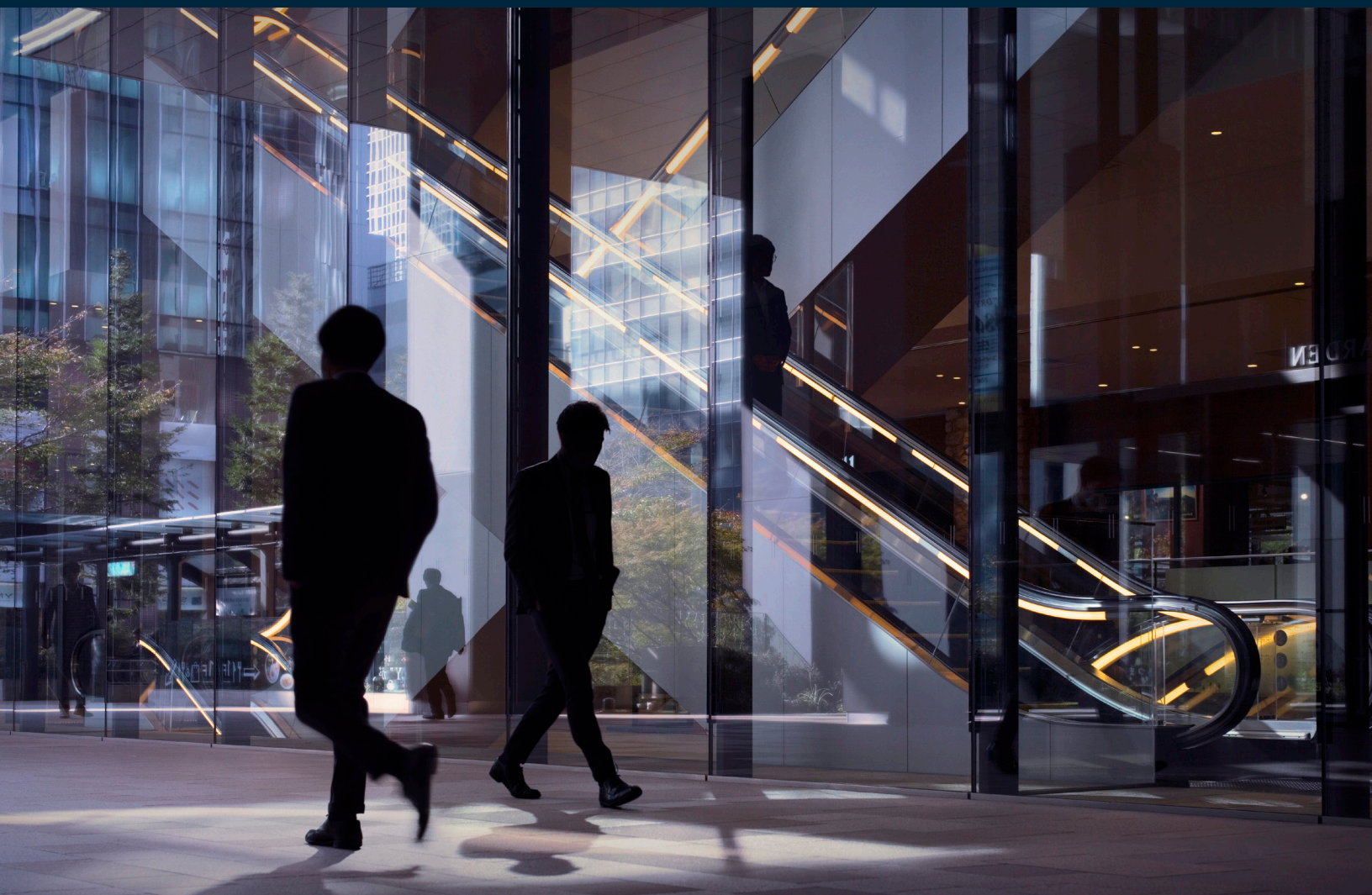
