VectorX

Security Assessment

True security is knowing what could go wrong before it does and preventing it.

The security of your Salesforce org is at threat level midnight. Access is unbridled, permissions allow elevated user control, and your customer data is on display for all to see. But with a Salesforce security assessment, you can fight back and protect your valuable assets. Get ready for a digital deep-dive to secure your org.

How it Works

Security Assessment Kick-Off

*Stakeholder Interviews & Reverse Demos**

Examination of Salesforce Org & Environment

Development of Scorecard, Findings & Recommendations

Executive Readout of Security Assessment Report

Benefits of a Secure Org

Data Protection

Best Practices

Loss Prevention

Risk Mitigation

Types of Assessments

Essential Security Assessment = Inspection w/Report

*Amplified Security Assessment = Essential + Tailored Recommendations & Consultation

Ready to bulletproof your org?
Reach out to us via phone or email.
470.243.4770 | engage@vectorx.com

VectorX.com

Security Assessment

VectorX

Service Overview

Why do a Security Assessment?

- Identify Security Vulnerabilities: Get an understanding of org access and control, data leaks, or configuration errors.
- Optimize Your Security Posture: Identify areas of weakness and take proactive steps to reduce risk
- Protect Your Reputation: Security breaches can damage your organization and result in losses. This will get you ahead of them.
- Stay Ahead of the Threats: Regular security assessments can help to avoid fatal errors in an ever-changing environment.

What's Included

- Benchmarking of your system against industry standards and best practices
- A comprehensive understanding of the security status of your org and a report outlining the findings
- A scorecard that summarizes your security standing, making it easy to track progress and measure imrovements over time.
- *A reverse demo and deep dive into your org to gain a deeper understanding of your system's intricacies (Amplified Version Only)

Common Security Vulnerabilities

- Inadequate Access Controls: User permissions and access controls not configured properly can give users access to data for functionality they shouldn't have access to.
- Unsecured APIs: If your APIs are not properly secured, attackers may be able to access or manipulate data through these interfaces.
- Malware of Phishing Attacks: These types of attacks can open your org to data breaches or unauthorized access.

Security Inspection Areas

Login & Session Settings

Record Sharing & Access

User Permissions

System Updates

Custom Development

Digital Experiences

Information Security