DigitalXForce
Digital Trust Inside Out

Whitepaper

Redefining The Future of Cybersecurity With Digital Trust

www.digitalxforce.com
info@digitalxforce.com

DigitalXForce
Digital Trust Inside Out

Authors

Lalit Ahluwahlia
Founder & CEO
DigitalX**Force & i**TrustX**Force**
lalit.ahluwalia@cyberxforce.com

Desiree Wilson
Chief Information Security Officer
DigitalX**Force**
desiree.wilson@digitalxforce.com

www.digitalxforce.com
info@digitalxforce.com

DigitalXForce
Digital Trust Inside Out

Redefining The Future of Cybersecurity With Digital Trust

Index

DigitalXForce
Digital Trust Inside Out

Redefining The Future of Cybersecurity With Digital Trust

Executive Summary

The conventional CIA triad of confidentiality, integrity, and availability (CIA) is a good starting point for defining cybersecurity, but it is just one side of the coin. To evolve to a safe and secure digital era, there's a need to shift focus from "standard cybersecurity" to "Digital Trust".

Admittedly, the security risk profile has shifted from just information and financial loss to loss of life. This means that the "trust" dimension must take center stage as a new definition of cybersecurity.

To build confidence in the responsible consumption and usage of emerging technologies, our digital ecosystem and services must adhere to not only confidentiality, integrity, or availability, but also the trust tenet.

As a result, the "CIA" must be changed to "I-ACT: Integrity, Availability, Confidentially, Trust" and "Cybersecurity" must be changed to "Digital Trust". By incorporating the trust tenet, or "I-ACT", organizations can better protect their data, systems, and people and build the secure future of tomorrow.

Introduction

The digital world is rapidly evolving. Thanks to real-time security news on digital transformations, it is now evident that cyber-attacks, data leaks, and vulnerability risks have had a fair share in “staining” the entire digital landscape as our reliance on technology increases.

This begs the question: Are we adapting to these rapid changes or just following the status quo?

Sticking to the generally accepted cybersecurity tenets encourages a focus ONLY on confidentiality, integrity, and availability - eliminating the true concept of “TRUST” in digital interactions.

Redefining these tenets will not only take us a step closer to a more balanced digital matrix, but will eventually bridge the gap between cybersecurity and digital trust, and build resilience inside out.

Key Takeaway

This begs the question: Are we adapting to these rapid changes or just following the status quo?

Key Tenets of Cybersecurity

In a world where information systems and data security are top priorities, cybersecurity is a very important subject matter. For decades, we have been taught that cybersecurity consists mainly of three Tenets called the “CIA Triad” - which upholds the following pillars: Confidentiality, Integrity, and Availability.

Confidentiality means that data is kept private and only accessible to those who are authorized to view it. Integrity focuses on the accuracy of data and making sure data has not been tampered with.

On the other hand, availability means that data is available and accessible when needed. These three pillars make up the conventional principles or “tenets” of modern cybersecurity.

When it was defined, it did fit the definition and purpose. At the time, we were mainly concerned with “information systems, data, and services”.

Key Takeaway

When it was defined, it did fit the definition and purpose. At the time, we were mainly concerned with “information systems, data, and services”.

However, the need and demand for cybersecurity has increased as technology evolves. While the CIA triad is important, it is not enough. In today's world where we share and exchange data constantly, there’s a need to add a new tenet to the mix - specifically, “trust”.

Understanding The New “T – TrusT” Tenet

Trust is the foundation of any successful relationship, and it's no different when it comes to human-computer interactions in cybersecurity. When we trust our systems and our data, we're more likely to use them safely and securely. To redefine cybersecurity, we need to focus on building trust.

For instance, creating systems that are secure, reliable, and transparent and educating users about cybersecurity risks and how to protect themselves will not only build trust, but will also save lives because of risk awareness. By focusing on trust, we can create a more secure and resilient cyber environment and security posture.

Just like the conventional CIA triad for Information Systems, digital trust is the foundation for any digital business and helps build confidence in the consumption of digital services and other digital interactions. Digital trust is built on factors such as security, privacy, transparency, and accountability.

From integrated risk management, performed and measured in real time, to factual and data driven insights validated on a continuous basis with automation, the importance of digital trust in Cybersecurity cannot be over emphasized.

Pillars of Trust

Consider the following supporting pillars for a new “T-Trust” tenet in Cybersecurity:

- **Integrated Risk Management**

Digital trust in integrated risk management ensures the provision of integrated insights on an organization’s security posture, how it manages threats, security risks, and all other aspects of operations, including its physical and information security, as well as its people and processes.

- **Continuous Monitoring**

When trust becomes a priority, continuous monitoring is the only way to track progress or failure. This concerns the collection, analysis, and constant tracking of digital assets to avoid security breaches.

- **Real-time Data Insights**

Data is data, but generating real-time data insights makes the difference. This dimension ensures that all data comes directly from the source. In this case, collected and registered are displayed in real-time with no third parties tampering with the data flow.

