

# Cyence Risk Analytics

A risk assessment tool for cyber underwriters

The Cyence Risk Analytics dashboard provides a comprehensive overview of Nordstrom, Inc.'s cyber risk profile. Key metrics include:

- Overall risk grade:** C (54) - Percentile: 41st
- Probability of incident:** 15.4% - Percentile: 16th
- Average Annual Loss (AAL):** \$8.8M - Percentile: 34th
- Top exposure signals:** Spam activity (Detected), Foreign hacker activity (Detected), Network complexity (High)
- Breakdown of probability of incident:** Data breach probability: 10.4%, Ransomware probability: 8.2%
- Ground up AAL:** \$8,842,106

Legend for coverage types:

- Liability: \$187,432
- First Party Data Breach: \$7,831,937
- Business Interruption: \$113,306
- Contingent Business Interruption: \$708,920
- Cyber Extortion: \$210



# About Cyence Risk Analytics

Cyence is a cyber risk analytics tools used by underwriters to evaluate a risk of a business with online presence.

The underwriters than use this information to make underwriting and pricing decision.

It helps them to underwrite a risk with appropriate premium for insuring an online / digital business.

## Team

1 UX Designer, 1 Product Manager, 1 Data Scientist, 1 Subject Matter Expert

# Persona

## Cyber Underwriter

### ⚠ Problems:

- I don't have enough information to determine a business risk.
- Risk evaluation is a time taking process due to administrative tasks.
- I struggle with gathering information about possible next action based on identified risk.

### ❑ Needs:

- I need to understand a company's risk faster and efficiently.
- I need actionable items to make effective underwriting decisions.

"I identify, understand, measure, and evaluate highly complex risk and provide applicable terms and conditions to make profitable decisions for my company."



I instantly gain differentiating insights to identify emerging risks.

I obtain necessary data points to write a company and determine pricing efficiently.

I am able to quantify risk based on experience history and forecasting methods.



### MY RESPONSIBILITIES AND DECISIONS...

#### Solicit new and renewal submissions:

- What information do I need to collect to complete the submission?

#### Determine appropriate pricing of complex risks:

- How should the company be priced? How do I justify the risk I write?

#### Analyze highly complex risks underwritten:

- How do I evaluate the quality, quantity, and profitability of risks I write?

#### Interact with Agents:

- How can I engage them around why information is needed?

### I'M FRUSTRATED WHEN...



- I don't have enough information to determine a business' risk.
- I'm unable to locate and document risk evaluation data.
- Valuable time is spent on administrative tasks.
- I can't keep up with trends in the quickly evolving marketplace.
- It's hard to differentiate from competition based on pricing and offerings.

### MY SUCCESS IS MEASURED BY...



- The number of profitable businesses written.
- Growth of the company portfolio.
- Quality of interactions with Agents and colleagues.
- Timeliness and accuracy.
- Compliance with guidelines.

### DESIGNING FOR JAMES:

I need clear guidance on how to use the tool and I want to understand how it can improve my work efficiency. It's important that I be able to effectively integrate it within my risk evaluation process.

I want to leverage the power of the tool to understand a company's risk thoroughly. Standardized metrics with easy-to-understand visualizations can be very helpful.

# Design Process

The design process is broken down in 2 stages

## Pre-production

 User Research

 Ideation & Design

 Usability Testing

 Reiterate Design

 Deliver & Develop

## Post-production

 Onboarding Design

 Release

 In-App UI Feedback

 Track Usage

 Design Backlog



# User Research

## Research Insights:

- # of customer involved: **7**
- # of users: **10** (Underwriters and Underwriter leadership)
- Research set up: **1hr online zoom calls**

## Research Goals:

- To understand the reason behind identified usage patterns.
- To understand how users are currently using all the information within application.
- To identify problems and friction points users are facing while using our risk analytics tool.



