# Cyber 2027: 10 key moves to elevate your cybersecurity game

#### WAVESTONE

Cyber Insight Day 2024



Gérôme BILLOIS Partner gerome.billois@wavestone.com



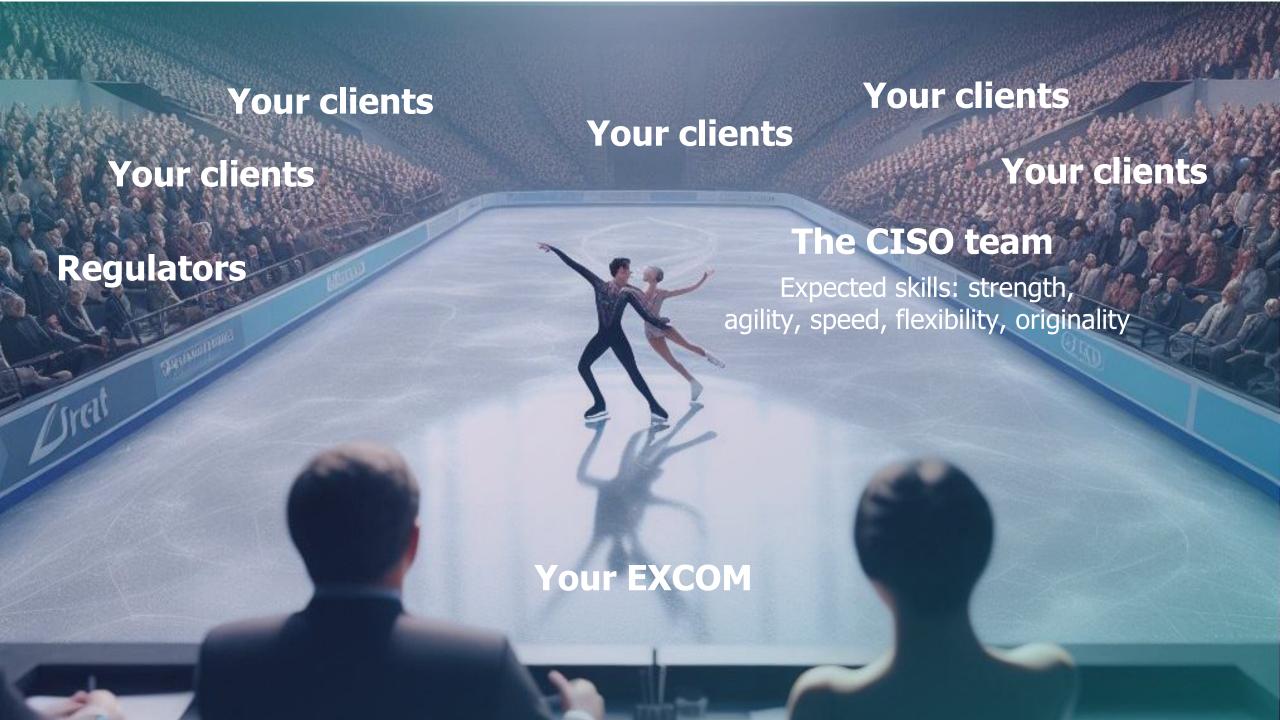
Matthieu GARIN
Partner
matthieu.garin@wavestone.com

#### Let's state the obvious

the *cybersecurity landscape* will constantly uncover

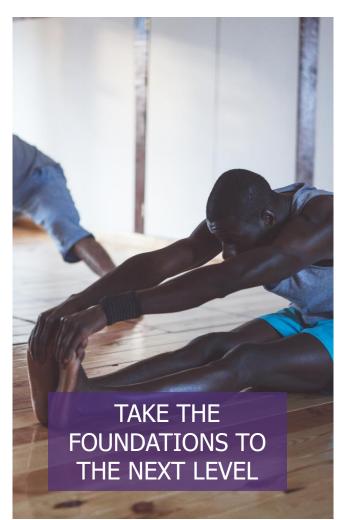


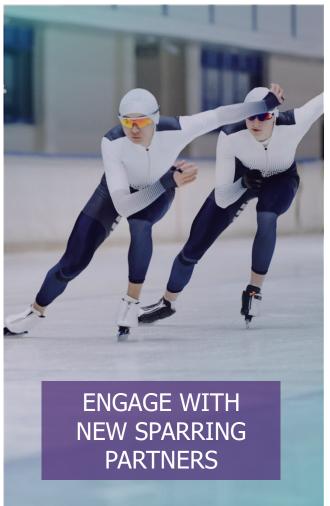
To face this ever-changing environment, CISO need to develop multiple skills: strength, agility, speed, flexibility, originality