- **Data-Driven Analysis**

Unlike the CIA triad, the T-Trust tenet encourages the use of analytical and data-driven approaches to make fact-based assertions about cybersecurity. This dimension is achievable with real-time data insights.

- **Proactive Defense**

One of the ways to ensure security risk mitigation is through predictive analysis with a proactive defense approach. Emerging cyber threats making waves in today's digital landscape have made proactive solutions a necessary recipe for digital trust.

As seen above, the TRUST tenet is becoming increasingly important as our reliance on technology grows. In the past decade, security was primarily focused on protecting information and financial assets.

However, as technology becomes more pervasive in our lives, security must also focus on protecting people.

Key Takeaway

In the past decade, security was primarily focused on protecting information and financial assets.

For example, a cyberattack could be used to control critical infrastructure, such as power grids or transportation systems. This could lead to loss of life or property damage.

This calls for a CIAT framework (confidentiality, integrity, availability, and trust) which provides a more comprehensive approach to cybersecurity.

But why do we need to redefine cybersecurity from a "Trust" perspective?

Need to Redefine Cybersecurity with ‘Digital Trust’

The need to redefine cybersecurity cannot be overemphasized. Cybersecurity is no longer just a concern for IT departments. In today's world with increasing digital transformations, we are living in an entirely new era. The “Digital Era” as we call it is fuelled by smart devices, AI, cloud, and mobile devices.

Our lives are dependent on technology, and in some cases, this makes us incapable of even performing primary tasks as humans. We are not just consumers of digital services but living in the digital itself. The risk profile has shifted from data or finance loss to even loss of life. The situation? Over-reliance on technology! This situation has worsened with increasing technological advancements. The result?

Every organization, regardless of size or industry, is at risk of cyberattack. This is no news. It is already happening.

There are several reasons why there is a need to redefine cybersecurity.

First, we are not only consumers of Digital services but are living in the “Digital” itself. The risk has stretched beyond the standard norms of data and finance loss to the loss of life.

Key Takeaway

The risk has stretched beyond the standard norms of data and finance loss to the loss of life.

Second, the threat landscape is constantly evolving. Cybercriminals are constantly developing new ways to exploit vulnerabilities in systems and software.

Third, the digital world is becoming increasingly interconnected. The rise of cloud computing, mobile devices, and the Internet of Things has made it easier for criminals to gain access to sensitive data.

While the risk we knew before used to be around Information Systems and Services with a focus on loss of data, service, or finance, it has grown much bigger now.

With the adoption of smart devices and new digital methods, however, the risk has increased to include the loss of human life.

Unfortunately, this cannot be addressed or contained within the three Tenets of the traditional “CIA Triad" – Confidentiality, Integrity, and Availability. When faced with such a reality as this, there is only one way out: the pragmatic introduction of a new dimension and Tenet “T – Trust” which focuses on building trust across digital interactions.

Why Digital Trust is MORE CRITICAL than Cybersecurity & Privacy

We all know that cybersecurity and privacy are becoming more and more critical with digital transformation. The sophisticated threats with national hacktivism and cyberwarfare have increased the overall risk and need for proactive cyber defense.

Complement that with the expanded attack surface with the adoption of Cloud, Hybrid ecosystem, OT, and IoT turning everything “smart"—smart cities, smart campuses, remote healthcare, etc. Emerging technologies such as AI, ChatGPT, blockchain, etc., are being leveraged by bad actors in a way that increases the intensity of the attack.

But what do we need to be worried about? Assume you are in a self-driving car in the middle of a running highway, and you get a call from a hacker that your car has been compromised. What is the first question that comes to your mind at that time?

To check the audit and compliance of the car, or why did you trust the car? The same applies to Smart Cities, Smart Homes, Remote Healthcare, Space Tourism, and many other things today.

Hence the need for "Digital Trust," creating confidence among the end users (citizens, customers, non-users, and anything that is part of the digital ecosystem) to trust the digital services.

Key Takeaway

Emerging technologies such as AI, ChatGPT, blockchain, etc., are being leveraged by bad actors in a way that increases the intensity of the attack.

Digital Trust vs “Standard” Cybersecurity & Privacy Measures

The need of the hour is Digital Trust versus standard Security and Privacy measures. Digital trust is the foundation for any digital business. To build digital trust, we need to have Integrated Risk Management that can be analyzed and measured in real-time, factual (data-driven), and validated continuously.

Given today's time and age with a sophisticated threat landscape, it needs to be automated versus human-dependent.

How is digital trust different from standard cybersecurity and privacy? While cybersecurity and privacy are more focused on the confidentiality, integrity, and availability of the service, Digital trust involves building confidence in the consumption of digital assets and emerging technologies.

Building Digital Trust

Digital Trust is built by providing data-driven, real-time, and continuous Integrated Risk Management with proactive defense.

Here’s a quick rundown of how you can start building digital trust:

Data-Driven Analytics - Use data-driven and analytical methods to make more fact-based decisions about cyber security.