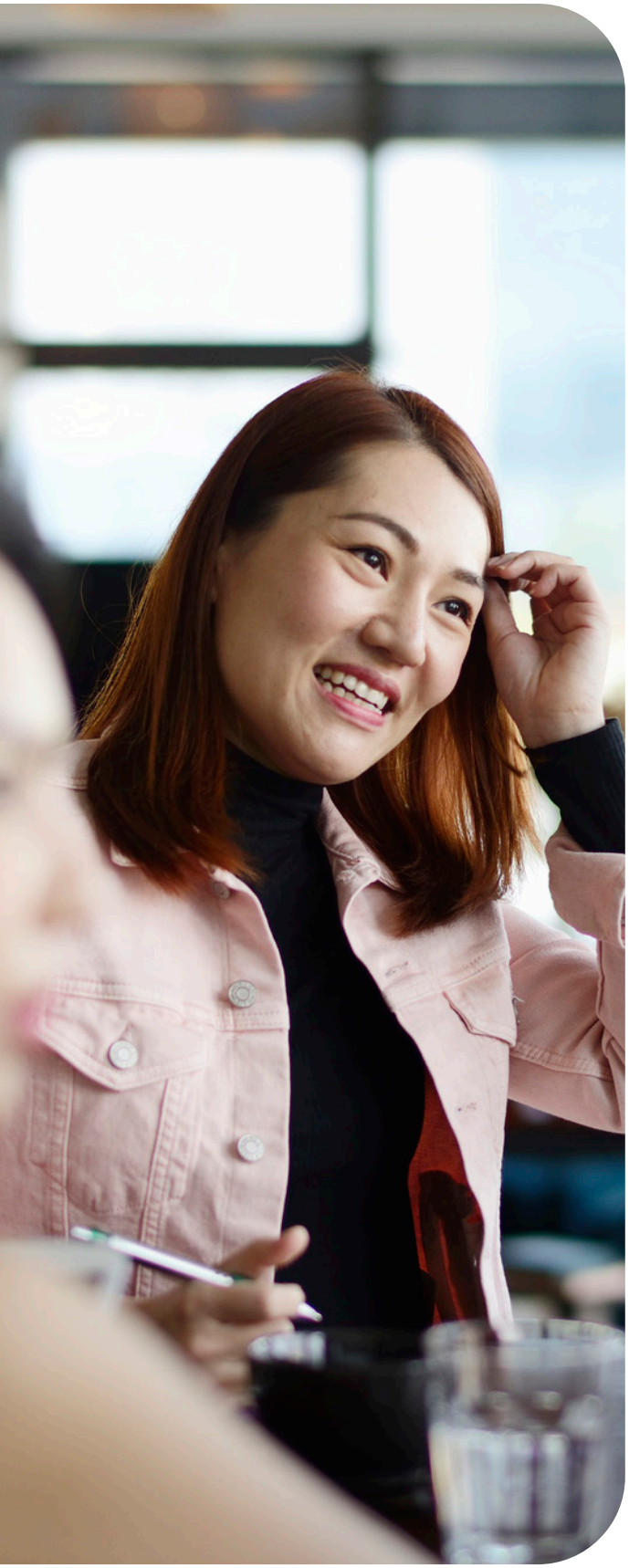
alteryx

