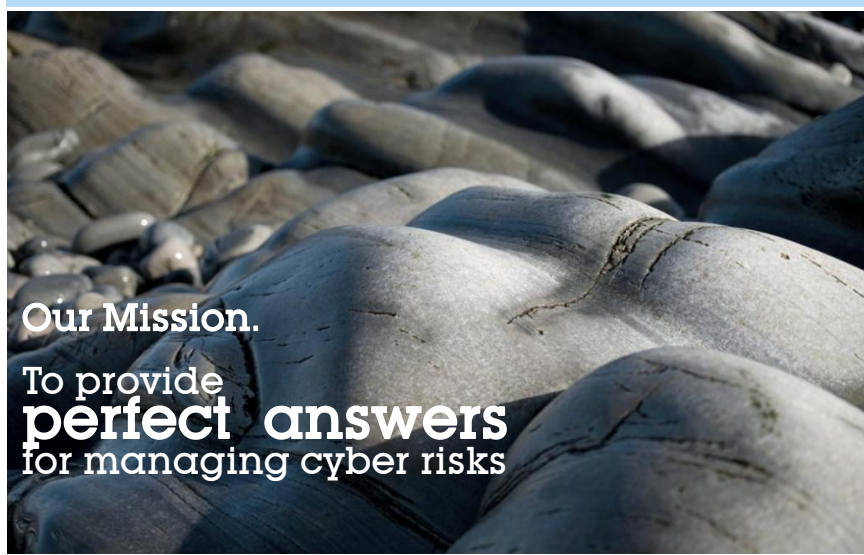


STONESOFT

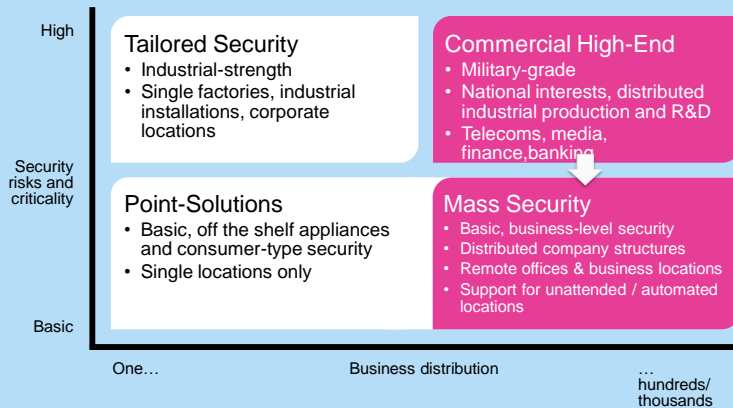


Our Mission.

To provide
perfect answers
for managing cyber risks

STONEISOFT

More complexity and security -
more value we can bring in.



STONEISOFT

We are securing



Data centers



Mission Critical Networks



Sensitive Data



Connectivity



Business systems

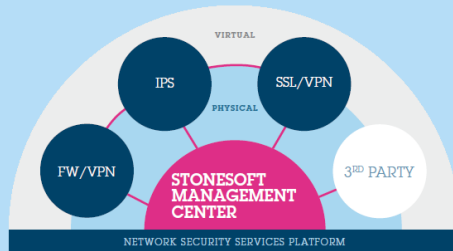


Financial transactions

STONESOFT

Product Scope

Network Security Services Platform



- Antievasion ready
- Context and situation aware
- Adaptive to physical, virtual and hybrid
- Dynamic
- Easy to manage

Stay connected and secured in a dynamic world.

Now and in the future.

STONESOFT

10 Perfect Answers to Next Generation Security Needs...

- Can Stonesoft offer **Software** based and **dynamic protection**?
- Has Stonesoft experience and knowledge to protect against **advanced threats and hacking methods**?
- Is Stonesoft **adaptive** to virtual, physical and/or hybrid environments?
- Can Stonesoft provide **intelligent and context aware security**?
- Can Stonesoft offer better **real-time situational awareness** and visibility "across everything"?
- Is Stonesoft technology based on a **single software and platform design**?
- Can Stonesoft help to minimize **human errors**?
- Can Stonesoft **simplify security management and operations**?
- Is Stonesoft **easy to manage** and is the usability high?
- Is Stonesoft **inexpensive to buy, operate and own**?

YES!

YES!

YES!

YES!

YES!

YES!

YES!

YES!

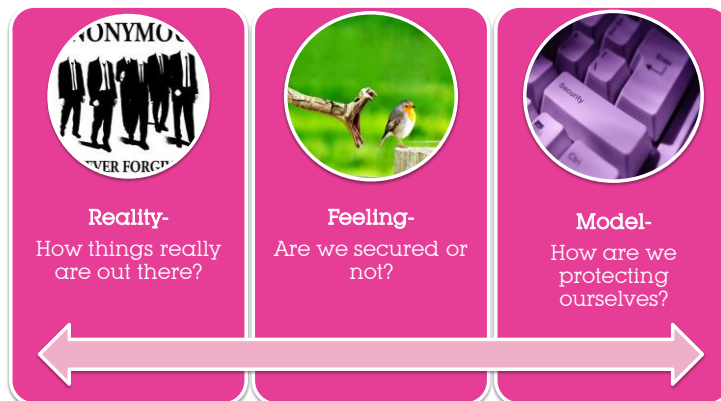
YES!