Real-Time – Fetch data in real-time directly from the source (as soon as it’s collected and registered).

Continuous Monitoring – Collect, analyze, and monitor continuously.

Integrated Risk Management - An integrated view of how well an organization manages its unique set of security risks.

Proactive Defense – Apply security risk mitigation on a proactive basis through predictive analysis.

Are We Doing Enough To Build Digital Trust?

Given the ever-changing digital landscape, we have a lot of work ahead of us. First and foremost, we need to understand, promote, and prioritize the need for digital trust and create more awareness.

We need a total mindset shift from standard cybersecurity measures to new ways of enabling digital trust.

Most organizations are relying on point-based solutions to fix specific issues which generally results in siloed function versus integrated view.

The lack of integration in the overall cyber defense ecosystem leaves behind multiple blind spots that can be easily exploited by bad actors.

Key Takeaway

We need a total mindset shift from standard cybersecurity measures to new ways of enabling digital trust.

Building Digital Trust is critical for the success of any digital organization or digital transformation initiative.

Take the following steps to enable digital trust:

1) Know your digital assets and develop Asset Inventory & Attack Surface.

2) Apply defense in depth mechanisms for a multi-layer protection.

3) Secure by design leveraging modern-day architecture such as Zero Trust at all layers.

4) Automate the End-to-End security measures in all aspects: “Identify”, “Protect”, “Detect”, “Respond” and “Recover”.

5) Use real-time integrated mechanisms versus point-based solutions.

6) Train and enable the workforce to be aware of the latest and the greatest threats and technologies.

7) Do more than just “Check the Box”. Standard Audit and compliance will not be sufficient to enable Digital Trust. It creates a false perception of security.

Consumer adoption of any digital service from an organization hinge on what organizations does to build confidence through responsible usage of emerging technology such as ChatGPT, and its cybersecurity and data privacy practices; and establishing digital trust is critical to any digital business growth.

The organizations that are best positioned to build digital trust are also more likely than others to see annual growth rates.

The Threat Landscape

Top Threats

- RANSOMWARE / MALWARE
- DATA THEFT
- INSIDER THREAT
- PHISHING ATTACK
- WEB DEFACEMENT/BRANDING

IT ASSETS

IT SERVER	- 750	FIREWALLS	- 12
IT APPLICATION	-210	DATA BASES	- 270
SOFTWARE	- 120	MOBILE DEVICES	- 1020
WORKSTATION	-2100	CLOUD SERVICES	- 6
PRINTER	- 480		

CYBER SECURITY SERVICES

GRC - SERVICENOW	DLP - SYMANTEC
IAM - OKTA, SAILPOINT	TVM - TENABLE, NESSUS
SIEM - SPLUNK	
END POINT PROTECTION - TANIUM	
FIREWALL SECURITY - PALO ALTO, ZSCALER	

SECURITY KPI'S

KPI 1 KPI 1

SECURITY KRI'S

KRI 1 KRI 1

“We are at the forefront of revolutionizing the cybersecurity landscape and instilling digital trust in the modern era.” - DigitalXForce