Security at Alteryx

Get a detailed preview of our Information Security Program used to govern the protection of the company's data, assets, and products.





About Us

Alteryx is a trusted partner in intelligent decision-making. Alteryx software empowers enterprises worldwide with automated, AI-driven insights, enabling data democratization across various use cases for impactful business outcomes. With over 8,300 organizations relying on our platform, Alteryx takes Information Security seriously.

Alteryx's Information Security Program is founded on a defense-in-depth approach, combining technology, processes, and skilled employees serving as the first line of defense to protect data and operations. Holding ISO 27001 and SOC2 Type II certifications, we offer our customers and stakeholders the assurance of aligning to security industry standards. Moreover, Alteryx proudly follows respected global security frameworks like ISO 27001, NIST Cybersecurity Framework, and CIS Controls, reinforcing our dedication to data protection, a secure environment, and secure products.

Purpose

This document transparently shares Alteryx's Information Security Program, fostering a strong and secure partnership built on reliable support and trust. We look forward to collaborating with our customers to achieve intelligent decision-making with confidence.

Certifications

Alteryx's compliance certifications provide assurance to customers and stakeholders that the organization has been certified by independent third-party auditors and follows security best practices.

ISO 27001

Alteryx's ISO 27001 certification demonstrates the implementation of a comprehensive framework for managing and protecting its information assets. It signifies a commitment to maintaining the confidentiality, integrity, and availability of information, as well as ongoing monitoring and improvement of the Information Security Management System (ISMS).

SOC2 Type II

Alteryx's SOC2 Type II certification demonstrates the effective implementation and maintenance of internal security controls and measures to protect customer data, ensure system availability, and maintain the confidentiality and privacy of sensitive information. Alteryx continues to update and extend the scope of its SOC 2 Type II audit program.

Corporate Security

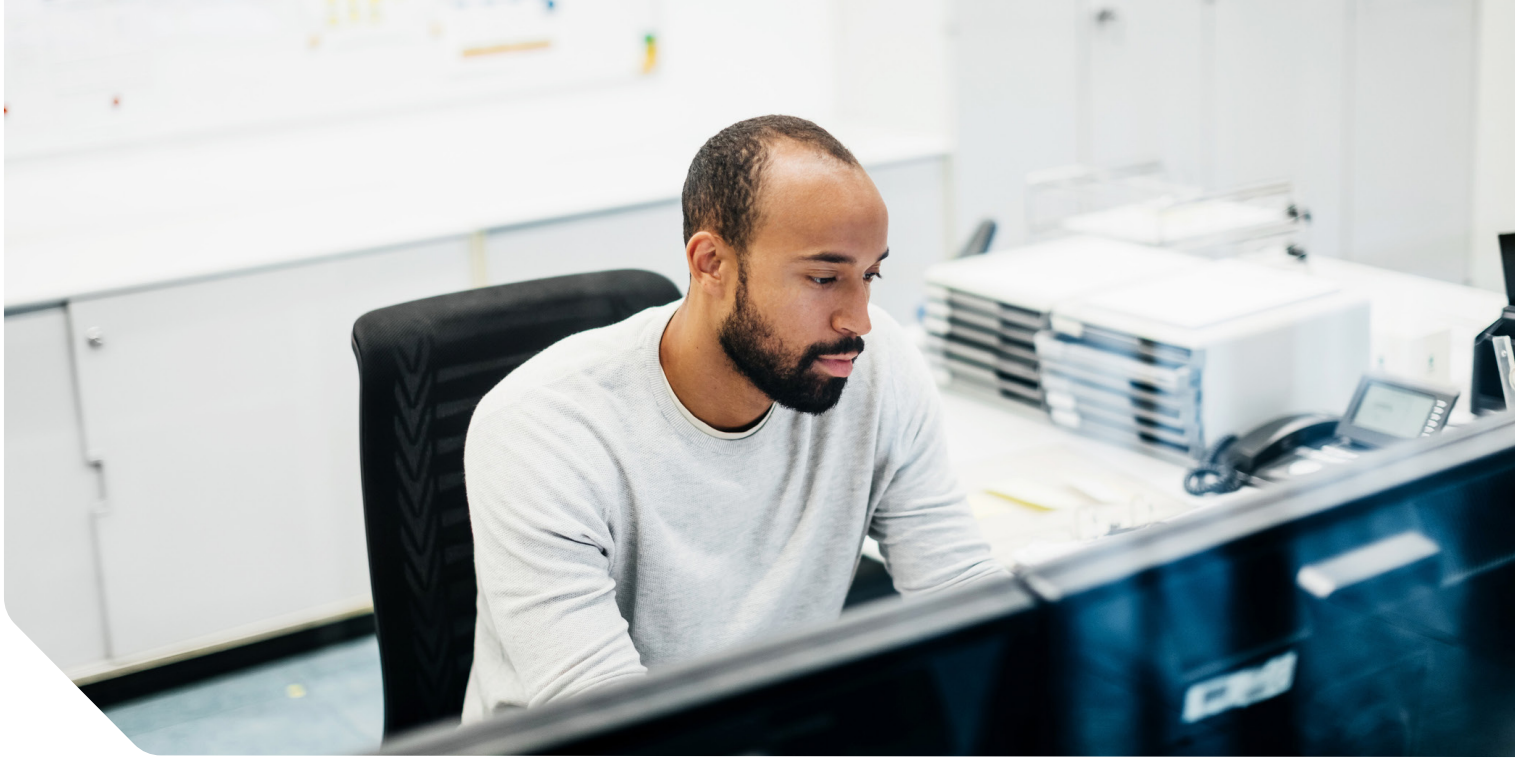
At Alteryx, we are committed to upholding the highest standards of information security. As part of our dedication to protecting the confidentiality, integrity, and availability of our systems and data, we have implemented policies, standards, and processes that follow global security frameworks such as ISO 27001, NIST Cybersecurity Framework, and the CIS Controls.

