DATA INTENSITY
dataintensity.com

VULNERABILITY MANAGEMENT SOLUTIONS

Threat, Exploitation, Impact!

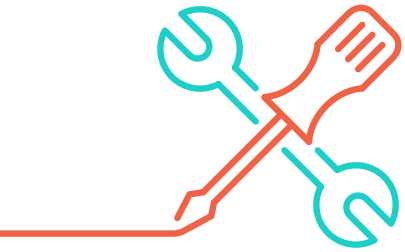
The most severe vulnerabilities often hide deep within infrastructure layers. The imperfection can be small yet have a huge organizational effect based on actor and asset reach.

83% of tech executives say that security breaches could have an impact on their organization in the next 12 months. 78% of IT executives say that the threat of major security breaches will impact their organization's investment plans.

- IDG

53% of IT and IT-security professionals rate their ability to investigate threats as ineffective. 42% say the average resolution time is months or years.

– Ponemon Institute



Risk-mitigation requirements never cease. Protection against known and unknown vulnerabilities is top of mind — and top of responsibility — for every executive, lead, and manager in the enterprise.

In the realm of IT assets, unsecured configurations, missing patches, outdated versions, and outgunned technology — to name only a few common maladies — produce a vulnerability ripple effect on current and future operations. The average breach costs millions in direct and indirect costs. Comprehensive strategies and effective methods for securing digital assets exist. So why do so many breaches, intrusions, and attacks still occur? And why do so many companies not heed the alarms and warnings?

Even the most proactive and vigilant organizations remain exposed to real and powerful vulnerabilities due to unavoidable combinations of:

- Number of Patches, Updates, and Upgrades Too Exhaustive to Maintain (Often Invalidating SLAs)
- Outdated Tools to Combat Cyberattacks, Encrypt/Mask Data, and Manage Users and Access
- Ongoing Resistance from End Users, Asset Owners, Enterprise Units, and Third Parties
- Indiscriminate Policy and Process Adoption Across the Organization (No Architectural Standards)
- Complexities Resulting from New Apps, Technology Growth, Cloud Sprawl, and Shadow IT

What will indecision or inaction cost your company? You need a common strategy and amelioration framework to address and assure security levels enterprise-wide.

How We Help

Data Intensity Vulnerability Management Solutions stand on two decades of managing complex application and database platforms, across a hybrid of cloud tenancies, employing a trifecta of intelligent, customized, and advanced security-driven techniques. We assess technologies, integrations, and workflows as well as different client groups, for vulnerabilities, irregularities, and threats and then apply a set of point and prevention solutions. Our tested portfolio approach includes automated one-off, distributed, and regularly scheduled scanning; comprehensive documentation with strategic and tactical prioritization; and targeted remediation procedures. As always, all of our work is founded in globally recognized and partner-accredited, best-practice industry standards.

Customer Results

- 100% Patch Accuracy
- 140 Databases
- 8 Appliances
- 75% P1/P2 Reduction

Data Intensity was able to successfully design, execute, and manage our strategy with expertise we simply could not find elsewhere."

- CIO, Multi-National Retailer

Patch and Configuration

Identify, log, remediate OS, hypervisor, app, and DB workload risk from CVEs, against CIS standards, and versus CIS Critical Controls, DISA, STIG, DoD, ISO, NIST, HIPAA, ITIL, FFIEC, NERC-CIP, GDPR, CCPA, PCI DSS policies.

Web Application

Scan public-facing URLs to document development, deployment, and operational vulnerabilities to enterprise web apps, including REST-based and SOAP APIs that too often are subject to hacking activity.

Cloud

Diagnose, locate, help correct security risks, access deviations, configuration shortfalls in shared-/public-cloud tenancies with API interrogations of AWS, Azure, Google and multi-node security brokerage for Oracle clouds.

By 2022, approximately 30% of enterprises will adopt a risk-based approach to vulnerability management…organizations that use the risk-based vulnerability management method will suffer 80% fewer breaches.

– Gartner

66% of IT and security respondents say spending is prioritized based on compliance mandates. 62% of respondents say budget dedicated to security solutions is increasing.

– IDC

Data Intensity Vulnerability Management Solutions customers are able to realize:

- Improved IT Asset Availability and Value
- Reduced Potential for Loss and Compliance Risk
- Heightened Exposure Awareness and Response Readiness
- Enhanced Security Position for Corporate Liability
- Enterprise Standards Founded in Best-Practice Strategies

The Data Intensity Difference

The digital domain is fluid. Digitalization and transformation strategies must embrace new technologies that take advantage of machine learning, image recognition, and process automation. Greater digitization — applied properly, to drive revenue — inherently begets vulnerability. Data Intensity meets vulnerability challenges head-on and full-throttle. Our solution partners are the best in the business.

ORACLE Platinum Partner Cloud Select North America
Oracle Cloud Managed Service Provider

Microsoft GOLD CERTIFIED Partner

amazon web services

Data Intensity is a trusted Managed Services Provider, delivering business transformative solutions and services tailored to help our customers succeed in a hybrid multi-cloud world. Our purpose-built solutions and services target the technologies and platforms that power our customers' business transformations — from front-end strategy and design, to implementation and migration, to ongoing support and operation — all from a single vendor. Customers choose us — and stay with us — because working with Data Intensity allows them to focus on their critical business needs, while we focus on their applications and multi-cloud investments to drive faster time to value.

Data Intensity
team@dataintensity.com

United States
22 Crosby Drive, Ste. 100
Bedford, MA 01730

United Kingdom
Floor 1 & 2
4 City Road
London, EC1Y 2AA

Australia
Level 13
144 Edward Street
Brisbane QLD 4000