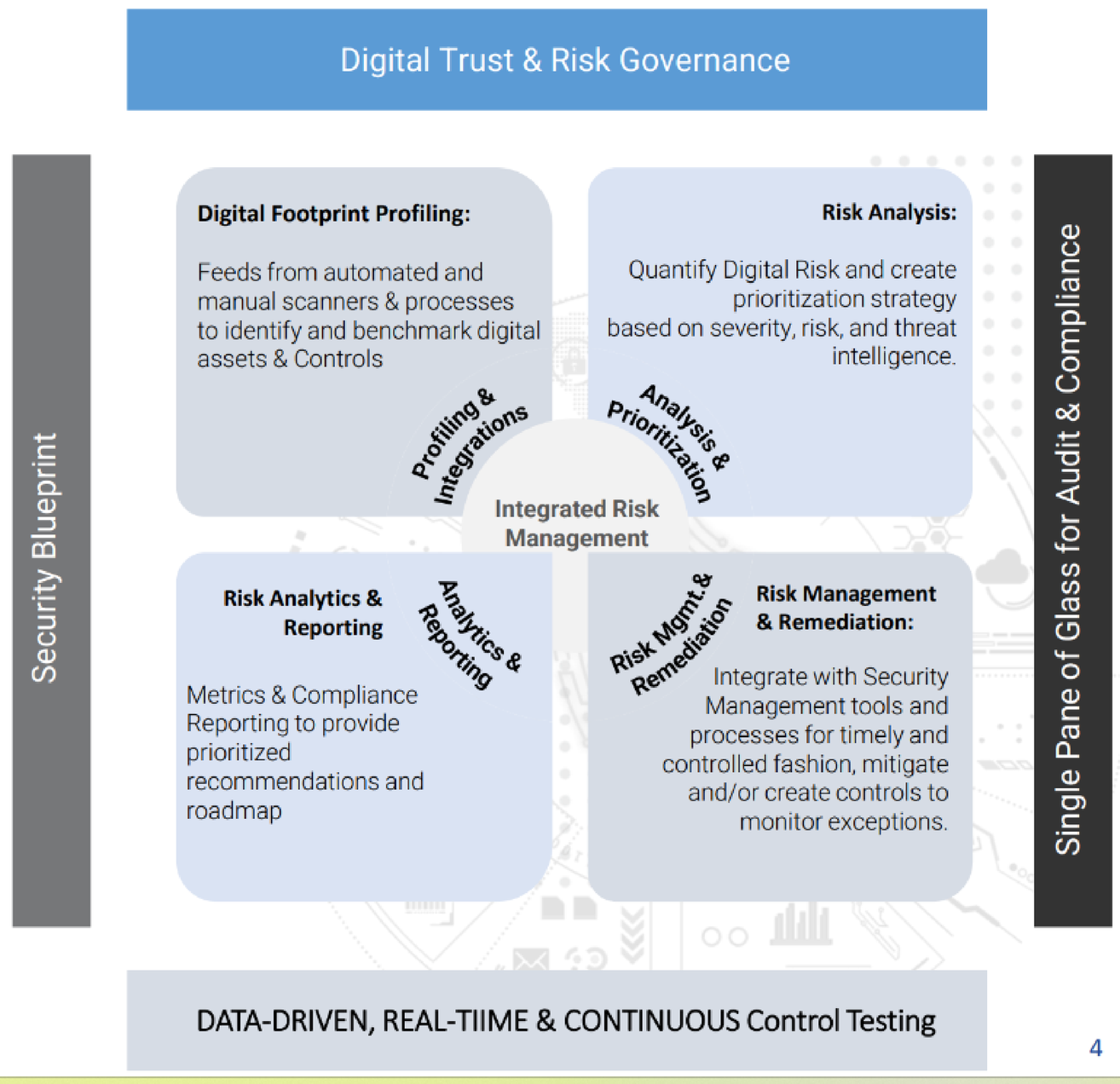
DigitalXForce, known as "Digital Trust for the New Era," presents a unified SaaS digital trust platform that provides real-time, continuous integrated risk management. By leveraging data-driven insights, security blueprints, and regulatory control mapping, DigitalXForce optimizes and automates the digital risk posture of your organization.

DigitalXForce Functions & Architecture

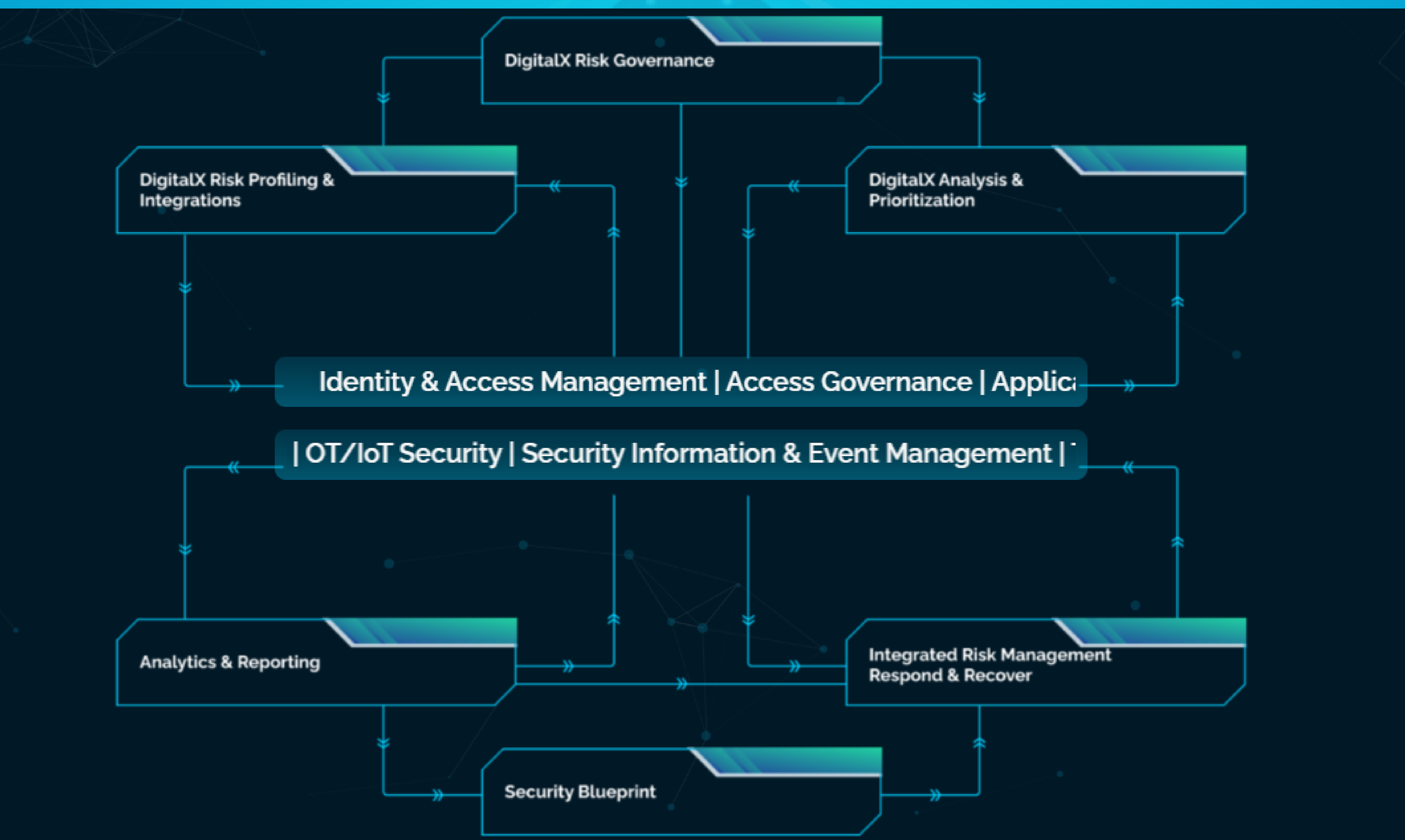
DigitalXForce - *Digital Trust For the New Era*