Information Security Policies

Adherence to company policies and procedures ensures a secure and compliant environment where information is handled responsibly and in accordance with industry best practices. Alteryx policies and procedures serve as a set of guidelines and rules that employees, contractors, and other stakeholders must adhere to when handling information and using the organization's IT infrastructure. Alteryx policies are updated regularly to keep pace with changes in regulations, technologies and industry security best practices. Alteryx information security policies are made available to all personnel and acknowledged annually, further reinforcing the commitment to maintaining a secure and compliant environment.

Personnel Security

Personnel are subject to background checks before employment, an important step to ensure the security and integrity of our workforce in handling sensitive data. Additionally, personnel are subject to confidentiality obligations, highlighting Alteryx's commitment to safeguarding customer information. By requiring personnel to acknowledge and adhere to Alteryx's Information Security Policy, Alteryx reinforces a culture of data security and creates a workforce that prioritizes the responsible handling of systems and data.



Security Training & Awareness

At Alteryx, we recognize the critical role of our employees in bolstering our organization's security posture and serving as the first line of defense against potential threats. The primary objective of this program is to foster a robust security culture within the organization. Through comprehensive and targeted role-based training, Alteryx instills responsible information handling practices and empowers individuals to effectively identify, report, and respond to security risks.

Additionally, Alteryx offers role-specific training to engineers, focusing on critical aspects such as secure coding, OWASP Top Ten, and Privacy by Design. By integrating security by design principles into our development culture, we further reinforce the importance of security throughout the software development lifecycle of our products.

Physical Security

Alteryx Global Physical Security ensures the safety of individuals, property, and assets by deploying a range of measures, including access control systems, security officers, alarms, and an incident response plan. These proactive measures effectively reduce physical risks and safeguard our employees, guests, and assets.

Asset Management

Alteryx has an asset management and governance framework to oversee its technology assets throughout their lifecycle, ensuring operations remain reliable and secure. This includes both physical and virtual technologies, ensuring secured use, regardless of the asset's location.

Business Continuity & Disaster Recovery

Alteryx's business continuity and disaster recovery framework assures data recovery in the face of disruptions such as server failures, data breaches, or natural disasters, ensuring minimal data loss and downtime. All systems within our environment are diligently accounted for, with documented recovery time objective (RTO) targets and regular backups, enabling the restoration of critical systems and data in case of an incident. Regular efficacy testing and

third-party auditor oversight further bolster the effectiveness of our Disaster Recovery plan. Additionally, our updated and exercised business continuity plans offer detailed recovery steps for applications, facilities, vendors, and our most valued asset: our employees.