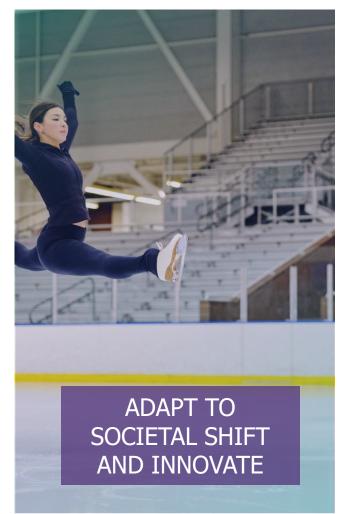


# +20 CLIENTS' STRATEGIES analysed...

## 10 key moves







Cloud Security

Zero-Trust

TAKE THE FOUNDATIONS TO THE NEXT LEVEL

Culture Change







#### Shift to run mode Ensure your basics are strong

- /Make security a **priority in infrastructure projects** with a *secure-by-design* approach
- /Break down silos between the security team and the cloud center of excellence with an agile delivery approach



## Leverage security advantages *Automate and measure*

- / Facilitate **seamless scaling** through the **CI/CD** automation chain and employee upskilling
- /Improve efficiency with continuous control and agile methods
- /Adopt new strategies: "no admin" approach in collaboration with your CTO, deceptive security...

#### **Zero-Trust:**

#### Beyond the philosophy, now we know what to do

Metherly						ALC: UNKNOWN		Towns Co.
MORISH								
_	Sentine on substituted ung white passions or nutricial substitution (RE), with most and permanent scores for ents ubstitution to stored and managed remains and uniquestions.	poster victivi dia ecceptia and access partient, in serie di compliana, configuration in	The netroil archaecus use tarp opinior or netro appreciali. Reset sulle as injection, fact, a serip and existly. Taffic is serip and existly and the seriminal reliens replaces for certises.	Access to applications in based on coops authorization. The company performs manual application excurts, testing prior to delignate manual control points delignated in mediatants. See these folial applications are directly accessible to comprise the memoral will all others excluded trimingly a 10%.	Date is musually destribed, company angles limited and act free date congestration appelithes. Furly date is available from on-precise stress with no bestupe or a fine off size facility. Enrygation is any minimal and mixed or minimal and mixed or mixed or		Company while on opinic and thereal processes to sometime special and recommendation with longic automation.	Circumy implements policie if an ad flac manner access the amongree, and pulpose will and an amongree processes or state technique mediaments.
-	Circiany subvections dentity using 198 the may include guaranced and number suicides. It is also and number of subvections for account of a subvection are stand both on opening and white head standard or the subvection of which head standard.	company and regions device dissupported to the very limited influences to recovering it made and investigate related used and investigate related using a related to the company of the company of the company of the company of the company of the company of the related to the company of the co	Darlet state viet to all	Company bagins to authorities access to applications based for companied other states and bagins in sequence states a process of the companied application workflows. It provides reflects states for development, states and produced workflows, and the companied of the companied o	Date are stored both on premise and in cloud or months and in most of an partial, investment Cumpans organized begins to incorporate months are pained data see and to in impagement a data interpretation mixings, premain months, 4th data in barrier or months, 4th data in barrier are controlled.	mission orbital functions and requirely assesses processes for gap in	Circuity bagins automating archesters and reporter patricine is against if orbital resource functions.	Campany define and begins inclinating public to present a designation with mornal autorapea and manual colonia.
-	Company begins to authorisate of distributions using plasting resident and passervices TMs. It determines most destroy in All authorisate analysis and directive video.	Company uses automated method to traverage of physical and other assess, segment eithers, and shortly submetabless and negal paceline. It begins no side-ellow and extraorrise view of all methods as automated processors. It also happens in regions or regions as regions.	cone internal incre engineeration, company instalments dynamic natives have configurations for recovere optimization find are periodically membrated. Provident application of internal and external traffic and a recoveranced by ber	decions with effected explanal conditions. These protections in conditions are consistent of conditions are conditional terms for the discretion and condition and resignate explanation assums and resignate explanation assums.	gen state attributes. Data	automated solitation of logs and electronic enterprise mide (middleg initial) and consequently for consisted analysis that consistes across multiple assumes	Company automates contention and reporter and history energine with temping to metallal internation from multiple assumes to inform discourse	Cargony individuals send, palmed palme emerginench palme benager pubmellar infere position to supply designation from palmed palmed position palmed palm
_	security integrated within all partners. Role are determined	compliants and automatically imagestes or forware configuration and null residently management across of physical and original seasobs. It also has mainthream inter- ful assets across comprises and null seasobs across comprises and	to internal and external locations to encounted and incomprates that practices for organization practices for organization and the	Spinner press crown regress aplicator south rating thoughts the others device an	cliud das less prevention stranges are dinamically literary automated data selfitation. Company uses dinamic materials to optimize data positionity and encounts of	Company mandaring companies and collection and an artist collection of committee of the collection of	Company unfrecision and regional activities (financial) regional to principal and charging regularisation and antiferrantial charges.	Company implements and fully automate errors have sele- ptime the wealth seleval load operate with portropials with committee of dynamic uniforment and dynamic uniform.