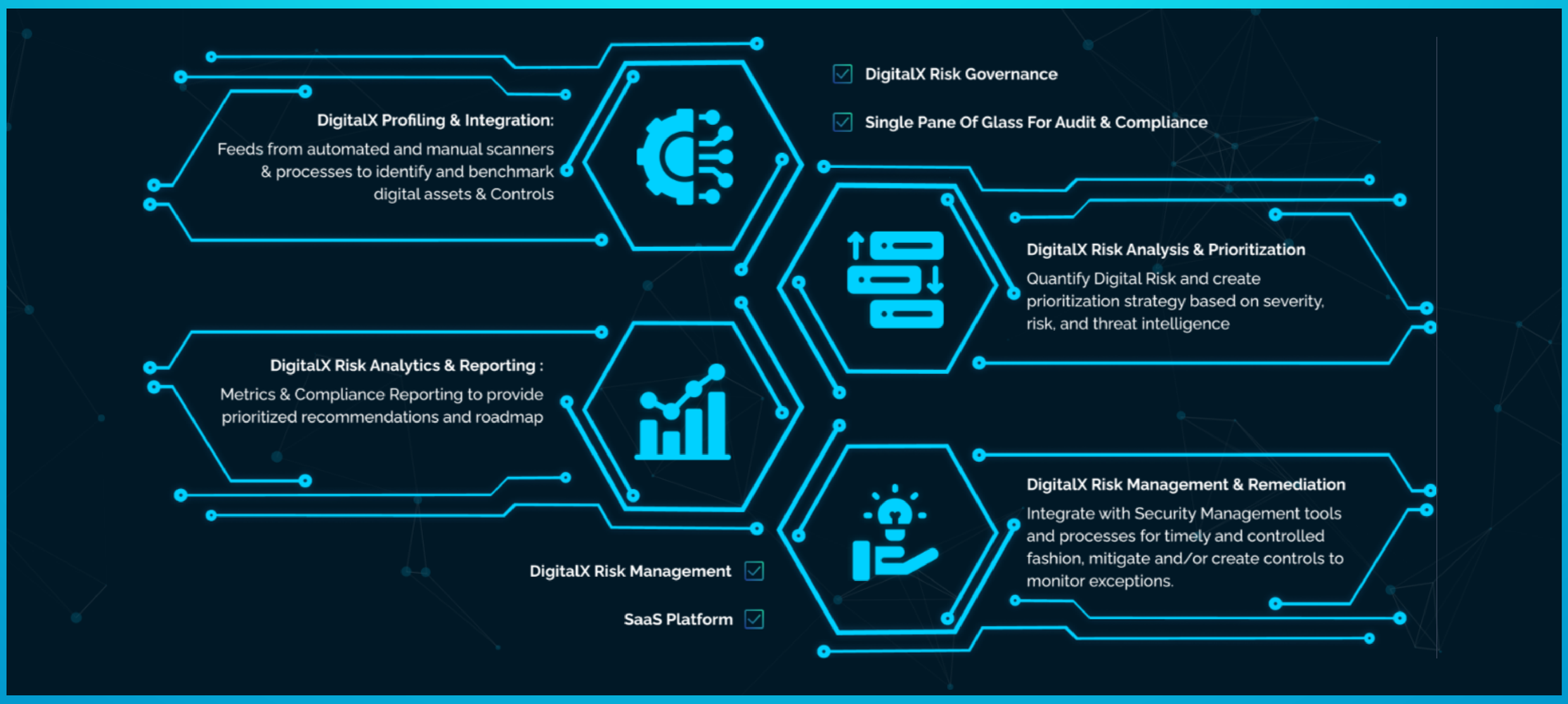
- NIST 800-53 / NIST CSF driven **SaaS platform** to protect enterprise digital assets by integrating security services into central hub model while maximizing visibility, effectiveness and efficiency with unified view through measurable KPIs/KRIs. DigitalXForce follows the model of Identity, Detect, Protect, Respond and Recover to service end to end security with AI, ML and integration into enterprise services.

