Troux Technology Lifecycle Management for Cyber Security

Troux enhances cyber security programs by providing essential insight into technology risk to help executives and IT professionals develop a plan to mitigate the risk of cyber-attacks. According to cyber security experts we've reached a tipping point in cyber-crime. Cyber-crime affects more than 200 million users worldwide every year. The protection of valuable intellectual property and business information is now a critical business management issue. Troux helps business and IT leaders reduce the risk of cyber attacks by identifying end-of-life technologies that exist across the enterprise.

Key Benefits

- Identify what IT assets are currently in use across the enterprise
- Quickly see the life-cycle phase for asset in use
- Simplifies the identification of unsupported technologies that put the enterprise at-risk to a cyber attack
- Ease in understanding the business capabilities and information that are impacted as a result of end-of-life technology

Opening the Door to Cyber Risk

The rate and maliciousness of cyber security threats against large enterprises is accelerating. To make matters even worse the ability to address these threats is often made more complicated by the business's inability to understand what technologies are in place as well as the impacts associated with the out-of-date technology assets that present easy points of entry for hackers.

The continued surge of obsolete IT infrastructure and applications is effectively creating an open door to cyber attacks that targets valuable intellectual property, business critical information and confidential data.

It's All Connected

In today's connected enterprise the number of interconnected technology assets make it burdensome if not improbable for an enterprise to identify cyber security impacts created by the vulnerabilities from just one application.

Consequently, if an application were to become compromised, the dependencies of other corporate applications would hinder timely recovery from a security breach. Minimizing the information security impact of cyber security breaches demands an understanding of how the different pieces and dependencies of an enterprise technology portfolio fit together.

Identify, Rationalize and Roadmap

Troux helps enterprises address the cyber security challenges that come along with the inability to properly identify and rationalize technology assets that have reached or will reach their end-of-life date. Troux provides business and IT stakeholders with the visibility and transparency needed to properly identify the existing software and hardware assets that present end-of-life risks to ensure information security risks are minimized.

Once this identification is complete, Troux delivers the insights needed to evaluate technology portfolio remediation alternatives in the context of the business capabilities that will be impacted most. Technology remediation proposals are turned into intuitive visual scenarios, which can be compared against each other to identify the appropriate course of action. Final portfolio change initiatives can then be roadmapped and communicated across the business to drive execution.

Answer the Right Questions

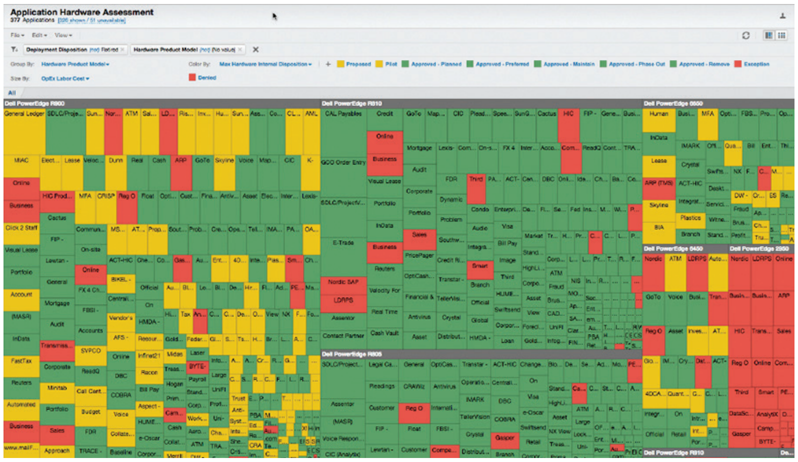
To ensure cyber security risks are minimized Troux delivers the enterprise intelligence business leaders need to see the big picture and better understand exactly where they should be addressing exposures across their technology portfolio. Enterprise intelligence delivers new levels of transparency and enables business stakeholders and technology owners to answers important technology portfolio planning questions such as:

1. What applications and technologies are deployed across the business and who owns them?

2. What applications and technologies are about to go unsupported due to their end-of-life date?

3. What business capabilities are impacted due to these unsupported technologies?

4. What critical assets are exposed to cyber threats based on these vulnerabilities?



Application Hardware Assessment
377 Applications [326 shown / 51 unavailable]

Deployment Disposition (not) Retired
Hardware Product Model (not) (No value)

Group By: Hardware Product Model
Color By: Max Hardware Internal Disposition
Size By: OpEx Labor Cost

🟨	Proposed
🟨	Pilot
🟩	Approved - Planned
🟩	Approved - Preferred
🟩	Approved - Maintain
🟩	Approved - Phase Out
🟩	Approved - Remove
🟥	Exception
🟥	Denied

Application Hardware Assessment Heat Map helps identify applications that are running on at-risk hardware

5. Do our application and technology remediation plans mitigate future cyber threats?

Understanding the answers to these questions enables the IT team to focus their efforts on proactively addressing the end-of-life applications and technologies that support the most sensitive assets and have the highest exposure to cyber threats.

Key Features

Technology Inventory and Relationship Perspectives delivers a family of out-of the-box capabilities and perspectives that provide decision makers with an easy way to establish a single source of record for all enterprise technologies and view their relationships to business capabilities, organizations, people and projects.

Technology Assessment Perspectives standardizes the assessment of technologies that are nearing end-of-life against a set of predefined qualitative and quantitative criteria such as cost, redundancy, risk, regulatory compliance, capability alignment and strategic fit. Areas of concern can be identified and change initiatives can be planned to take corrective action.

Technology Remediation Perspectives enables decision makers to see what remediation initiatives (e.g. application retirement, upgrade, replacement) should be considered to minimize cyber threats.

Technology Roadmapping and Planning helps business leaders see the impact of proposed technology portfolio changes on business capabilities. Remediation proposals can be roadmapped and compared against each other to identify the best course of action.