YES!

STONESOFT

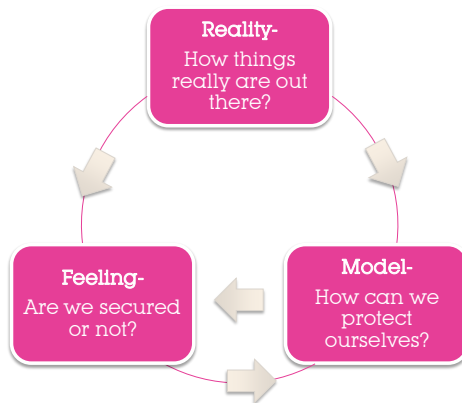



Security Trinity. It is a combination of...



STONESOFT

Dynamics of Security



Some reality checks:

- Feelings and model must be grounded in **reality** – NEVER the other way around.
- Changing a model or feeling never changes the **reality**.
- Marketing can make you **feel secure**, but the reality can be different
- We always need to ask if the link between **Reality=Facts=Research** has changed and act on that.

STONESOFT

Reality has Changed

- Hacktivism increasing
- Nationalization of Cyber Crime
- Industrialization of Hacking
- Advanced attacks and persistent threats
- Advanced Evasion Techniques

At the same time...

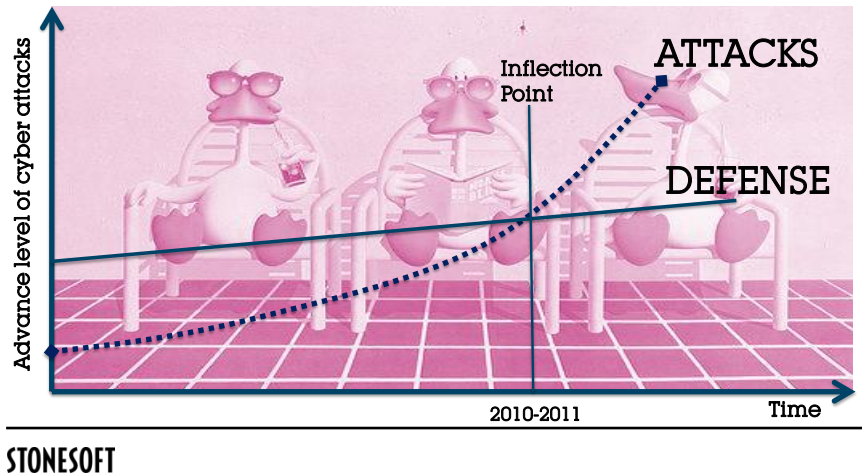
- Business is more dependent on IT and networks
- Information and money are digital
- Diversity and complexity of IT increases
- IP connectivity increases
- Mobilization
- Consumerization

Unpleasant thruth:

Internet is broken but we need it more and more.

STONESOFT

Sorry to say...Established Secure Brands are Sitting Ducks?



TRUE STORY - 100% MADE IN FINLAND

DISCOVERY

- **Stonesoft** security researchers in the outskirts of Europe discovered that there are **millions and millions of ways** to bypass **the most advanced and leading network security solutions** without leaving any traces or alerts on control or management systems.
- Being a good citizen Stonesoft has reported in public only 410 out of those millions and millions.
- But you can "do the math" yourself

Those ways are called:

**ADVANCED
EVASION
TECHNIQUES**

www.antievastion.com

STONESOFT

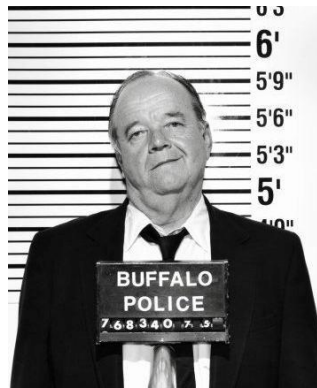
Advanced Evasion Techniques disguise and make cyber attacks /malicious payloads/ exploits look normal and safe when the security device inspects the data traffic. The number of AETs can be virtually limitless as you can combine, vary and modify them dynamically.



**Because of the fundamental design flaws
current security devices can see only this much today..**

STONESOFT

...as they should see this much!



STONESOFT

Why worry?

- AETs can breach sensitive data (data centers, IPR)
- AETs can ruin brand reputation (customer trust)
- AETs can cause financial losses (online banking and financial transactions)
- AETs can exploit industrial systems and services (SCADA networks)
- AETs can stop and harm business operations (ERP, SAP systems)
- AETs can risk critical infrastructure (Communications, electricity)
- AETs can risk national security (governmental sector, military)

Currently AETs
work as a
Master Key that
security
vendors **SIMPLY**
DO NOT HAVE.