- The security capabilities include, but not limited to:
  - Identify ALL Digital Assets
  - Integrates with ALL Cyber Security services in play
  - Integrate with and Analyze cyber security services
  - Develop Security Blueprint
  - Develop Security Scorecard and Dashboard
  - Develop Security Plan of Action
  - Operationalize Security Plan



How DigitalXForce Helps





Maximize Your Cybersecurity Return on Investment (ROI)

DigitalX – Board Dashboard

Demonstrates organizational KPIs and KRIs through Security Scorecards and Security Blueprints.

DigitalX – Identify & Profiling

Identifies all IT / Business Assets and Security Tools through feeds from automated and manual scanners & processes to identify and benchmark digital assets & Controls

DigitalX – Security Management & Operations Plan Generator

Generates a plan for security management and ongoing operations

DigitalX – Connect

Connects Cyber Security services in play for execution of control scripts for Automated DigitalX risk management

DigitalX – Policy Reviewer & Generator

Reviews and analyzes the systems and policies implemented for comprehensive security management.

DigitalX – Analyze

Real Time and Continuous Analysis of Cyber Security Services designed to monitor potential security incidents for their coverage, capability and effectivenes

DigitalX – Report

Metrics & Compliance Reporting to provide prioritized recommendations and roadmap

DigitalX – Respond & Recover

Integrate with Security Management tools and processes for timely and controlled fashion, mitigate and/or create controls to monitor exceptions

DigitalXForce Solution & Modules

DigitalXForce

Automated Audit & Compliance and Risk Assessment	❖ Reduce the time and effort required to maintain compliance, enhance their risk management capabilities, and ultimately build a more secure and resilient IT environment.
Attack Surface Management & Asset Inventory	❖ Attack Surface Management (ASM) and Asset Inventory form the crux of a robust cybersecurity program. Reduce the risk of a security breach by identifying, monitoring, and managing digital assets.
Real-time, Continuous Integrated Risk Management	❖ Proactively identify and address potential threats, reduce the impact of security incidents, and ultimately build a more secure and resilient IT environment.
Board Level Metrics & Report Generator	❖ Equip your board members and executive leadership with information to make informed decisions on cybersecurity strategy, resource allocation, and risk management to build a more resilient IT environment.
Cybersecurity Risk Quantification & Prioritization	❖ Make informed decisions on resource allocations and risk mitigation strategies to proactively address potential threats and minimize the effect on business operations.
Cybersecurity Policy, Plan and Procedures Reviewer & Generator	❖ Create and maintain a robust policy framework aligned with industry standards, best practices, and regulatory requirements
Cybersecurity and Privacy Risk Remediation Planner	❖ Proactively address potential security risks and vulnerabilities, improving their overall security posture and reducing the likelihood of security incidents.
Security Blueprint Generator	❖ Design and implement an effective and tailored security strategy to improve overall security posture and maintain compliance with industry standards and regulations.
Third Party Risk Management	❖ Proactively identify and address potential threats, reduce the impact of security incidents related to Third Party.
Crisis Simulation / Tabletop Exercises	❖ Perform Incident Tabletop Exercises and Crisis Simulation with pre-defined scenarios/scripts and automated report generation
Cyber Insurance Application Processor	❖ Profit from a faster, more efficient application process, better coverage options and more competitive premiums with an automated cyber insurance application processor

iTrustXForce - Global Pioneer of Digital Trust

iTRUSTXForce is a global **DigitalX** (Cybersecurity, Privacy & Digital Trust) Service provider. iTRUSTXForce offers end to end **Outcome Based & Packaged DigitalX Services** in "DigitalX-as-a-Service" and "Managed Services" format powered by proprietary **iTRUST** (Integrated | Tailored | Realtime & Risk Based | Unified | Secure-By-Design| Threat Based) framework and toolkits to enable Digital Trust.

iTRUSTXForce's DigitalX services enables business resilience through a highly specialized workforce addressed as "**Guardians of the XForce Galaxy**", Our eco system partnership model through "**Digital Trust Consortium"** Service Partners with global delivery network capabilities, Full Suite end to end cybersecurity service offerings, and partnerships with leading technology players.

iTRUSTXForce is Industry's ONLY Service Provider providing **Outcome Based & Packaged** Cybersecurity & Privacy services and clients **DON'T** pay until the OUTCOME is delivered

What makes iTRUSTXForce Unique

TRUSTED PARTNER

- Deliver Outcomes versus stand along tool deployments
- Vendor neutral company to deliver the solution that fits your needs