Source: Wavestone Zero-Trust Maturity Assessment (based on CISA maturity assessment v2)

Identity, Device, Network,
Applications & Infrastructures,
Data

Visibility & Analytics, Automation & Orchestration, Governance

**76** topics, **4** Maturity levels

**Zero-Trust specific projects** 

**Zero-Trust Access** 

Micro-segmentation

#### an obvious target but an incremental journey

#### **Build for the future: adopt a convergence approach**

**Monitor and demonstrate convergence** towards Zero-Trust through dedicated KPIs

- 1 % of critical applications managed with conditional access
- 2 % users covered by Zero-Trust Access principles
- 3 % of applications covered by entitlements management
- 4 % of critical environments covered by micro-segmentation
- 5 Number of criteria to assess the level of trust

and ensure all new projects are **compatible** with Zero-Trust

## Move from awareness to

#### culture change

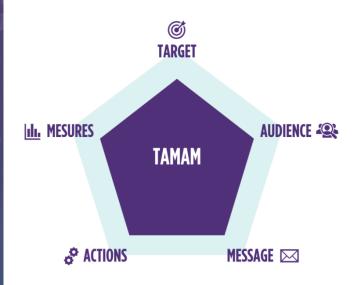
To move towards targeted behavioural change:

**Engage** with *local populations* to understand practices and **identify** *risk areas* to target

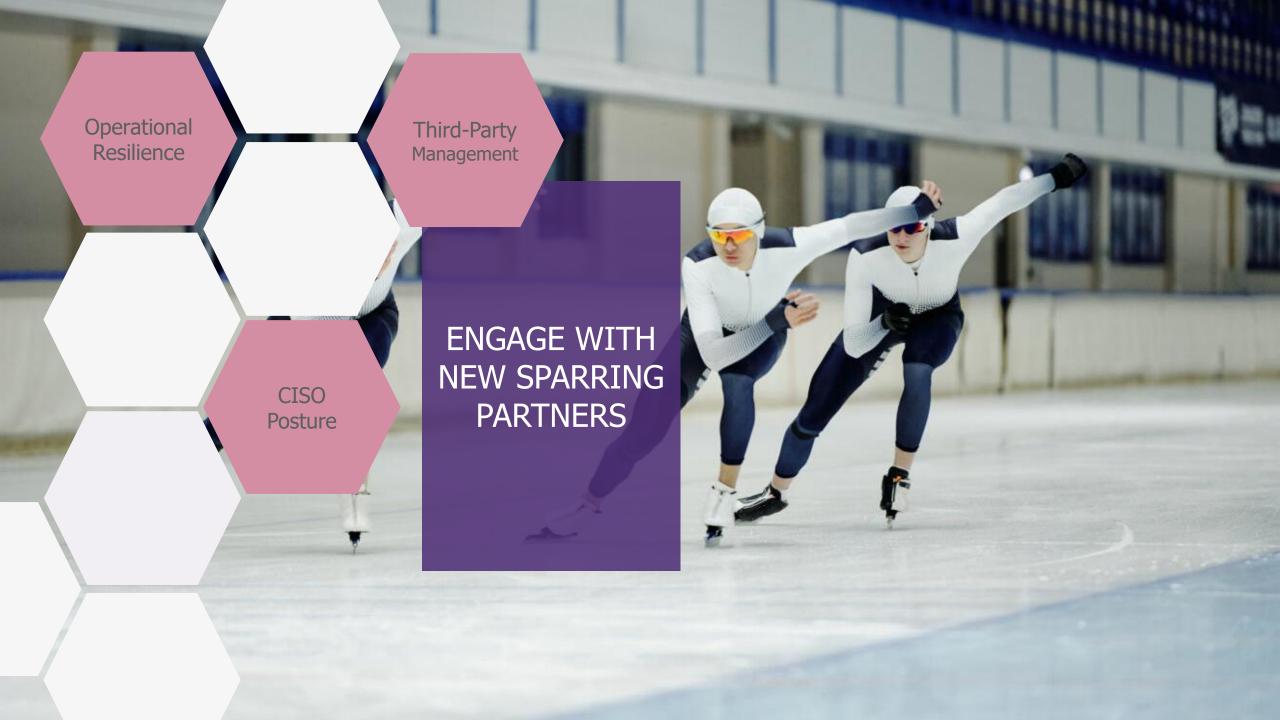
**Collaborate** with them to develop *tailored messages & solutions* for each audience