## 4 key identified problems...



Hard to understand the correlation between data



Hard to find impactful and most concerning information



Don't know what to do with certain information

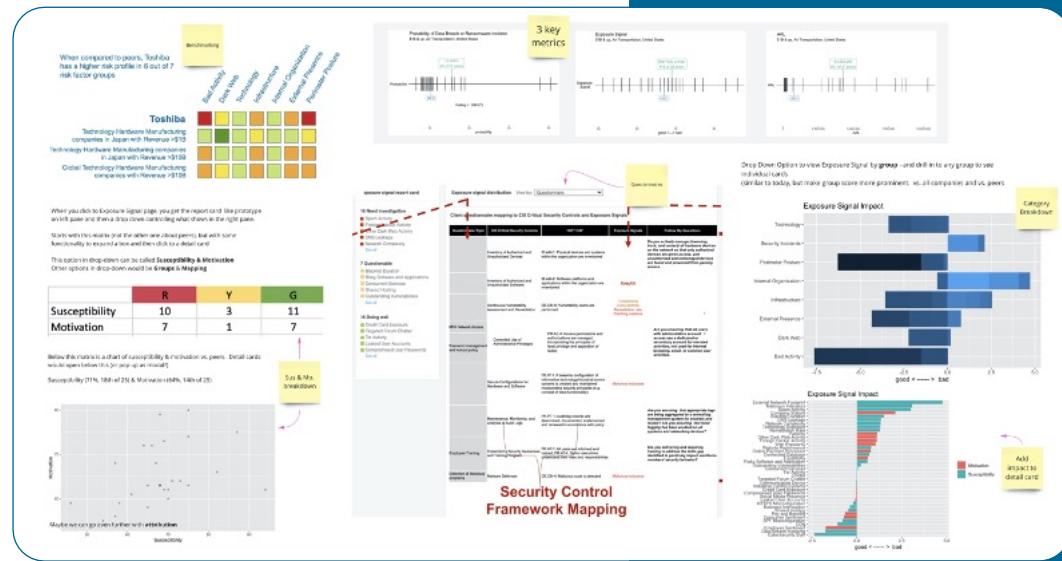


Found the UX and printable report old and outdated

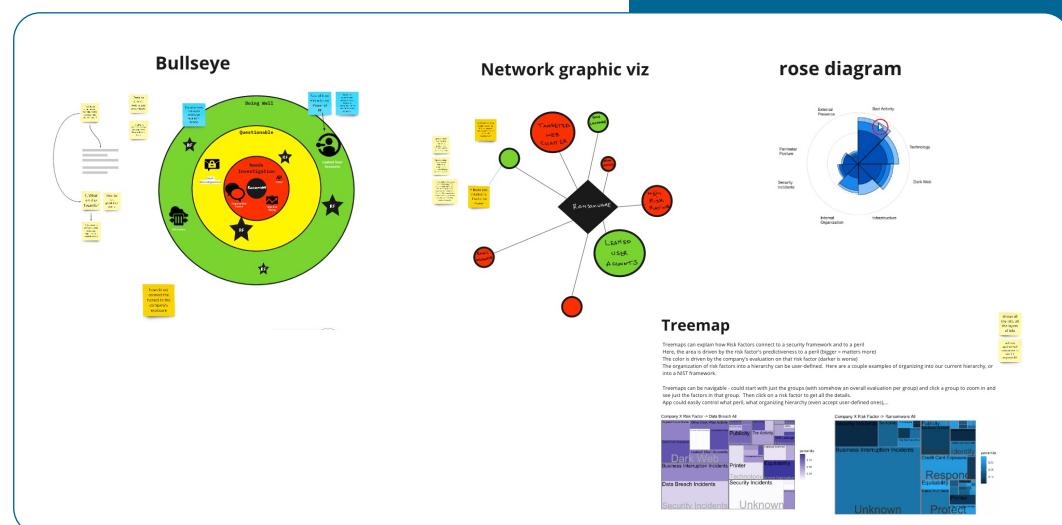
# Proposed Solution

- Provide users a clear representation about the correlation of different data points throughout the UI.
- Revamp the overview page with most important information in order to increase productivity.
- Provide help text and guide to enable users to understand the usage of information along with actionable measures.
- Provide users a new experience for the downloadable report format like new UI.

Ideation board

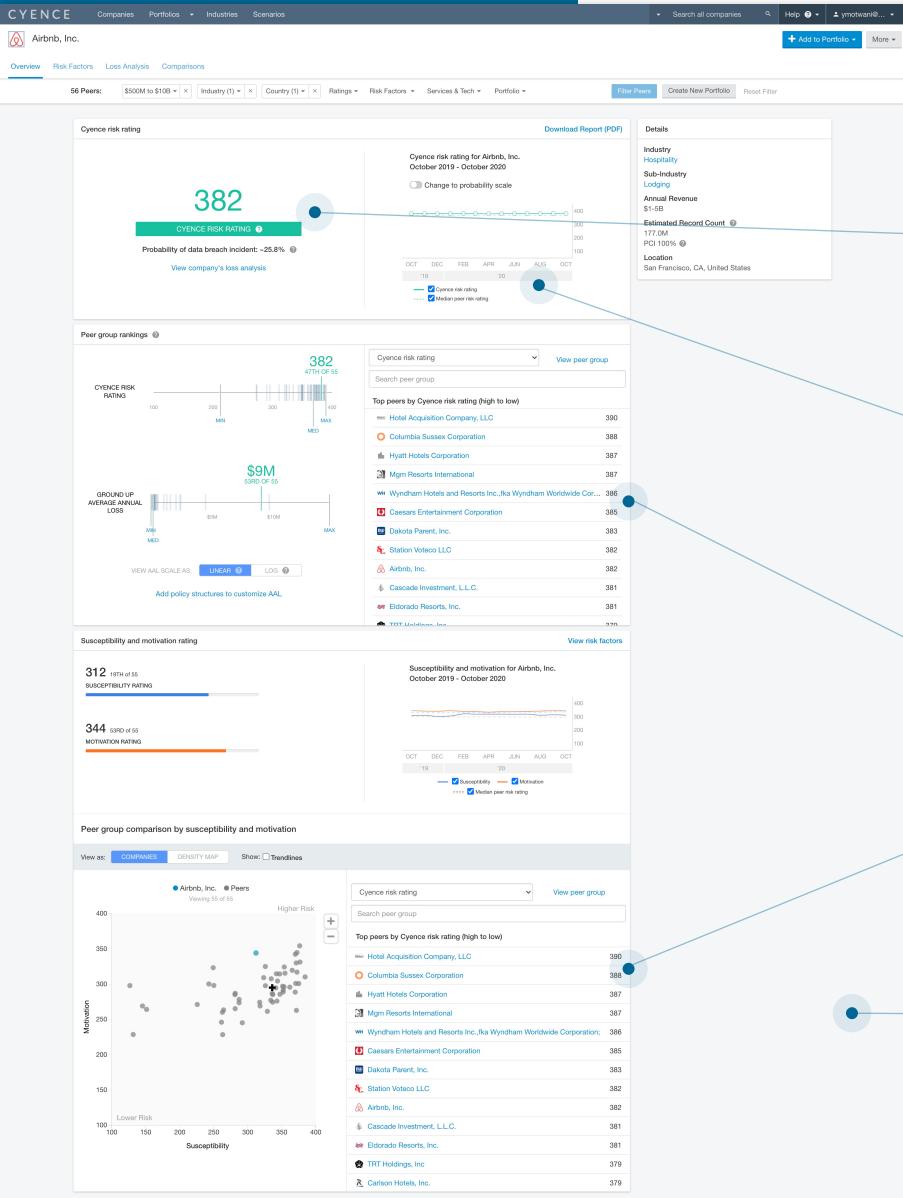


Data visualization exploration



# Company Overview Page

## Problems with old UX



01

A primary metric which is usually misunderstood by underwriters

02

Historical trend is a secondary information but is highly emphasized on UI

03

Repeated information and list of ranking which is not used that often

04

A lot of white space and different metrics spread out in a long page

# Company Overview Page

C Y E N C E Companies Portfolios Industries Scenarios

Nordstrom, Inc.