* CLIENTS DON'T PAY UNTIL OUTCOMES ARE DELIVERED

DIGITRAL TRUST CONSORTIUM powered by Proprietary iTRUST

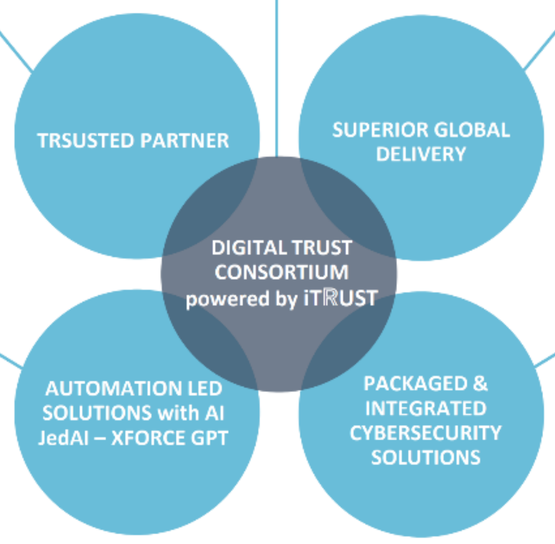
- Proprietary **iTRUST** framework (Integrated |Tailored | Real Time & Risk Based | Unified | Secure-By-Design | Threat Based)
- Delivering Digital Trust & cybersecurity solutions with Specialized Teams

GLOBAL DELIVERY NETWORK

- Global Delivery Model (Onshore, Near Shore, Offshore)
- Delivered seamlessly, on-demand, wherever and whenever our clients need us

AUTOMATION with AI JedAI – XFORCE GPT

- Build in innovation and automation for better efficiency
- Platforms and Toolkits for accelerated delivery & standardization



OUTCOME BASED PACKAGED CYBERSECURITY SOLUTIONS

- Help clients improve security posture by bringing business outcome driven solutions with specialization
- XF Universe for Digital Trust, iTRUST XFG 4 Cyber Threat Management, iTRUST XFG 4 Cloud & EDGE Security, iTRUST XFG 4 IAM,

What You'll Get...

Our Digital X Service Offerings

OUTCOME BASED & PACKAGED SERVICES	INTEGRATION SERVICES W SPECIALIZATION	EXPERT & CAPACITY SERVICES
ITRUST XFORCE UNIVERSE (XFVERSE) 4 DIGITAL TRUST		
➢ ITRUST XFGALAXY 4 RISK MANAGEMENT ➢ ITRUST XFGALAXY 4 CYBER THREAT MGMT. ➢ ITRUST XFGALAXY 4 CLOUD & EDGE SEC. ➢ ITRUST XFGALAXY 4 DIGITAL IDENTITY & ACCESS MGMT. ➢ ITRUST XFGALAXY 4 APPSEC & DEVSECOPS	• DIGITAL TRUST & AI RISK MANAGEMENT • IDENTITY & ACCESS MANAGEMENT • CLOUD & INFRA SECURITY • APPLICATION SECURITY & DEVSECOPS • INTEGRATED CYBER THREAT MGMT. • DATA PROTECTION & GOVERNANCE • SECURE EDGE (OT/IOT) SECURITY	• DIGITAL TRUST MGMT. • IDENTITY & ACCESS MANAGEMENT • EXTENDED ENTERPRISE (CLOUD, OT & IOT, EDGE) SECURITY • APPLICATION SECURITY & DEVSECOPS • MANAGED SECURITY SERVICES

INDUSTRY SECTORS – HEALTHCARE, PUBLIC SECTOR, FINANCIAL SERVICES, ENERGY & UTILITIES, TECHNOLGY, CONSUMER SERVICES & RETAIL, REAL ESTATE, HIGHER ED

DIGITAL TRUST CONSORTIUM

TECHNOLOGY PARTNERSHIPS | **SERVICE PROVIDER PARTNERSHIPS**

DIGITAL TRUST CONSORTIUM

OUR COMMITMENT : Cybersecurity should Build Digital Trust and SHOULD not be a Complex or Costly Affair

Consortium with over 2 decades of Experience

Hundreds of Cyber Specialists

Hundreds of Active Clients spanning globally

Global Digital Trust Hubs

10+ IP / Platforms

25+ Alliances & Partnerships

GOAL Become **Trusted Partner** for Outcome Based Digital X (Cybersecurity, Privacy & Digital Trust) services powered by proprietary **iTRUST** framework (Integrated |Tailored | Real Time & Risk Based | Unified | Secure-By-Design | Threat Based)

Mission Serve the Community with Purpose & Secure the Future by enabling "***Digital Trust Inside Out***"

OUR DIFFERENTIATION: We are **Industry's ONLY Service Provider** providing **Outcome Based & Packaged** Cybersecurity & Privacy services through **Digital Trust Consortium** in "DigitalX-a-a-Service" and "Managed Services" format and clients **DON'T** way until the **OUTCOME** is delivered

