



UNLOCKING CYBER SECURITY



Whitepaper

From best practices to defensive AI and ML— know the practical solutions








USA | Costa Rica | India



info@feuji.com

Table of Contents

	Where do We Start	02
	Start Here: Don't Fall for Myths.	02
	Cybersecurity Implementation Using Defensive Artificial Intelligence (AI) and Machine Learning (ML)	04
	Combating Ransomware Using Technical and Organizational Solutions	05
	Four Ways You can Fill in Some Blanks	07

Where do We Start

A security strategy will provide you with expertise and guidance as you develop and implement a holistic, enterprise-wide approach to cyber risk management. It may be necessary to hire a consultant or security expert who can see beyond the obvious and make assessments relevant to your infrastructure.

Start Here: Don't Fall for Myths

You don't just have external hackers to deal with but internal agents as well.

43%

of all data breaches are [internal](#) to the organization

Identifying the "right" metrics can end up being the wrong metric

72%

of 200 CEOs interviewed said that they needed better metrics to take actionable decisions when it came to cyber security

You aren't secure just because you are a small company

Just because you are small, it doesn't make you less vulnerable.

70%

of all hacking happens due to [financial motivation](#).

Having a dashboard is good enough to monitor security

87%

of 200 CEOs interviewed felt that the dashboard, no matter how pretty it looks is not sufficient to thwart an attack

Confidence is not a good metric

37%

of respondents felt their organizations were very secure. Assessments suggested that they had insignificant risk mitigation and security protocols



The answers you look for must be based on



**Current and future
cybersecurity risks**



**What threats need to
be prioritized**



**What controls need to
be put into place**



**How your teams are
currently managing
cybersecurity programs**

Cybersecurity Implementation Using Defensive Artificial Intelligence (AI) and Machine Learning (ML)

To counter the rapidly evolving threat of ransomware, organizations should take a risk-based approach to automation, using AI and ML to stay abreast of changing attack patterns.

There is a rapid evolution happening as you read this article, on the future of cyber security. AI and ML can be used to understand the evolving nature of ransomware attacks, predict future attack vectors, and develop automated technical responses to limit damage during an attack. Companies are realizing that using CAPTCHA is simply not sufficient as AI is able to read through.



Both AI and ML have come through as crucial technologies to combat cybercrime, detect malware, potential DDOS, intrusion, threats from bots and other cyber threats. Machine learning (ML) helps you predict what could happen using regression-based algorithms and complex statistical analysis of data. Ultimately, humans have to get involved in the process to use AI and ML effectively to prevent or at least reduce threats.

Combating Ransomware Using Technical and Organizational Solutions

Ransomware has evolved significantly, and the sophistication and frequency of attacks are increasing. To counter these developments, organizations must respond with changes to their technical environment and operational culture. To prepare for ransomware and other cyber-attacks, you need to combine a technical response with an organization-wide response. The technical changes might include using resilient data infrastructure and repositories, automated responses to malicious encryption, and advanced multifactor authentication to limit the potential impact of an attack.

Organizations need to plan for all options and contingencies so that business continuity and disaster recovery can be executed by experienced executive decision makers. A business continuity plan defines the roles, responsibilities, and actions of key personnel in the event of an emergency. Business continuity planning is not a one-time event. It requires ongoing development and support over time. Preparation activities include conducting tabletop exercises, developing detailed, and multidimensional playbooks, and preparing for all options and contingencies including executive response decisions to make the business response automatic.





***“If you think you know-it-all about cybersecurity, this discipline was probably ill-explained to you.”
— Stephane Nappo***

Four Ways You can Fill in Some Blanks

According to this [McKinsey](#) report, the response to the third trend of increasing resource gaps and regulatory scrutiny is four-fold:

a

Creating a secure software development life cycle (SSDLC)

Many companies use software development life cycle (SDLC) to create software, but these processes often ignore security. By building security into SDLC from the outset, organizations can develop more secure software that is less vulnerable to cyber threats. One way to do this is to have security and technology risk teams engage with developers throughout each stage of the development process. Another way is to ensure that developers learn certain security capabilities best employed by themselves, like threat modeling, code, and infrastructure scanning, and static and dynamic testing.

b

Taking advantage of third-part cloud environments

Third-party cloud environments can offer a path to a more secure, cost-effective, and scalable future for organizations. Cloud providers handle many routine security, patching, and maintenance activities and provide automation capabilities. Migrating some or all your infrastructure to third-party cloud environments such as platform as a service, infrastructure as a service, and hyperscale providers can benefit cyber teams by simplifying the management of infrastructure and workloads.

However, when migrating to the cloud, organizations should closely consider the basis of their current security posture and how it might change. While moving to the cloud can simplify management and maintenance, new risks can also emerge. For example, some cloud service-level agreements do not include explicit support for critical systems or cybersecurity events. Cyber teams should closely examine such contracts and develop plans to address gaps in service-level agreements' protections during transition periods or emergencies.

c

Codifying and standardizing infrastructure and control-engineering processes

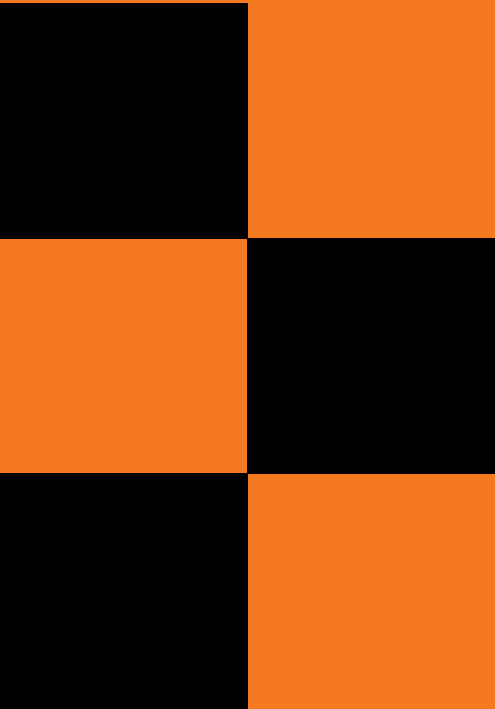
The emergence of multi-cloud environments has challenged enterprise IT teams to manage the complexity of multiple clouds and their hybrid deployments. Creating a standardized, codified infrastructure and control-engineering process in hybrid and multi-cloud environments can simplify management and improve the system's resilience. This approach enables processes such as orchestrated patching, rapid provisioning, deprovisioning, and more.

d

Detailing all components and supply chain relationships used in software

Compliance rules are continuously changing. How your team meets these challenges will impact the efficiency of your software development, as well as your security posture. To help mitigate compliance risk, organizations should expand documentation on all components used in codebases and their third-party relationships through new software development processes. By creating a detailed bill of materials that includes open-source and third-party components used in software, organizations can ensure that they are prepared for regulatory inquiries and satisfy growing compliance requirements.





To get a free consultation on how we can help you deal with this enormous problem, and find solutions that are tailored to you, it would help you to have a conversation with us. We'd be excited. Just drop a note by contacting us via www.feuji.com/contact/



CONTACT US

 USA | Costa Rica | India

 info@feuji.com