Industry Retail Trade Sub-Industry Department Stores # of subsidiaries 2 Annual revenue \$50-\$70B Estimated record count 315.2M • PCI 100% Employee count 10,000+ Location San Mateo, California, USA

Add to Portfolio Cyence Risk Report

Overview Exposure Signals Security Measures Loss Analysis Peer Comparison 39 peers filtered Filter Peers

**Exposure Signals** Areas that may have cyber vulnerabilities

Overall risk grade C (54) Percentile: 41st Risk grade and score, and position as compared to 39 peers

View peer group ranking

Probability of Incident Chance of experiencing a cyber incident

Overall probability of incident In percent (%), as compared to 39 peers

15.4% Percentile: 14th

View peer group ranking

Loss Analysis Expected cyber loss per year, averaged over many years

Average Annual Loss (AAL) In USD (\$), as compared to 39 peers

\$8.8M Percentile: 84th

View peer group ranking

Top exposure signals Viewing 3 exposure signals that need investigation

Spam activity Detected

Foreign hacker activity Detected

Network complexity High

View 13 More

Breakdown of probability of incident In percent (%)

10.4% Data breach probability

8.2% Ransomware probability

Ground up AAL: \$8,842,106 Breakdown of coverages type

- Liability: \$187,432
- First Party Data Breach: \$7,831,937
- Business Interruption: \$113,306
- Contingent Business Interruption: \$708,920
- Cyber Extortion: \$210

© 2015-2021 Cyence LLC  
Privacy Policy | Terms of Use | Cyence Support

## New UX

### New Information Architecture

New hierarchy of information to highlight the most important information up front.

### Simplified Layout & Insights

New 3 column layout to provide the distinction of 3 different data points to identify risk.

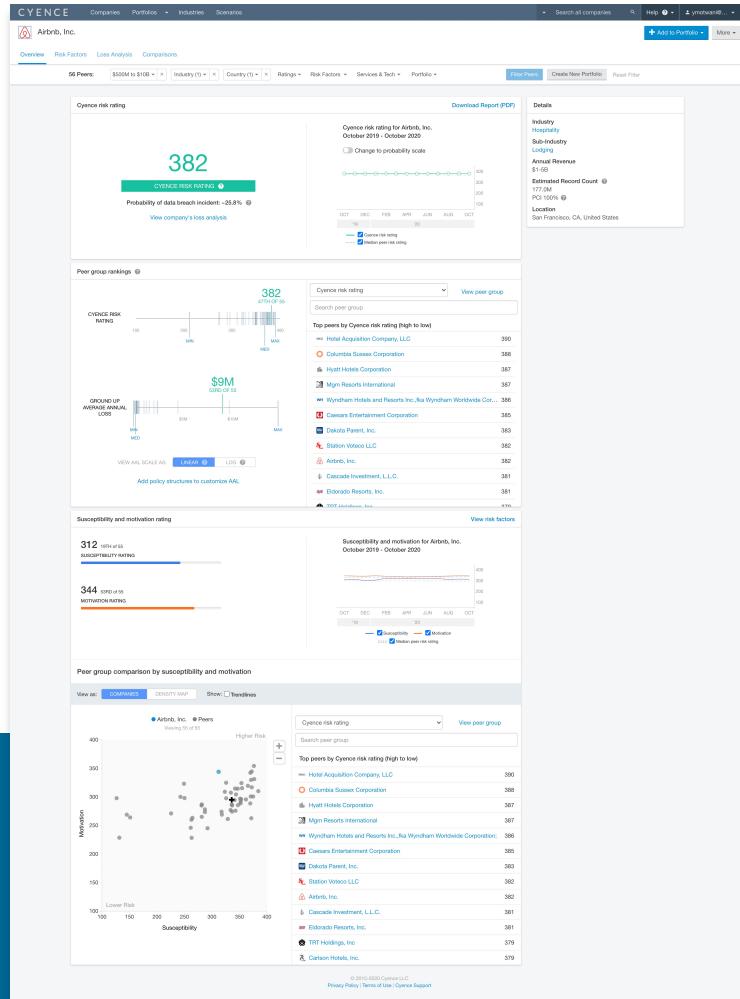
### Simplified Data Visualization

Sparkline graphs to show the history trendlines for different data points to further simplify the experience.