Eco System Partnerships with leading Technology & Service Partners. Unmatched security expertise with ongoing **Alliances & Partnerships** with Business Outcome driven **Technology & Service Partners** to create cost effective solutions

Digital Trust Consortium enabling Global Delivery With Localized Teams Delivered seamlessly, on-demand, wherever and whenever our clients need us

Digital Trust & Cybersecurity Industry Leader Advanced Security capabilities- — powered by iTRUST, DigitalXForce and iTRUST Cyber toolkits, are recognized by Industry Analysts

*** The numbers above are collective number from our Digital Trust Consortium**

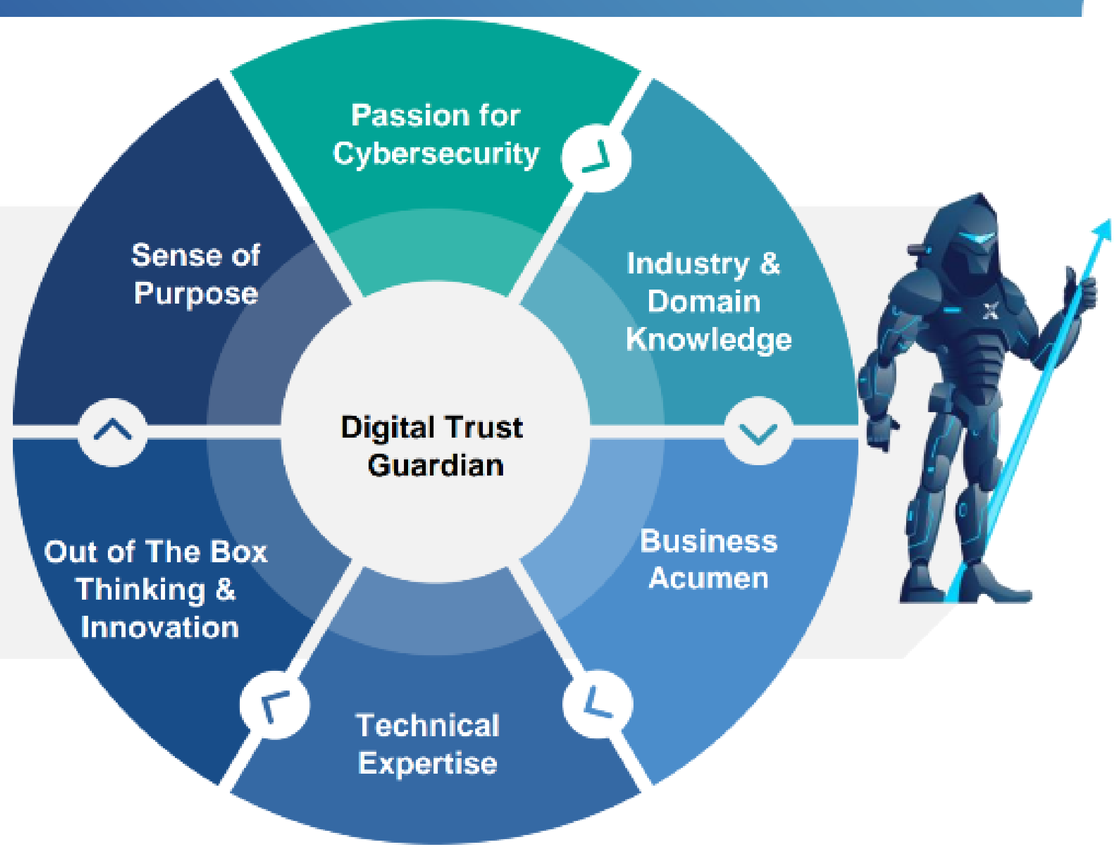
Lalit Ahluwalia is the CEO & Global Leader for Cyber Security and Digital Trust Solutions at iTRUSTXForce.

Lalit has over 23 years of experience in the consulting space delivering and managing enterprise-wide cyber programs. He leads the go-to market strategy for Cyber Services bringing “iTRUST” based and Industry tailored services to global clients through an integrated delivery model with built in innovation & automation platforms and in partnership with ecosystem partners and alliances.

Lalit’s leadership, management and creativity were integral to the thriving global security practice at Accenture, Wipro and Deloitte encompassing the Health and Public Sector, Retail, Resources and Financial Services industries nationally and internationally

Our service quality and high performance is a direct outcome of our people, referred as “**Guardians of XForce Galaxy**”, that are collaborating with our clients, aligned with their mission, and serving them with integrity. We are committed to partner with cybersecurity professionals and Consortium Partners that share our passion.

Our professionals have dedicated their careers to cybersecurity, paving the way for many organizations to achieve their cyber goals, and will be actively engaged with you.



Need to talk? Reach out!

Lalit Ahluwahlia
Founder & CEO
DigitalXForce & iTrustXForce
Tel: +1 (972) 342-0073
Email: lalit.ahluwalia@cyberxforce.com