STONESOFT



Déjà vu

Automobile safety in 1959	Network security in 2010?
Status Quo: Before 1959 all the established automobile brands marketed that cars were safe and users believed and felt safe.	Before 2010 all the Network Security vendors marketed that their solutions offered high level of protection and organizations felt their digital assets were secured.
Disruption: Then came one Nordic brand, VOLVO, who claimed that current cars are not even close to being safe and innovations are needed.	Then came one Nordic brand, STONESOFT, who claimed that the current security solutions are not as secure as they should be. (Disruption)
Technology breakthrough: In 1959, they introduced Three Point Seat Belts.	Technology breakthrough: 2010 They introduced Advanced Evasion Techniques and innovative technologies to fight back.
Claim: They claimed lives can be saved if all brands would start adding Seat Belts to their cars. (Tested facts and reality)	Claim: They claimed governments, businesses and brands can be saved if their anti-evasion technologies are taken into use.
Industry Response: "This is marketing, extra costs, no relevance to safety, dangerous, uncomfortable, people won't use, theoretical only.	Industry Response: "Most kept silent and others claimed "This is marketing, we can fix this, only extra costs, no relevance to security, unproven, theoretical, not happening in reality."
Bottom Line: Millions of human lives have been and will be saved.	Bottom Line: Organizations will be saved if AET threat is taken seriously

STONESOFT



STONESOFT

For the record...



"Advanced Evasion Techniques can evade many network security systems. We were able to validate Stonesoft's research and believe that these Advanced Evasion Techniques can result in lost corporate assets with potentially serious consequences for breached organizations."

– Jack Walsh, Program Manager



"If the network security system misses any type of evasion it means a hacker can use an entire class of exploits to circumvent security products, rendering them virtually useless. Advanced Evasion Techniques increase the potential of evasion success against the IPS, which creates a serious concern for today's networks."

– Rick Moy, President



"Recent research indicates that Advanced Evasion Techniques are a real and credible – not to mention growing – and growing threat against the network security infrastructure that protects governments, commerce and information-sharing worldwide. Network security vendors need to devote the research and resources to finding a solution."

– Bob Walder, Research Director



We believe AETs pose a serious threat to network security and have already seen evidence of hackers using them in the wild. It is also promising to see that Stonesoft is taking the threat posed by evasion seriously as they have been overlooked by many in the past

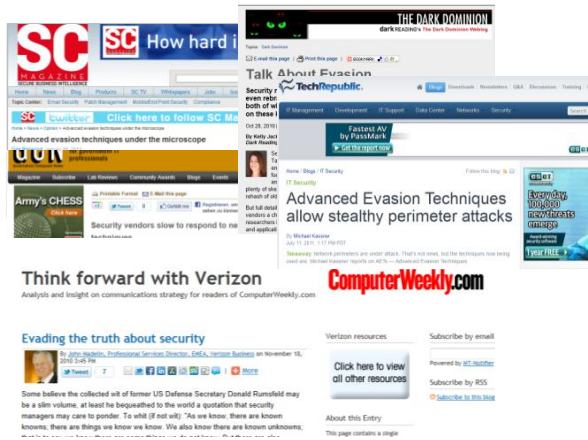
– Andrew Blyth, Professor of Glamorgan University

Meanwhile,
other
security
vendors
keep radio
silence.



STONESOFT

For the record...



Meanwhile,
other
security
vendors
keep radio
silence.



STONESOFT

Off the Record

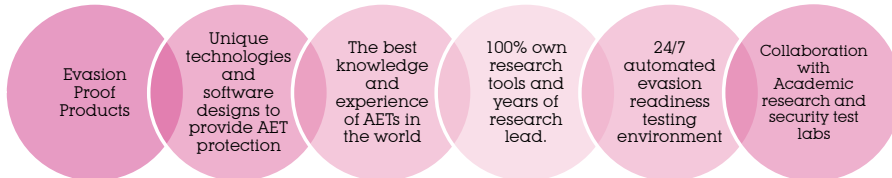
- Some are acquiring anti-evasion technology and knowledge from Stonesoft
- All are focusing on surviving next public tests
- Some are doing workarounds and quick fixes
- All are downplaying the threat and risks - if they are asked
- All are protecting their business at the expense of customers
- Some have truly started to investigate their design flaws
- Some ignore and do NOTHING!

Meanwhile,
other
security
vendors are
saving their
business.



STONESOFT

Good to Know that Stonesoft Has...



STONESOFT

WHERE IS THE BUSINESS BEEF?

AET Impact on Stonesoft Business

- Stonesoft is shortlisted more often when Next Generation Security is chosen
- Interest towards Stonesoft's Antievasion technology
- Improved brand recognition and thought leader position
- New collaboration opportunities
- Better access to power
- Better and easier business for partners

Bottom Line:

"Stonesoft threat research last year concerning evasions has increased security credibility and visibility for the company"

Gartner Quote

STONESOFT