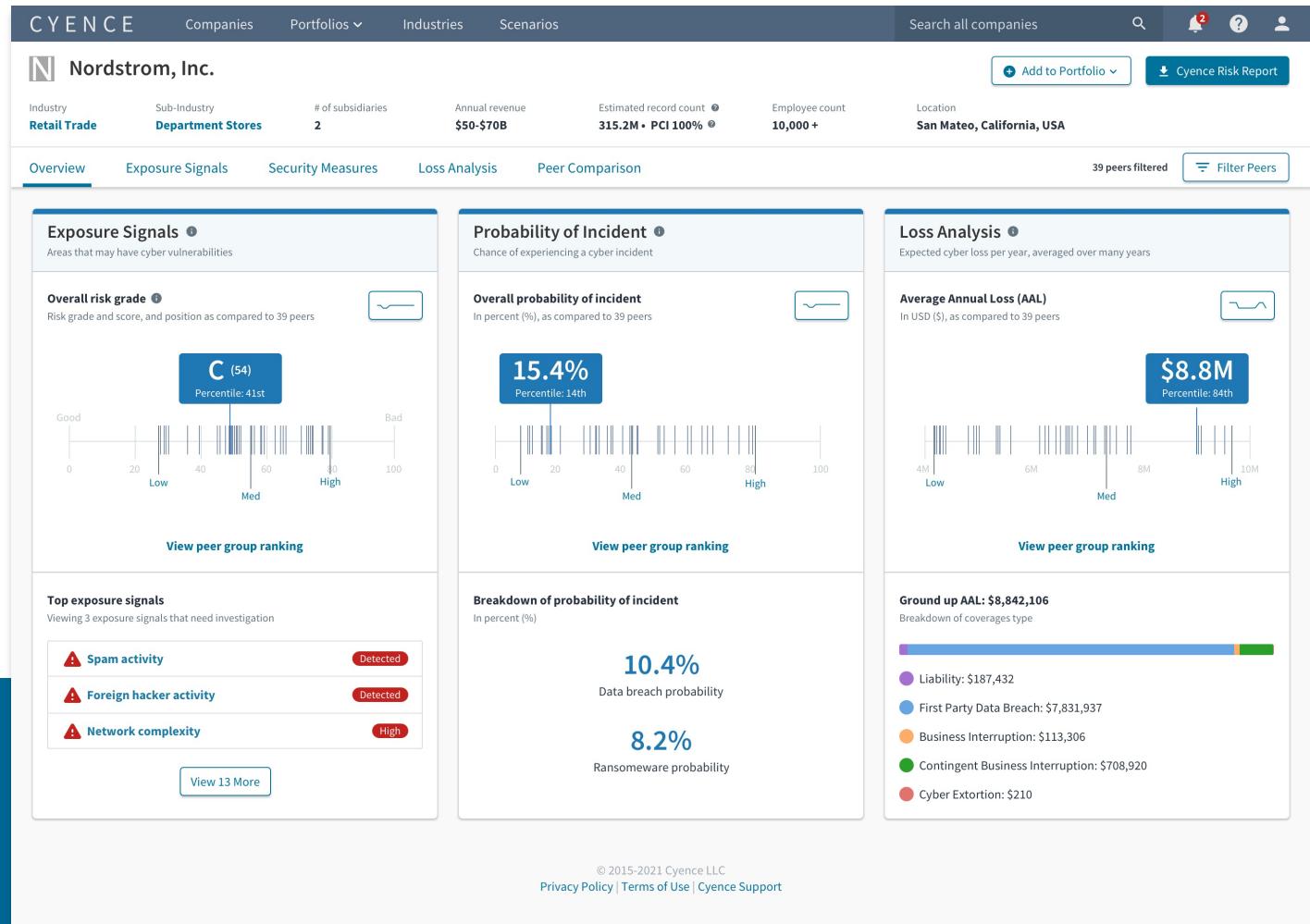
# Old vs New UX

## Company Overview Page

### Old UX



### New UX



**CYENCE** Companies Portfolios Industries Scenarios Search all companies Help ymotwani@... Add to Portfolio More

Overview Risk Factors Loss Analysis Comparisons

56 Peers: \$500M to \$10B Industry (1) Country (1) Ratings Risk Factors Services & Tech Portfolio Filter Peers Create New Portfolio Reset Filter

**Top risk factors**

- Positive Risk Factors**
- Negative Risk Factors**

**Infrastructure**

**Employee Sentiment** – Happy workforce

**Infrastructure**

**SPF Misconfiguration** – Not detected

**Dark Web**

**Leaked User Accounts** – Detected

**External Presence**

**Company Stature** – Extensive footprint

**All risk factors**

**Bad Activity** – Improved

**Dark Web** – Unchanged

**Technology** – Unchanged

**Infrastructure** – Worsened

**Internal Organization** – Unchanged

**External Presence** – Improved

**Perimeter Posture** – Unchanged

**Security Incidents** – Unchanged

**Services & technologies**

**Service provider** (5)

- Acmail (All Regions)
- CDN provider
- Amazon Virginia (East US/Canada) (Cloud service provider)
- CloudFlare (All Regions) (CDN provider)

Show More

**Software** (17)

- Apache HTTP Server (Web server)
- Mail server
- Drupal (Web application)

Show More

**Payment processor** (13)

- Adyen
- Alipay
- American Express

Show More

Expand All

No peers are better

98% of peers are better

2% of peers are better

23% of peers are better

4% of peers are better

82% of peers are better

5% of peers are better

73% of peers are better

© 2015-2020 Cyence LLC  
Privacy Policy | Terms of Use | Cyence Support

# Exposure Signals Page

## Problems with old UX

01

Underwriters didn't care about positive risk factors

02

Showed high impact risk categories but didn't tell users what's driving it or any actionable insights

03

A lot of white space and when the cards expanded, it leads to scrolling

The screenshot shows the CYENCE platform interface for Nordstrom, Inc. at the top. Below it, the main content area displays the 'Exposure Signals' page.

**Header:** CYENCE Companies Portfolios Industries Scenarios Search all companies

**Company Info:** Nordstrom, Inc. Industry: Retail Trade, Sub-Industry: Department Stores, # of subsidiaries: 2, Annual revenue: \$50-\$70B, Estimated record count: 315.2M + PCI 100%, Employee count: 10,000+, Location: San Mateo, California, USA.

**Navigation:** Overview, Exposure Signals (selected), Security Measures, Loss Analysis, Peer Comparison, 39 peers filtered, Filter Peers.

**Exposure Signal Breakdown:** Overall Exposure Signal: C (54). Categories: Technology, Risk Grade: D (74), Peer Comparison: 79% of peers are better. A tree view shows:

- Exposure Signals: Online Payment Processor (Detected), Risky Software and Applications (Restrained), Connected Database (Not Detected), Technology Exposure (Low), Communication Device (Not detected), Exposed Printers (Not detected).
- Status: Detected (red), Restrained (orange), Not Detected (green).
- Impact: - (red), - (orange), + (green).

**Exposure Signal Report Card:** Total Exposure Signals: 39. Categories: Worse than Peers (6 red, 2 orange, 2 green), Similar to Peers (9 red, 4 orange, 13 green), Better than Peers (1 red, 1 orange, 1 green). Needs investigation (16): Spam Activity (Detected), Compromised User Passwords, DNS Leakage. Suspicious (7): Network Complexity, Risky Software and Applications, Shared Hosting. No issues (16): HTTPS Misconfiguration, Targeted Forum Chatter, Connected Database.

**Report Card Detail:** All (39) Pinned (2). Spam Activity (Detected): Propagation of unsolicited junk email distributed to a large number of recipients. IP Address detected: 48.155.250.79, 214.46.244.249, 196.64.8.69, 109.219.90.255. Underwriting Considerations: Questionnaire and actions we recommend based on different security frameworks like CIS and NIST. Ask your client:
 

- Do you block all email attachments entering your org's email gateway if the file types are unnecessary for the organization's business?
- Do use sandboxing to analyze and block inbound email attachments with malicious behavior.
- Do you use DNS filtering services to help block access to malicious domains?

 Was it helpful?

# Exposure Signals Page

## New UX

Exposure Signals is the most used page in the app, and as part of improvement we wanted to make this more effective and useful for our users by introducing:

### ① Updated Prioritization

The new prioritization was based on type of signal and severity. Now users can also pin them.

