

VISIONET

Assure Resilience Across Your Enterprise

An ultimate guide to thrive
in the face of uncertainty



TABLE OF CONTENTS



- 02 Introduction
- 03 What entails enterprise security?
- 04 A Zero-Trust Paradigm for a Perimeter-less World
- 04 Why is a Sound Enterprise Cybersecurity Solution a Business Essential?
- 07 How can Team Visionet Help you Achieve that?
- 07 Additional Benefits
- 08 About Visionet
- 08 Contact Visionet

Introduction

In the past decade, the attack surface for many businesses has dramatically taken new turns. Conventionally, companies would only be liable to secure data housed in on-premise systems and implement cutting-edge security measures to keep their systems safe and prevent data breaches. With the fast-paced tech revolution, cyberattacks are also evolving.

What was once limited to monetary gains has now extended to social or political benefits or just an unfair advantage over a competitor.

Customer demands are transforming at the speed of light, and so are technological advancements. More companies now use integrated technologies to cater to a large user base, streamline procurement solutions, and enable ideal working solutions for their geographically dispersed teams. However, adapting to a digitised ecosystem doesn't come without its costs. Exposure to even a minor risk could cost businesses millions in just a few seconds. This requires incorporating a defence mechanism that doesn't just do the bare minimum and protects your data from all attack surfaces.



What entails enterprise security?

In simple terms, enterprise security refers to the strategies, methodologies, and policy implementation for protecting data and IT assets against unauthorised access, malicious attacks, and vulnerabilities that could compromise an organisation's privacy, integrity, and reliability. Enterprise security progressively expands to critical data transfer across multiple channels, including integrated networks, servers, and end-users – catering to Technology, People, and Process, to build a secure digital space for an enterprise..

Security Threats in the New Normal

Without a surprise, COVID-19 has disrupted how the digital world operates, forcing us to change our perspective and rethink how things are practically done. The world is on the continuum of shifting to a disruptive place where more businesses are switching to innovative technologies, including cloud infrastructures and SaaS applications, where more employees are mobile and dispersed, and where our identities and connections are increasingly stored on digital fronts. As a result, more personally identifiable information and other sensitive data are now easily available.

Organisations of every scale now have the leverage to access high-end and configurable technology, mitigating the limitations of geographical boundaries. Although many enterprises can now successfully extend their operations globally, a great amount of data remains inaccessible to all key stakeholders. Using cloud computing but not having complete access to all the stored data and cloud software is a significant caveat. Therefore, the adoption of multi and hybrid cloud ecosystems further complicate security landscape.



That said, cybersecurity experts must assume that their environments are not safe, their systems have been infiltrated, and that internal attacks may be equally as detrimental as those coming from outside the company. To put it another way, we must transform our security notions from transitive to zero-trust.

A Zero-Trust Paradigm for a Perimeter-less World

As organizations navigate to hybrid cloud solutions, businesses also need to look into effective measures for managing the data security risks that accompany it. A zero-trust security strategy, following a deny-by-default policy and access for every interaction, both internal and external, helps organizations transform to a more perimeter-less corporate environment, keeping your data, users, and resources secure.

Add more content

Companies that didn't deploy Zero Trust suffered an average data leakage cost of

\$5.04 million

Source: IBM Cost of a Data Breach Report 2021

Why is a Sound Enterprise Cybersecurity Solution a Business Essential?

A sound enterprise cybersecurity solution lays the foundation for your business to adopt a modernized security strategy based on zero-trust principles. It offers a comprehensive and integrated range of enterprise security solutions and services powered by AI, empowering your business to:

Align your security plan with your enterprise's needs.

Integrate solutions to safeguard your online users, resources, and

Leverage technology to manage your security against ever-increasing risks.

Govern risks in hybrid multi-cloud settings.

Future-proofing security solutions for long-term viability:

Enterprises can further ensure their business's resilience by leveraging the following service capabilities:

Security Operations Center (SOC)

An optimal Security Operations Center (SOC) serves as the brain of an effective cybersecurity program, operating as a hub for corporate-level threat detection capabilities for individuals entrusted with thwarting cyber security risks. Employing a SOC with intelligent integration and automation can assist an organization's information security governance as with real-time data synchronization, they're more empowered to proactively respond to incidents in a more precise and efficient manner. In a nutshell, businesses can detect and resolve threats, vulnerabilities, and data leakages faster and at early stages.



Intrusion detection

Digital forensics extends from the branch of forensic science that centers on recovering and analyzing data that was retrieved from the digital devices used in cybercrimes. This service has since expanded to encompass network forensics, which entails examining network vulnerabilities, malware attacks, and data leakages, among other things. Our team of experts meticulously assists in the recovery, analysis, and restoration of computers and relevant materials in such a way that they can be presented as evidence in the legal proceedings as well as the postulation of the act's intent followed by the identity of the main perpetrator, whether internal or external.