**Be creative** with the *actions* in the program & prioritise **guilt-free** approaches

**Measure the** *program's impact* on behaviour, **highlight** *best practices* to empower employees and **share your** *successes* with your clients

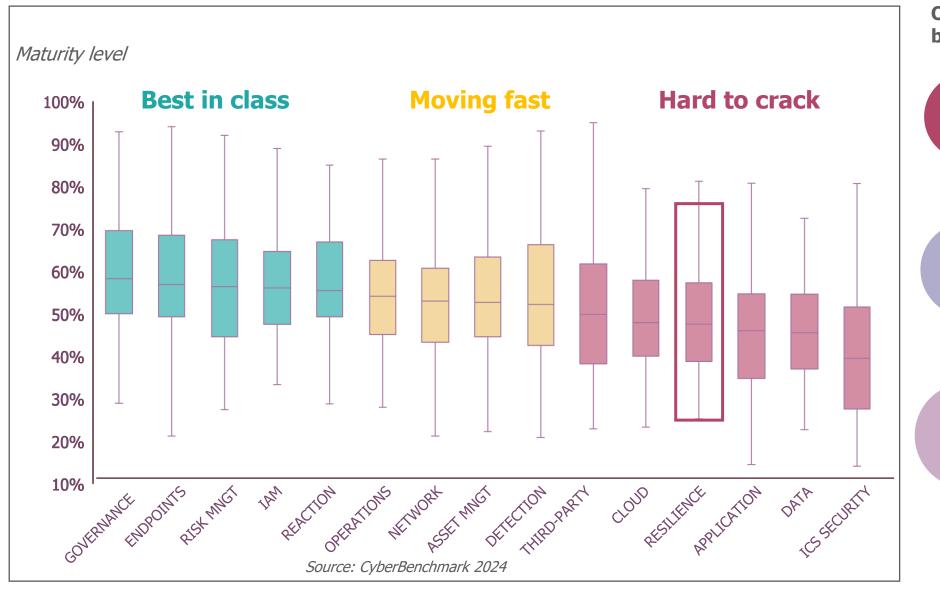


Source: Wavestone TAMAM framework



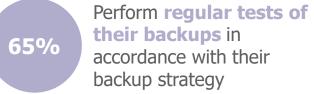
## Operational Resilience

Despite **regulation-driven investments** and substantial infrastructure efforts, the overall **maturity level is increasing** but **key challenges remain** 



#### Of the organisations in our benchmark:







#### Operational Resilience

Onboard business to ensure the resilience of your Minimum Viable Company

**Identify** your *minimum viable company* 

Approx. 10 to 15% of business chains

**Define** impact *tolerance* with the business

Using empirical data on the impact over time

"We must settle 80% of payments intraday"

"We must deliver our product to all vulnerable customers intraday and within 3 days for non-vulnerable ones"

Map value chains and underlying assets

IT, third-parties, users and admins

**Identify** and assess your "red-zone" scenarios

Ransomware, third-party outage, fraud...