### ② Introduced Report Card

To enable users easily navigate through most concerning risks.

### ③ Simplified Data Visualization

A tree view for underwriters to identify the most vulnerable risk through grading and risk impact.

### ④ Actionable Security Measures

We provided our users a set of follow up questions they can ask to their customers to mitigate the risk.

# Old vs New UX

## Exposure Signal Page

### Old UX

This screenshot shows the old CYENCE platform's exposure signal page for AirbnB, Inc. The top navigation bar includes links for Companies, Portfolios, Industries, Scenarios, and a search bar. Below the header, there are tabs for Overview, Risk Factors, Loss Analysis, and Comparisons. The main content area is divided into several sections:

- Top risk factors:** A comparison between Positive Risk Factors (e.g., Infrastructure, Internal Organization) and Negative Risk Factors (e.g., Dark Web, Compromised User Passwords).
- Services & technologies:** A list of service providers and software used by the company.
- Overall risk grade:** Shows the overall risk grade and the percentage of peers that are better or worse.
- Peer Comparison:** A detailed breakdown of how the company compares across various categories like Technology, Security Incidents, and Infrastructure.
- Bad Activity:** A section detailing specific不良行为 (Bad Activity) such as Bad Web, Technology, Infrastructure, and Internal Organization.
- External Presence:** A section detailing the company's presence on the dark web.
- Perimeter Posture:** A section detailing the company's network security posture.
- Security Incidents:** A section detailing recent security incidents.

The bottom of the page includes a footer with copyright information and links to Privacy Policy, Terms of Use, and Support.

### New UX

This screenshot shows the updated CYENCE platform's exposure signal page for Nordstrom, Inc. The layout is more modern and organized:

- Header:** Includes the company logo, name, industry (Retail Trade, Department Stores), number of subsidiaries (2), annual revenue (\$50-\$70B), estimated record count (315.2M), employee count (10,000+), and location (San Mateo, California, USA).
- Top navigation:** Similar to the old version, with tabs for Overview, Exposure Signals, Security Measures, Loss Analysis, and Peer Comparison.
- Exposure Signal Breakdown:** A central card showing the overall exposure signal (C (54)) and the percentage of peers that are better.
- Peer Comparison:** A detailed breakdown of how the company compares across various categories like Technology, Security Incidents, and Infrastructure.
- Exposure Signal Report Card:** A summary card showing the total exposure signals (39) and a grid comparing the company to peers across three categories: Worse than Peers, Similar to Peers, and Better than Peers.
- Details:** A large list of specific exposure signals categorized by risk level (Red, Orange, Green) and status (Detected, Significant). Examples include Spam Activity, Compromised User Password, DNS Leakage, Network Complexity, Risky Software and Application, Shared Hosting, and Foreign Hacker Activity.

# Downloadable Report

## Old UX

Nordstrom, Inc.  
Cyence Unique ID: b10e9f1e  
Report generated on December 14, 2020  
with data from November 2020

**Company Overview**  
Nordstrom, Inc.  
Cyence Unique ID: b10e9f1e

**Company Overview**

Cyence Risk Rating	Susceptibility Rating	Motivation Rating
388 Out of 400	368 Out of 400	347 Out of 400
Peer range: 335-390	Peer range: 290-379	Peer range: 231-357
Peer median: 376	Peer median: 334	Peer median: 311

See following report for further details.

**Company Details**

**Details**

Industry: Retail Trade  
Sub-Industry: Apparel Retailers  
Annual Revenue: \$10-50B  
Estimated Record Count: 262.4M  
PCI 100%  
Location: Seattle, WA, United States

**Services & Technologies**

Service provider (13 found)  
Software (22 found)  
Payment processor (5 found)  
Auditor (1 found)

Refer to the Appendix for full listing of Services and Technologies.

This document and any recommendations, analysis, or advice provided by Cyence LLC ("Cyence") (collectively, the "Analysis") is intended solely for the entity identified as the recipient and is not to be distributed outside of that entity without the express written consent of Cyence and is intended for your internal use only, and may not be shared with any third party without Cyence's prior written consent. Any statements concerning professional advice, including recommendations and analyses, set forth in the Analysis are based on information and data that has been collected and analyzed by Cyence. The Analysis is not based upon any professional advice, for which you should consult your own professional advisors. Any mention of specific companies, products, services, or technologies is for illustrative purposes only and does not imply that they will be used or recommended. The Analysis may not be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources believed to be reliable, but its accuracy or completeness cannot be guaranteed or assured. All representations and warranties, express, implied, or statutory, including any implied warranty of merchantability, fitness for a particular purpose, title, non-infringement, and implied warranties of fitness for a purpose, are disclaimed and the Analysis is provided "as-is." Without limiting the foregoing, Cyence makes no warranty, guarantee, or representation, express or implied, that the Analysis will meet your or any other party's requirements, or achieve any intended result. Cyence shall have no obligation to update the Analysis and shall have no liability to you or any other party with respect to the Analysis or any other information or data provided in the Analysis. By accepting and/or using this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 3 of 39

**Company Overview**  
Nordstrom, Inc.  
Cyence Unique ID: b10e9f1e

**Company Overview**

Cyence Risk Rating	Susceptibility Rating	Motivation Rating
388 Out of 400	368 Out of 400	347 Out of 400
Peer range: 335-390	Peer range: 290-379	Peer range: 231-357
Peer median: 376	Peer median: 334	Peer median: 311

**Risk Overview**

Cyence Risk Rating	Risk Rating
388 Out of 400	The Cyence Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a data breach or other cybersecurity incident due to the handling of protected information. This is derived from a combination of technical and non-technical indicators, including the company's Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

**Probability of Data Breach**  
~36.4%

**37th of 39**  
Among its peer group of 39 companies

**Peer Risk Comparison**

Peer of Nordstrom, Inc., have Risk Ratings ranging from 335 to 390. The median Risk Rating among peers is 376.

