

Attack Yourself - mit Breach and Attack Simulation



Halle 7A 7A-318

What Are Your Biggest Risks?

Misconfiguration

With dozens of products, you must be 100% right, 100% of the time



Evolving Threats

Attack surface is getting bigger (Mobile, IoT), Attackers are evolving



Point Solutions

Complex security architectures due to a sprawl of point solutions



RISK

Alert Overload

Too many SIEM alerts to possibly process them all



Ransomware

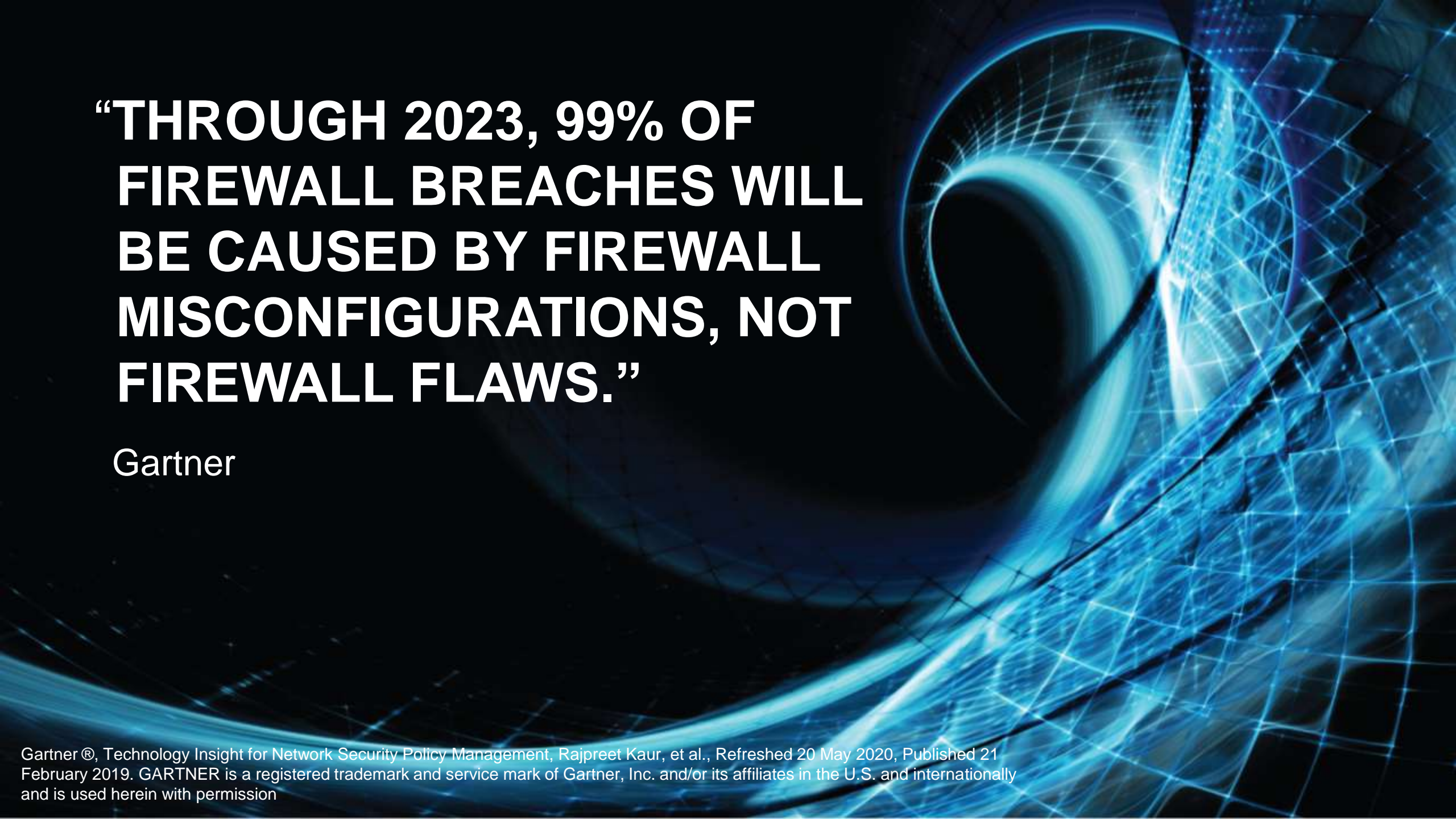
Downtime, lost production, theft and loss of IP



Limited Resources

Security staff are too valuable to waste time on tasks that could otherwise be automated





**“THROUGH 2023, 99% OF
FIREWALL BREACHES WILL
BE CAUSED BY FIREWALL
MISCONFIGURATIONS, NOT
FIREWALL FLAWS.”**

Gartner

Next-Gen Networks Demand Next-Gen Security

There is no magic bullet, otherwise you'd already have it



MEASURE

- Measure the efficacy of your security posture
- Identify vulnerable security gaps and misconfigurations
- Show how secure you are and justify tool investments



OPTIMIZE

- Prioritize fixes with product-specific remediations
- Maintain optimal security posture with proactive action
- Harden defenses against high-risk threats and attacks



MONITOR

- Test for vulnerabilities on a continuous basis
- Identify environmental drift before you get attacked
- Stay ahead of new / emerging TTPs and attacks

You need to know that your **network, data, and critical infrastructure** are safe.

But how can you be sure **security is moving at the pace** of your business?

Keysight Threat Simulator

Accelerate Your Defenses With Keysight



Test Your Network Defenses

Network, email,
endpoint assessments

20,000+ TTPs
supported, including
lateral movement and
MITRE ATT&CK



Maximize Your Security Stack

Detect and remediate
configuration drift

Save money by
optimizing existing
security controls /
processes before
purchasing new tools



Find & Fix Vulnerable Gaps

Product-specific
remediations

Insights to optimize
security posture

Priority Threat
Mitigations reduce risk



Improve Detection & SIEM Rules

Be confident in policies
working as expected,
even after changes

Protect all digital assets
in one place (email,
WAF, DLP, NGFW, etc.)

A Turnkey Solution

Get Up And Running Quickly

Save Precious Time

- Ready to go out of the box
- No lengthy spin-up or configuration

Set It And Forget It

- Auto-updating, cloud-based SaaS
- Easy to create, schedule assessments
- API integration with SIEMs

Stay Safe

- No attacks or malware ever hit real servers or endpoints on live network
- Dark Cloud-based agents ensure safety by only communicating with each other



Threat Intelligence

Trusted Around the World

Trusted Library Of Attacks

- 7000+ live security attacks, 41000+ malware techniques, 100+ evasions
- DDoS, botnet, APT simulations

Leading Source Of Known Threats

- Curated set of proprietary, opensource, commercial datasets
- Billions of IPs, URLs
- Millions of SPAM records

Our Work Is Never Finished

- Continuously updated, global network of honeypots, web crawlers, security research labs



Priority Threat Mitigations

Stay Ahead of Imminent Risks

Don't Wait For Attackers

- Breaking updates on high-risk attacks from ATI Research Center
- Comprehensive assessments included, conduct within minutes

Make Sure You're Protected

- Proactively harden network, endpoints, email against emerging threats
- Product-specific remediations make it easy to close gaps



Call To Action

Attack Yourself!

- **Attack & Audit yourself before others do**
- Halle 7A Stand 7A-318
- Register for Free trial