Audit Compliance

Our customers can trust in the strength of our security practices as we actively review and uphold compliance with security laws and regulations. Through supporting internal and third-party assessments, we ensure that our information security controls, processes, and systems consistently meet defined thresholds.

Vendor Risk Management

A vendor risk assessment process supports the security and reliability of our software solutions. Prior to onboarding any third-party vendors, Alteryx conducts risk assessments and evaluates their security practices to ensure appropriateness. Periodic reviews and active monitoring, aligned with our risk management program, customer commitments, and regulatory obligations, further strengthen the security of our supply chain.

Data Retention and Destruction

Policies regarding the proper retention and destruction of data are essential for maintaining the highest levels of data security, compliance with regulations, and safeguarding sensitive information. Data is retained for the period required by applicable legal and/or contractual requirements and then disposed of in a secure manner

Application Security

Secure Software Development

The software components of Alteryx are developed in line with our Software Development Lifecycle (SDLC) policy. Alteryx uses a risk-based approach when applying its SDLC methodology, which may include performing security architecture reviews, automated security scans, and external penetration testing. Alteryx performs periodic security code reviews and scans source code as well as packaged software to monitor against malicious threats.

Product Vulnerability Management

Alteryx follows industry-standard security practices to identify and resolve vulnerabilities both before and after product release to provide reliable and secure products. Vulnerabilities go through evaluation, rating, and prioritization. Updates are released to address vulnerabilities in supported versions, with cumulative fixes incorporated in major and minor releases.

Security Architecture

Network Security

Network security at Alteryx follows defense-in-depth methodology and enforces the principle of least privilege by restricting network access to systems, applications, and services. Changes to these configurations are restricted to authorized personnel as well as monitored and approved through a change management process. The network is continuously monitored for health and performance, and periodic access reviews take place for accounts with advanced permissions.