Refer to the Appendix for peer group details.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 4 of 39

**Company Overview: Risk Overview**  
Nordstrom, Inc.  
Cyence Unique ID: b10e9f1e

**Risk Overview**

Cyence Risk Rating	Risk Rating
388 Out of 400	The Cyence Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a data breach or other cybersecurity incident due to the handling of protected information. This is derived from a combination of technical and non-technical indicators, including the company's Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

**Probability of Data Breach**  
~36.4%

**37th of 39**  
Among its peer group of 39 companies

**Risk Rating**

The Cyence Risk Rating is a measure of a company's cyber risk, or the likelihood that it would experience a data breach or other cybersecurity incident due to the handling of protected information. This is derived from a combination of technical and non-technical indicators, including the company's Susceptibility, Motivation, and Risk Factors. Based on a 100-400 scale, a higher Risk Rating indicates greater risk.

**Probability of Data Breach**  
The Probability of Data Breach is mapped to the Cyence Risk Rating. This represents the probability of a company having at least one breach over the next 12 months. Actual probabilities are estimates and actual probabilities may vary.

**Peer Risk Comparison**

Peer of Nordstrom, Inc., have Risk Ratings ranging from 335 to 390. The median Risk Rating among peers is 376.

Refer to the Appendix for peer group details.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 4 of 39

**Company Overview: Risk Overview**  
Nordstrom, Inc.  
Cyence Unique ID: b10e9f1e

**Historical Rating Over Time**

Risk

NOV '19 JUN '20 NOV '20

**Historical Probability Over Time**

Probability

NOV '19 JUN '20 NOV '20

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 5 of 39

**Risk Factors: Top Risk Factors**  
Nordstrom, Inc.  
Cyence Unique ID: b10e9f1e

**Top Risk Factors**

Top Risk Factors are the most significant factors impacting a company's Risk Rating. Positive Risk Factors are those that reduce a company's Risk Rating, while Negative Risk Factors are those that increase a company's Risk Rating.

**Positive Risk Factors**

- Infrastructure
- Cloud Environment
- CDNs offer redundancy and the ability to absorb or neutralize potential threats to a site like DDoS, diversifying the company's risk through an added layer of security.

**Negative Risk Factors**

- SPP Misconfiguration - Not detected
- A carefully tailored SPP record in the Domain Name System protects the company against email spoofing. The absence or improper configuration of SPP exposes the company to fraudulent use of its domain name for spam and phishing emails carrying fake sender addresses.
- Internal Organization
- Employee Sentiment - Content workforce
- Employees are responsible for a significant portion of cybersecurity breaches, either deliberately (by performing the attack themselves or collaborating with an outsider), or unwittingly (by engaging in risky behavior or falling victim to social engineering tactics). Poor internal sentiment increases not only the likelihood of inside job hacks, but also the risk of external attacks that prey on human error.
- Dark Web
- Compromised User Passwords - Detected
- Combinations of employee usernames and passwords may be used by malicious actors to gain access to corporate accounts, especially given the prevalence of password reuse.
- External Proxies
- Competitor Status - Extensive Footprint
- A company who holds top of mind awareness with the public also makes a more striking target in the eyes of criminal hackers.

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 10 of 39

# Downloadable Report

New UX

**GUIDEWIRE**

Cyence Risk Report for  
**Care Wear, Inc.**

Unique ID: bdqoeybjreq  
Report generated on February 26, 2020  
with data from November 2019

This document and any recommendations, analysis, or advice provided by Cyence LLC ("Cyence") (collectively, the "Analysis") is intended solely for the entity identified as the recipient herein ("you"). This document contains proprietary, confidential information of Cyence and is intended for your internal use only, and may not be shared with any third party without Cyence's prior written consent. Any statements concerning professional advice, including but not limited to actuarial, tax, accounting, or legal matters, are not to be relied upon as professional advice, for which you should consult your own professional advisor. Cyence makes no representations or warranties regarding the accuracy of the Analysis. The Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy or completeness. All representations and warranties made by Cyence, including implied warranties of merchantability, fitness for a particular purpose, title, non-infringement of intellectual rights, from course of dealing, usage or trade practice, are disclaimed and the Analysis is provided "as-is." Without limiting the foregoing, Cyence makes no warranty of any kind that the Analysis, or any results of the use thereof, will meet your or any other party's requirements, or achieve any intended result. Cyence shall have no obligation to update the Analysis and shall have no liability to you or any other party with regard to the Analysis or to any services provided by a third party to you by Cyence. By accepting and/or using this report, you acknowledge and agree to the terms, conditions and disclaimers set forth above.

Care Wear, Inc.  
Cyence Unique ID: bdqoeybjreq

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 2 of 35

Company Overview

## Care Wear, Inc.

**Company Overview**

Industry: Retail Trade  
Sub-Industry: Apparel Retailers  
Annual Revenue: \$10-50B

Estimated Record Count: 262.4M  
PCI 100%  
Location: Seattle, WA, United States

**Risk Overview**

**Risk Rating**

**310** of 400  
Based on 15.4% probability

**51st Percentile**  
Peer range: 290-400  
Peer median: 320

**Probability of Incident**

**15.4%**  
Probability in percent (%)

**26th Percentile**  
Peer range: 12% - 49%  
Peer median: 24%

**Average Annual Loss**

**\$8.1m**  
Losses in USD (\$)

**72nd Percentile**  
Peer range: \$3.1 - 9.4m  
Peer median: \$5.3m

Change in history



Nov '19 Jan Mar May Jul Sep Nov '20

Change in history



Nov '19 Jan Mar May Jul Sep Nov '20

Change in history



Nov '19 Jan Mar May Jul Sep Nov '20

This Company Peer Median

Care Wear, Inc.  
Cyence Unique ID: bdqoeybjreq

Confidential - Presented to Cyence LLC - For Internal Use Only

Page 2 of 35

Top Exposure Signals

## Top Exposure Signals

Based on peer comparison

**Needs investigation**

**Spam activity** Propagation of unsolicited junk email distributed to a large number of recipients Detected

**Foreign hacker activity** Discussions about the company conducted in non-English forums (such as Russian, Chinese, etc.) Detected

**Network Complexity** Measure of breadth and intricacy of the company's external network based on an evaluation of its DNS (Domain Name System) hierarchy High