The control action plan - along with its testing plan - will bring together cyber, IT and Business actions

Part of attack techniques that can be detected and/or mitigated

Recover

Time required to rebuild key assets

Part of business activities that Vaintain are operational during attack

## **Third party**

## empower

#### On all fronts



**Empower**: create a third-party evaluation platform **accessible to everyone** in the company and promote it internally

(and if you can, build a dedicated team to track your third parties!)



Learn how to manage a **crisis with your third parties** 



Contribute to ecosystem resilience

Identify non-substitutable third-party providers and set-up industry groups to work on resilience strategies and influence regulators

#### The CISO needs to embrace a larger scale perspective

Extending scope of responsibility

**Increased Accountability** 

Managerial & technological expectations

## CISO is dead, long live to...

#### The CSO in Finance

Expand your responsibilities to other teams (antifraud, physical security, resilience...) to ensure **improved coverage of the risks** 

Make it concrete with a Fusion Center



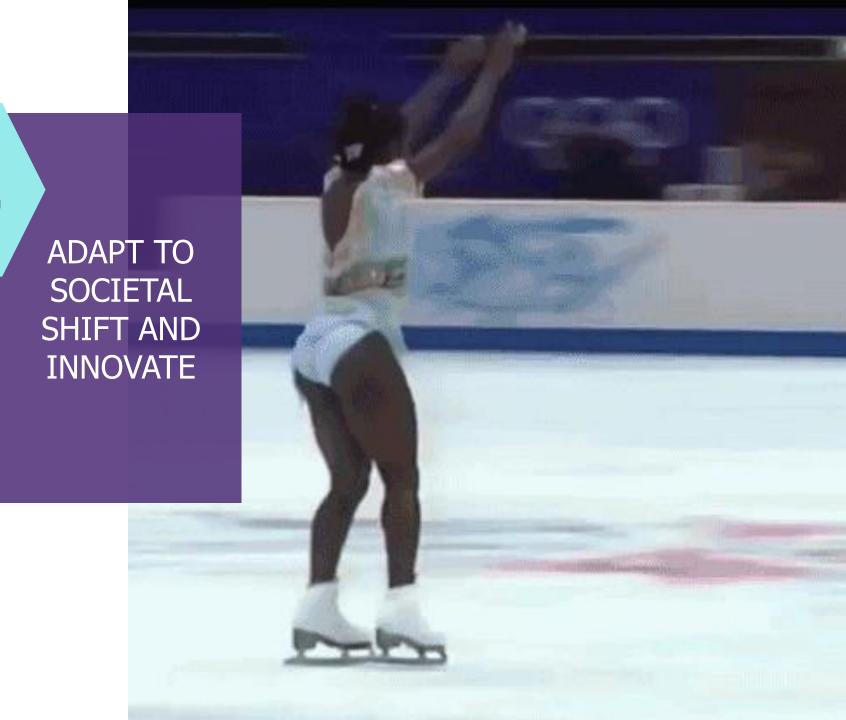


#### A broader CISO in Industry

Bring industrial & product security under one roof to optimize security level and increase trust for your clients

Get ready for the **compliance boom** (Cyber Resilience Act, White House Cyber Trust Mark)

Leverage the organization to make cybersecurity a **market differentiator** 



Next Gen encryption and quantum computing

ΑI

Decoupling

#### Start with **Securing A.I.**

#### ... don't rush on AI for cyber

Deploy safe-by-design A.I.

Develop a method to promptly classify AI-leveraging initiatives, prioritising high-risk projects

- / Define **governance and framework** against existing standards and **future regulations** (AI Act, NIST AI framework)
- Deploy risk analyses, training and awareness tailored to the specific risks and countermeasures

Plan for AI specific audit

AI-tailored red teaming: model stealing, poisoning, oracle, illusion attacks

AI has not proven to be a game changer for cyber yet

Start by building a security data hub to prepare for what's to come

#### **Next-Gen encryption & quantum computing**

a revolution underway for pioneers

Meet with providers to identify new solutions to **unlock new usages**:

- / Confidential computing (encrypted memory, encrypted processor register...)
- / Homomorphic encryption (use data without decryption)