Encryption

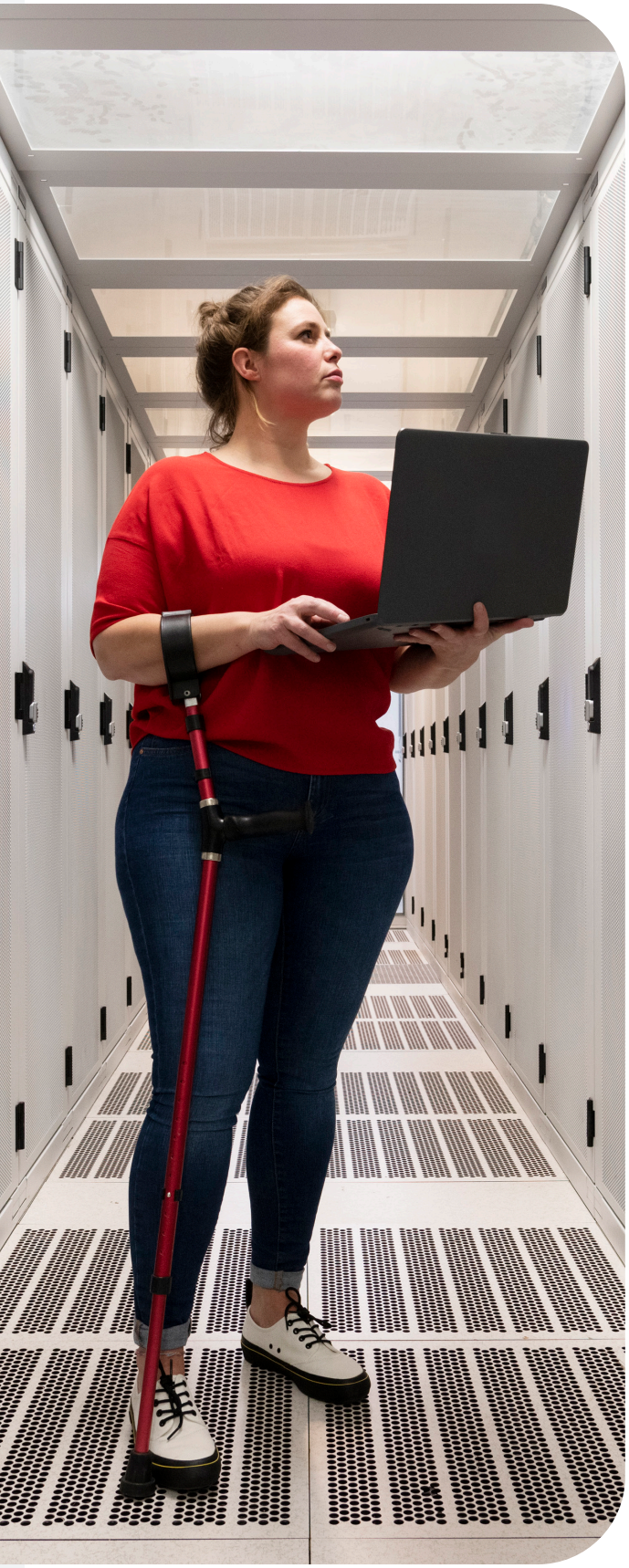
Encryption is a fundamental pillar of our security strategy, ensuring that sensitive data remains protected. At Alteryx, we follow industry-leading encryption standards, prioritizing the confidentiality and integrity of information. Our encryption practices are regularly reviewed and updated to align with the latest security best practices. By implementing robust encryption measures, we ensure data is shielded from unauthorized access, both in transit and at rest.

Identity and Access Management (IAM)

IAM controls ensure that only authorized individuals have access to sensitive data and critical systems, effectively reducing the risk of unauthorized access and enhancing overall security.

Alteryx maintains internal access controls aligned to industry best practices. System access is reviewed and granted by the platform or product owners on a regular, recurring basis. Systems are continuously monitored for events related to authentication, user account creation, restricted group access, and network device access.

Alteryx systems require role-based access utilizing the principle of least privilege. Authentication credentials are unreadable during transmission and storage. Passwords are required to be complex in accordance with our password policy. External access to corporate systems requires the use of the Alteryx Virtual Private Network (VPN) along with Multi-Factor Authentication (MFA). Automated account lockout occurs after multiple failed attempts and misplaced, lost, or untrustworthy devices are wiped remotely



FIPS Capability

Alteryx Designer FIPS, is our FIPS-capable desktop analytics solution meticulously designed to meet Federal Information Processing Standards (FIPS) thresholds set by the National Institute of Standards and Technology (NIST) and in accordance with the Federal Information Security Management Act (FISMA). This capability is a testament to our commitment to robust data security, ensuring a secure analytics environment. With Alteryx Designer - FIPS, users can confidently blend diverse data securely and efficiently, empowering seamless data analysis within highly regulated environments.

Security Operations

The purpose of Security Operations at Alteryx is to provide protective, detective, and responsive services. These capabilities have improved our cyber defense capabilities enabling greater visibility, quicker detection, and faster responsiveness.

Alteryx uses machine learning technologies to analyze datasets, optimize detection coverage, prioritize threat detections, automate threat hunting, and identify and enrich high-fidelity alerts and patterns that can be investigated by our Security Operations team.

Incident Management

The Alteryx Cybersecurity Incident Response Plan (CIRP) establishes the actions and procedures that help the Security Operation Center (SOC) team prepare for and respond to security incidents, including how to initiate responsive action, remediate adverse consequences, document lessons learned; and continuously improve the incident response processes. The CIRP is regularly tested using a combination of planned reviews and live simulations along with periodic training.