**Suspicious**

**Network Complexity** Lorem Ipsum is simply dummy text of the printing and typesetting industry. Detected

**Risky Software and Applications** Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy. Detected

**Shared Hosting** Lorem Ipsum is simply dummy text of the printing and typesetting industry. Lorem Ipsum has been the industry's standard dummy text ever since the 1500s. High

Care Wear, Inc.  
Cyence Unique ID: bdqoeybjreq

Confidential - Presented to Cyence LLC - For Internal Use Only

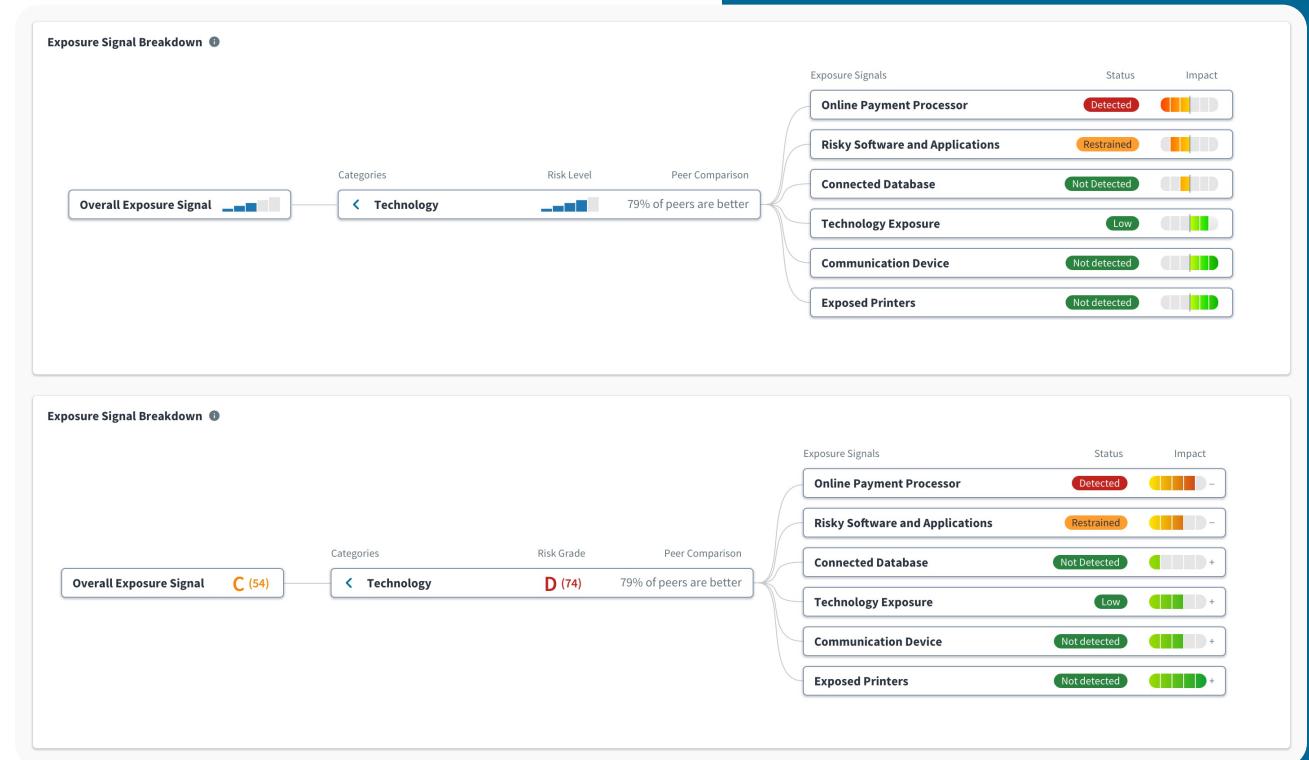
Page 3 of 35

# Usability and A/B Testing

## Risk Rating (Graph vs Grading)

We conducted A/B testing for deciding different data visualization and risk scaling system.

We ended up with Grading system because users were interested in granular differences of different risk level.



# Onboarding Design Process

List features & define steps

Create & review content

Create & publish guide

Topics	Changes	Pendo Walkthrough
Overview page (3 column layout)	<ul style="list-style-type: none"> <li>1. Top 3 exposure signals and security measures questionnaire snippet</li> <li>2. Probability of incident (including DB and RW breakdown) along with Risk Rating.</li> <li>3. Loss Analysis with AAL and Breakdown of coverages</li> </ul>	<p>Step 1: Highlevel 3 layout</p> <p>Step 2: New historical trend line</p>
Exposure Signal page	<ul style="list-style-type: none"> <li>1. Interactive Report Card           <ul style="list-style-type: none"> <li>◦ View by peer comparison</li> <li>◦ View by Sus/Mo.</li> <li>◦ Top 3 exposure signals of High, Medium, Low type</li> </ul> </li> <li>2. Exposure signal detail changes           <ul style="list-style-type: none"> <li>◦ Icons in addition to color for High, Medium, Low</li> <li>◦ Updated UI view on closed card</li> <li>◦ Past 3 month changes instead of 2 previously</li> <li>◦ Security Measure questionnaire</li> <li>◦ Security control mapping</li> </ul> </li> </ul>	<p>Step 3: Report Card</p> <p>Step 4: In context security measures and control mapping.</p>
Security Measures page	<ul style="list-style-type: none"> <li>1. NIST/CIS Security Measures           <ul style="list-style-type: none"> <li>◦ Common questionnaire for both frameworks</li> <li>◦ Downloadable questionnaire</li> <li>◦ Search for ESig withing Security Measures</li> <li>◦ Default sorting of ESig from High-Low</li> </ul> </li> </ul>	<p>Step 5: What is Security Measures?</p> <p>Step 6: Downloadable questionnaire.</p>
Peer Comparison page	<ul style="list-style-type: none"> <li>1. Sus/Mo (previously in overview page) in collapsed container</li> <li>2. List of filtered peers</li> <li>3. Company compare (Same as before)</li> </ul>	Step 7: Moved Sus/Mo.

