DENEXUS

Manage Risk in OT Environments with Forescout and DeNexus

Joint Solution Brief

By merging network access visibility and control with risk assessment, companies can accurately articulate cyber risk in monetary terms to assess compliance and security requirements. Forescout and DeNexus have joined forces to offer outcome-driven cybersecurity insights and trends that provide ongoing risk assessments by highlighting crucial mitigation strategies and requirements for enterprises.

Challenges to Address

Continuous risk assessments in OT environments are vital to identify and mitigate cybersecurity risks that can impact critical infrastructure. Security breaches in OT systems can lead to severe consequences like operational disruptions, safety hazards, financial losses, and environmental damage.

Limited visibility: It can be difficult to obtain a comprehensive view of all network assets and their connections in OT environments, leading to gaps in the assessment of risks.

Resource-intensive processes: Collecting and analyzing network asset information in OT environments often require specialized tools and expertise, which can be costly to implement and maintain.

Complex infrastructure: OT environments may consist of diverse and legacy systems that are challenging to inventory and assess in terms of security risks.

Potential for business disruption: Inaccurate or incomplete asset information can result in misinformed risk assessments, potentially leading to costly downtime or breaches.

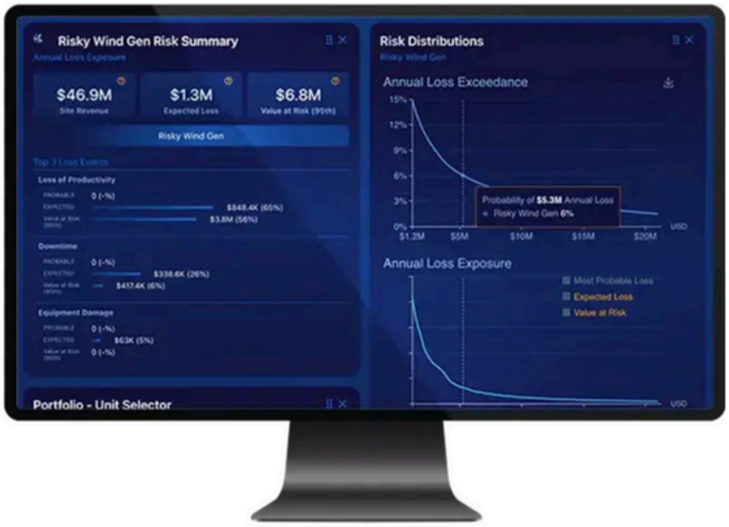
Compliance requirements: Meeting industry regulations and standards often necessitates investing in tools and processes to ensure proper asset management and risk assessment.

Architecture

Forescout gathers asset inventory metadata, offering a comprehensive list of features and vulnerabilities.

This information is then sent to the DeNexus DeRISK platform, where risk quantification metrics assist users in prioritizing mitigation efforts based on potential monetary loss.

DeRISK also uses the data from Forescout to highlight areas where users may have visibility gaps.



Advantages

- **Continuous vs. Point-in-Time Risk Assessments:** Cybersecurity assessments can help to provide some of these details, but they can be expensive, requiring specialized experts and months before the results are ready for decision-makers. The ICS/OT cybersecurity landscape is changing rapidly with new threats and vulnerabilities being disclosed daily. A static security assessment that takes months for collection to a report that is lagging the current threat landscape.

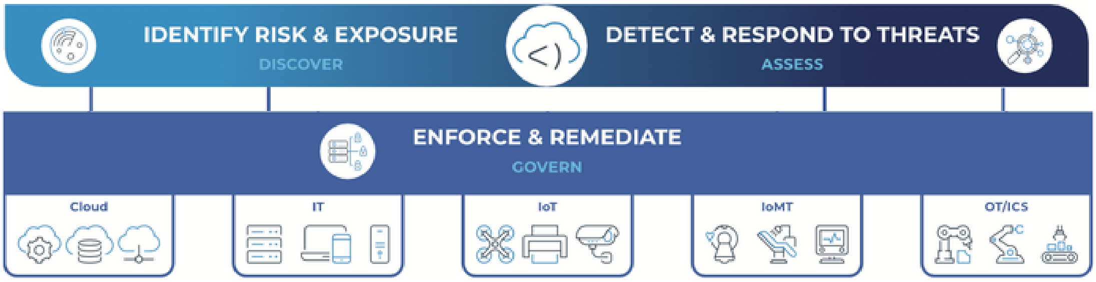
- **Drive Outcome-based Cybersecurity Indicators & Trends:** DeNexus DeRISK regularly pulls data from ForeScout eyeInspect and stores this history over time. DeRISK provides the leadership team with key indicators that show if their cybersecurity investments are making a difference, or if their risk is changing.

- **Communicate Cyber Risk in Dollars:** ICS/OT cybersecurity professionals often struggle to effectively communicate cyber risk to their executive leadership. Decisions at this level are often not reliant on data on the number of obsolete platforms, critical vulnerabilities, and potentially malicious events inside the ICS/OT system, but rather the probability of an event and the dollar impact of cyber incidents.

- **Risk Mitigation Budgeting:** Stakeholders struggle to provide evidence-based cyber risk mitigation options for their OT cyber security investments and measure the impact of their implementation in financial terms. DeRISK shows you the risk reduction impact of your cyber projects before you allocate your budget. Show your leadership team the ROI-based cyber risk mitigation projects in probabilities and dollars, not just in CVEs or compliance standards.

About Forescout

Forescout is the only automated cybersecurity vendor with a single platform for continuously identifying and mitigating risk across all managed and unmanaged assets – IT, IoT, IoMT and OT – from campus to data center to edge. For more than 20 years, we have delivered cybersecurity innovations that protect many of the world's largest, most trusted organizations in finance, government, healthcare, manufacturing and other industries.



The Forescout Platform delivers comprehensive capabilities for network security, risk and exposure management, and extended detection and response. With seamless context sharing and workflow orchestration via ecosystem partners, it enables customers to more effectively manage cyber risk and mitigate threats.

About DeNexus

DeNexus delivers a full-stack cyber risk quantification and management solution uniquely tailored to industrial sectors: energy, manufacturing, data centers, transportation and critical infrastructures with Operational Technology (OT). The company empowers stakeholders in cyber risk — CISOs, risk managers, executives, boards of directors, and insurers — to grasp the financial impact of cyber incidents and optimize cybersecurity programs.

Employing internal and external data, AI and millions of simulation runs, DeNexus calculates the likelihood of cyber events, quantifies risk in financial terms and identifies most effective risk mitigation strategies. DeNexus is trusted by Global 1000 companies across three continents offering an evidence-based methodology to optimize cybersecurity investments and reduce/transfer risk.

Learn More

Schedule a demo at forescout.com | denexus.io