Log Management

Alteryx maintains awareness of security-related events through the centralized collection and analysis of event logs from systems, applications, physical security assets, and services, providing a comprehensive view of the security and performance of its production infrastructure.

Detection & Monitoring

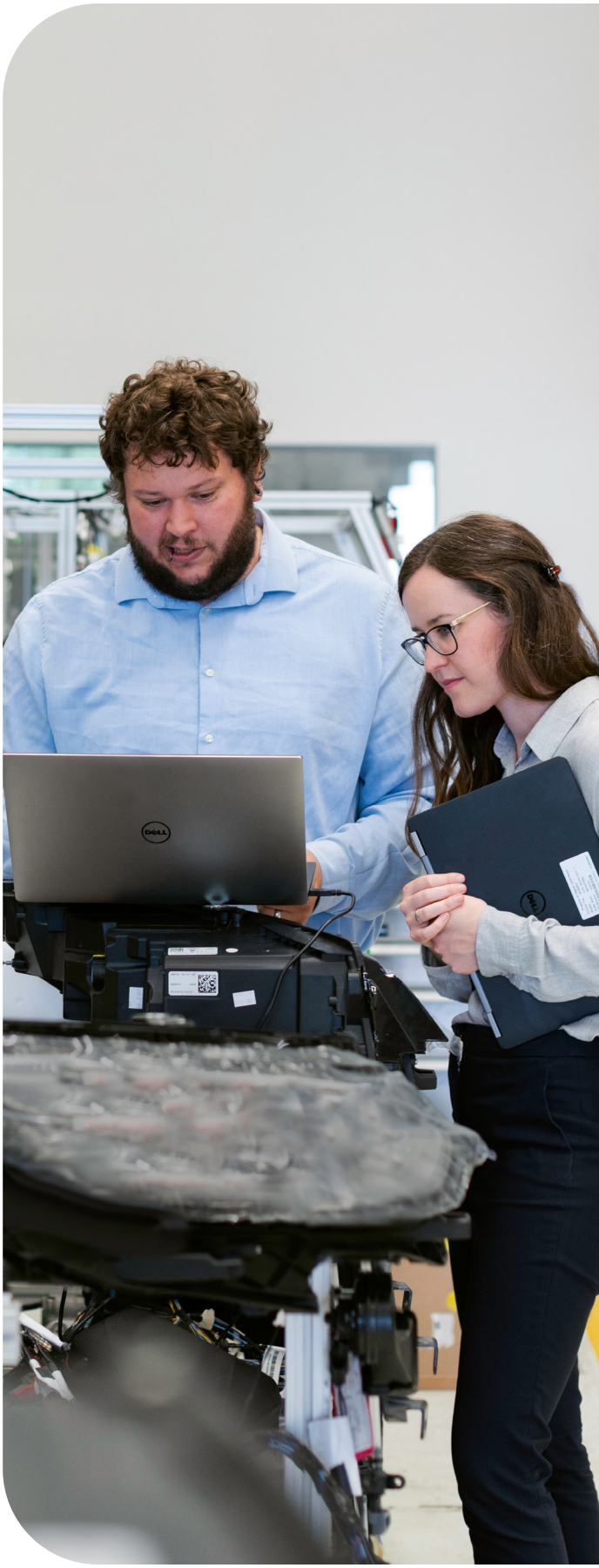
Alteryx leverages modern threat detection and prevention systems to safeguard and monitor against malicious exploitation, unauthorized disclosure, modification, and destruction. These systems are actively monitored, with potential problems or violations documented and escalated to the appropriate teams to ensure prompt remedial action.