## Cyence Onboarding Guide

### 1. What's New

We are proud to announce several new features for Cyence. 😊

1. On-demand assessments for new companies can be made directly from the application  
 2. Introducing the Underwriter Dashboard in the company 'Overview' page  
 3. Risk Factors are referred to as Exposure Signals  
 4. Exposure Signals are mapped to NIST & CIS cyber security frameworks and include actionable next steps

We encourage you to walk through the Quick Guide to familiarize yourself with the new user experience.

[Start Quick Guide](#)

Next: Updates to the company Overview page Continue

### 2. On-Demand Assessments 📈

<GIF on how to access and request an assessment>

Unable to find a company in Cyence? You can now request an On-Demand Assessment for a new company directly from the application and review the results in minutes!

Hunter Nielsen "from within the application"

Hunter Nielsen "from within the application"

Hunter Nielsen "We've updated the company 'Overview' page to highlight three methods that you can use to evaluate cyber risk."

Hunter Nielsen "by clicking the help icons (?) within the dashboard."

Next: Updates to the Cyence Risk Report (PDF) Continue

### 3. Introducing Underwriters Dashboard

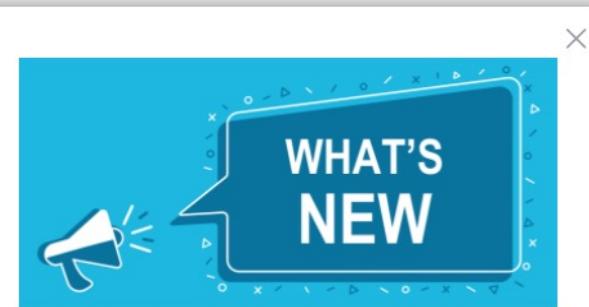
The company overview page is now updated to highlight the three methods by which to evaluate cyber risk. These include:

1. Exposure Signals
2. Probability of Incident (Risk Rating)
3. Loss Analysis

You can learn more about each method by clicking help icons (?) within dashboard.

Next: Updates to the Cyence Risk Report (PDF) Continue

[Back](#) [Continue](#)



We are proud to announce several new features for Cyence. 😊

1. introducing the **Overview dashboard** for underwriting and risk selection
2. **Risk Factors** are now referred to as **Exposure Signals**
3. **Exposure Signals** are mapped to NIST & CIS cyber security frameworks and include actionable next steps

We encourage you to walk through the Quick Guide to familiarize yourself with the new user experience.

[Start Quick Guide](#)

# Onboarding Design Samples

## Onboarding Guide

The screenshot shows the Cyence platform's onboarding guide. At the top, there's a navigation bar with 'CYENCE' logo, user info ('Hello, Yogesh Motwani'), and search/filter options. Below the header, a large 'My managed items' section shows 0 Company Policy Structures. To its right is a prominent 'WHAT'S NEW' modal window with a megaphone icon and a speech bubble containing the text: 'We are proud to announce several new features for Cyence. 🎉'. The modal lists three new features: 1. Introducing the Overview dashboard for underwriting and risk selection, 2. Risk Factors are now referred to as Exposure Signals, and 3. Exposure Signals are mapped to NIST & CIS cyber security frameworks and include actionable next steps. Below the modal, there's a 'Run Scenarios' button. Further down, the 'Recently viewed' section lists companies like Apple Inc., Guidewire Software Inc., Karam, Inc., and Alphabet Inc. The 'I want to...' section provides links for viewing scenarios, groups, portfolios, creating a portfolio, and running a scenario. At the bottom, it says '373,708 Companies'.

## In-App UI Feedback

The screenshot shows a feedback dialog box overlaid on the Cyence interface. The dialog title is 'In-App UI Feedback'. It asks, 'We recently changed the way you can evaluate a company using underwriter dashboard. How would you rate these changes?'. Below this is a rating scale from 1 (Horrible) to 5 (Awesome). A text input field below the rating scale asks 'Please explain your rating' with placeholder text 'Type your comments here...'. At the bottom of the dialog is a 'Submit' button. The background of the dialog is semi-transparent, showing parts of the main application's 'My managed items' and 'Recently viewed' sections.

# Product Success Metrics

The process of defining success metrics

 Define

 Review

 Track & Report

 Reflect

 Design Backlog

## Some key insights

Month-over-month comparison

JUNE 2021 TO JULY 2021

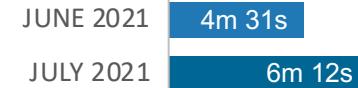
### Unique Companies Viewed

 21%



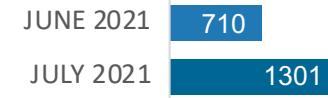
### Time spent on new pages

 49%



### Report Downloads

 83%





# Thank You!

CYENCE Companies Portfolios Industries Scenarios Search all companies

Add to Portfolio Cyence Risk Report

N Nordstrom, Inc.

Industry: Retail Trade Sub-Industry: Department Stores # of subsidiaries: 2 Annual revenue: \$50-\$70B Estimated record count: 315.2M+ PCI 100% Employee count: 10,000+ Location: San Mateo, California, USA

Overview Exposure Signals Security Measures Loss Analysis Peer Comparison 39 peers filtered Filter Peers

**Exposure Signals** Areas that may have cyber vulnerabilities

Overall risk grade: 54 (54) Percentile: 41st

View peer group ranking

**Probability of Incident** Chance of experiencing a cyber incident

Overall probability of incident: 15.4% (Percentile: 14th)

View peer group ranking

**Loss Analysis** Expected cyber loss per year, averaged over many years

Average Annual Loss (AAL): \$8.8M (Percentile: 84th)

View peer group ranking

**Top exposure signals** Viewing 3 exposure signals that need investigation

- ⚠ Spam activity Detected
- ⚠ Foreign hacker activity Detected
- ⚠ Network complexity High

View 13 More

**Breakdown of probability of incident** in percent (%)

- 10.4% Data breach probability
- 8.2% Ransomware probability

Ground up AAL: \$8,842,106 Breakdown of coverages type

- Liability: \$187,432
- First Party Data Breach: \$7,831,937
- Business Interruption: \$113,306
- Contingent Business Interruption: \$708,920
- Cyber Extortion: \$210

© 2015-2021 Cyence LLC  
Privacy Policy | Terms of Use | Cyence Support