**Opportunities** 

Threat

Quantum computing – by 2030/33

Launch project to update encryption mechanisms (3-5 years):

- / **Identify sensitive data**, required encryption periods and the systems managing this data
- / **Identify responsible for encryption** (provider, internal development, open source)
- / Deploy post-quantum encryption engines and adapt encryption key storage infrastructure

# If you are a multinational company exposed to

Geopolitical tensions

Regulations leading to digital fragmentation

# ...anticipate DECOUPLING

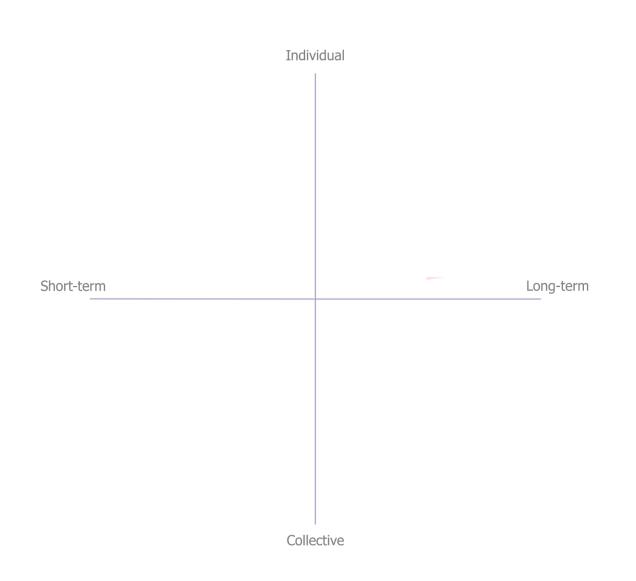
#### **Prepare for a rapid response**

- / Identify your critical geographies
- / Establish a "red-button" process: primarily for network and IAM/PAM
- / Review your crisis management procedures / What are the impacts of isolation?

#### Reinvent your cybersecurity architecture

- / Build a ready-to-isolate AD architecture
- / Introduce an additional security layer between countries as necessary
- / Review your vendors' contracts and assess trustworthiness

#### Talent management is a market-level issue



#### **Overall maturity score**



# Focus on what you have before looking elsewhere

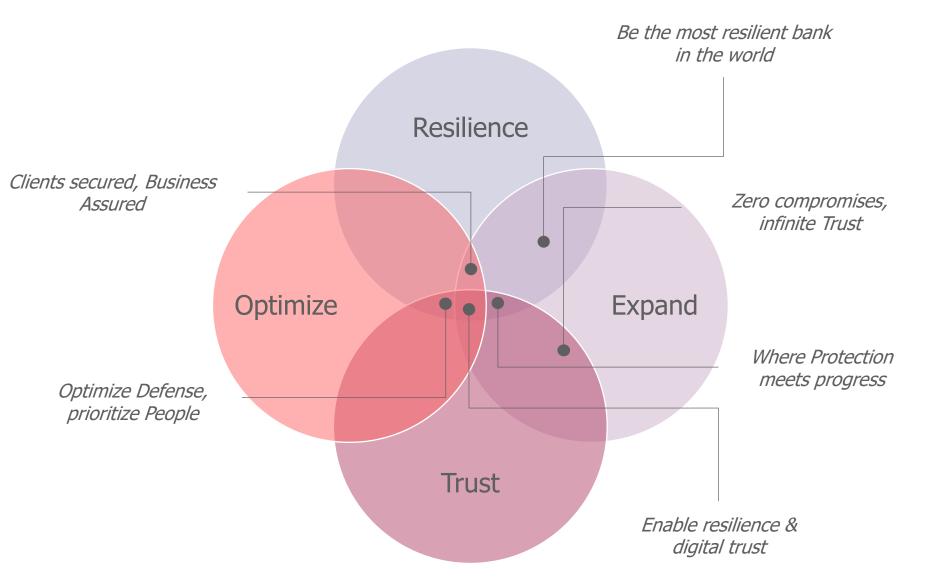
- >> Increase attractiveness internally and promote mobility
- >> Work on nurturing talent retention







## Market your strategy: chose your key message and your posture





## Any questions?



Gérôme BILLOIS
Partner
gerome.billois@wavestone.com



Matthieu GARIN Partner matthieu.garin@wavestone.com

contact@wavestone.com