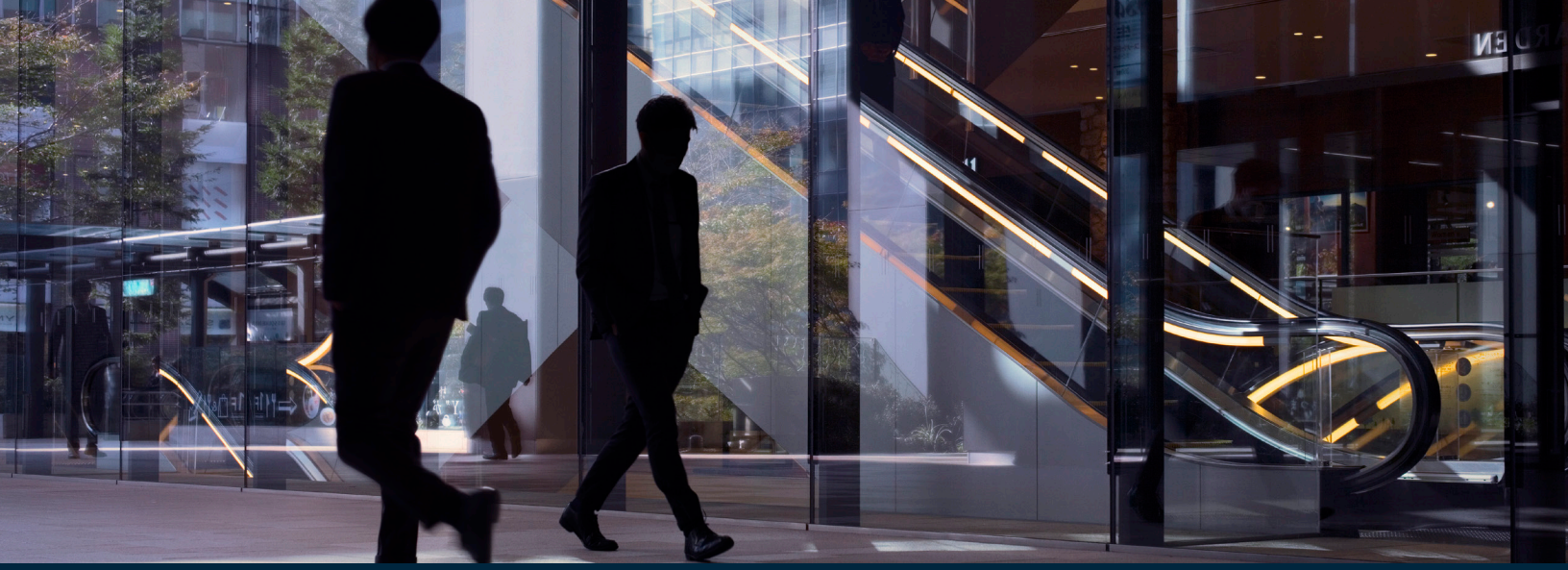
Endpoint Protection

Alteryx deploys controls to ensure endpoint devices are adequately protected from potential threats. Alteryx workstations run a suite of endpoint security and monitoring technologies to detect suspicious code, unsafe configurations, or anomalous user behavior quickly and efficiently.

Enterprise Vulnerability Management

Alteryx has a comprehensive vulnerability management program that manages any reported or suspected vulnerability across its lifecycle, with defined processes that cover identification, assessment, prioritization, remediation, verification, and reporting. All risks are triaged, with vulnerabilities addressed in line with guidance from NIST and other industry standards.





alteryx

We look forward to partnering with you.

Alteryx, through its award-winning Alteryx Analytics Cloud Platform, enables organizations to deeply integrate actionable business intelligence into decision-making processes across their organizations, from the front-line employees to C-suite executives. With our relentless focus on putting analytics within reach of everyone while providing the tools needed for enterprise security and governance, Alteryx empowers end users without adding complicated, time-intensive layers of maintenance and configuration to already-stressed IT resources.

You can find more information about our efforts and compliance certifications at alteryx.com/trust, and we're here for any other questions you have about our security program.

Welcome to the analytics movement.