Security Solution Implementation

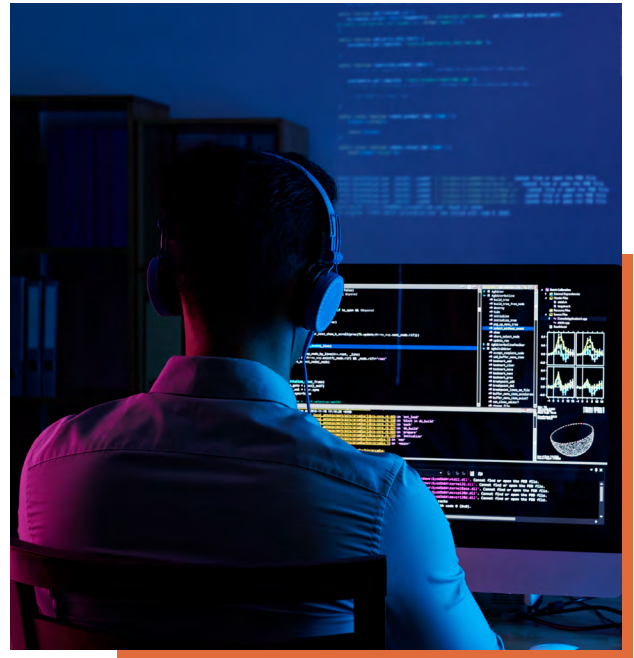
Have you ever considered why, despite the various "security solutions" accessible today, cybercriminals are effortlessly able to flare up millions of servers and computers around the world?

For many years, security experts have been misdirecting organizations into believing that firewalls and anti-virus technologies are the answers to a secure corporate infrastructure, which apparently is not! Many of the emerging security solutions today cater only to a fraction of the overflowing security challenges. But security is more of a process than just a single product or solution.

Our team of trained security consultants has extensive know-how and industry expertise in assisting businesses in identifying proven strategies to provide a secure IT and business environment. We follow industry-accepted best practice standards to ensure your projects are executed on time and under budget without compromising on data security.

Digital forensics

Digital forensics extends from the branch of forensic science that centers on recovering and analyzing data that was retrieved from the digital devices used in cybercrimes. This service has since expanded to encompass network forensics, which entails examining network vulnerabilities, malware attacks, and data leakages, among other things. Our team of experts meticulously assists in the recovery, analysis, and restoration of computers and relevant materials in such a way that they can be presented as evidence in the legal proceedings as well as the postulation of the act's intent followed by the identity of the main perpetrator, whether internal or external.



Vulnerability Assessment and Penetration Testing

Vulnerability Assessment and Penetration Testing (VAPT) refers to a variety of security assessment services designed to identify and mitigate cybersecurity risks across an organization's IT ecosystem. However, it is crucial to understand the many types of VAPT services along with the variations between them before choosing the appropriate form of an evaluation strategy meeting your organization's requirements. As VAPT evaluations vary dramatically in terms of depth, scope, complexity, and price, this knowledge is essential for ensuring that tests provide your business with the best value for money.

This is where Visionet always professes to achieve the best suitability according to the customer's security requirements. With our experience in a broad spectrum of compliance standards, we ensure smooth periodic assessments and audits, so your business can operate and grow without any limitations or data breach exposure.

How can Team Visionet Help you Achieve that?

The Visionet's Differentiator



Quick Expert Consultation

150+

certified experts to help you transform Zero Trust into action faster.



Proven Results

50+

successful automation and security project executions



Context based Security

Secure users, data, and resources with security AI and hyper-automation journey.



Up and Running Integrations

Frameworks to integrate your security tools with partner's ecosystems enabling seamless zero trust strategy.

Additional Benefits

Optimize levels of data access

When you transition to a hybrid, multi-cloud infrastructure, your resources are likely dispersed over several different IT environments differing in levels of visibility and management. It's difficult to tell if the appropriate users have access to the right information. Visionet's Zero Trust security services may help enterprises elevate their cyber resiliency and surpass the risks of the disconnected environment. Our model helps enterprises use the context to securely link the right users with the right resource, at the right time and under the right circumstances, all while preventing data leakages and cyber attacks.

Systematically tested to enhance cyber resilience

According to statistics, companies that have developed incident response (IR) teams and tested their incident response strategies faced \$2.45 million lesser data breach costs than those that didn't. Visionet experts capitalize on Zero Trust security services and test each system with real users and customers, allowing businesses to put the phrase "train like you fight, fight like you train" into practice. We assist businesses in developing and testing incident response playbooks to better equip them to respond to threats while also strengthening their cyber resilience.

Quantifiable Financial Impact

Visionet employs organization-specific data to enable businesses to identify potential security gaps, develop user-centric solutions and suggestions to help them minimize the impact of any attacks, and quantify security risks into immediate, quantifiable financial impact.

What's Next

About Visionet

Visionet's thorough security expertise and solid track record of delivering cutting-edge solutions broadened with IBM Zero Trust Acceleration services have helped improve hybrid cloud transformations, reduce complexity, build actionable zero trust plans, prevent data leakages and establish an integrated security framework for a perimeter-less business environment



World-Class Delivery

We approach technology delivery as a combination of high-value consulting and deep domain expertise. Our clearly differentiated value proposition consists of transformational technology delivery services and end-to-end support for selected software packages.



Deep Domain Expertise

Visionet has over 25 years of experience in serving the global security industry. With our experienced security consultants and overall experience in the industry, we provide unmatched value to our customers that help them stay ahead of their competition.



Seamless Technology Adoption

Disruption-free adoption and integration of technology to help you accelerate your zero trust security strategy



Guaranteed Compliance

Our compliance solutions accurately verify hundreds of business rules and regulatory standards in moments.

VISIONET

Digital Defined | Digital Delivered

www.visionet.com