

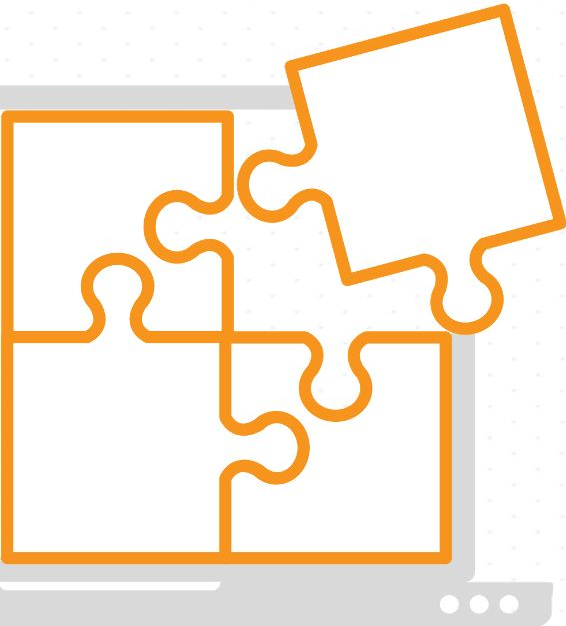


OPKALLA
IT SOLUTIONS REIMAGINED

Going *Beyond* the CISO

Lessons all C-Staff Need to Know about Security

Industry Challenges



IT is more important to the business today than ever before. With that comes new challenges and pressures on IT departments to drive innovation while still maintaining day-to-day operations.

Obstacles You Face:

- Operating in a lean IT environment
- Constant vendor/technology evaluations
- Navigating biased agendas
- Not enough time

Too much to tackle on your own.

Why Opkalla

	CONSULTANTS	MSPs	VARs	OPKALLA
Broad Technical Expertise	✗	✓	✓	✓
Vendor-Agnostic	✓	✗	✓	✓
Ongoing Engagement	✗	✓	✓	✓
Collaborative	✗	✗	✗	✓

Opkalla exists to challenge the legacy trend of partners representing a solution instead of representing the client. We work **alongside** IT teams to design, procure, implement and support the most innovative solutions without an agenda or technology bias. We strive to be your **Trusted Advisor**.



Partnering With Opkalla

1. Assessment

2. Analysis

3. Evaluation

4. Insights

5. Decision

Using the **Opkalla Methodology** we enable clients to quickly achieve their business objectives through our innovative portfolio of solutions and services.

Your best interest is always our focus, as we're guided by our core values – **trust, transparency, being agnostic, convenience and speed.**



21% Average Saved
Per Client on Annual
Contracts



**2,500+ Evaluations
Completed**
Since Our 2019 Inception



20+ Years of Experience
As IT Consultants



250+ Happy Clients
With Successful IT
Implementations



OPKALLA
IT SOLUTIONS REIMAGINED

Where can we engage?



Cloud Contact Center



Public Cloud Solutions



Disaster Recovery + Backup



Microsoft 365 for Business



Infrastructure



Unified Communication



Cybersecurity



Colocation



Mobility



Connectivity



SD-WAN



Virtual Desktops



OPKALLA
IT SOLUTIONS REIMAGINED



OPKALLA
IT SOLUTIONS REIMAGINED

Going *Beyond* the CISO

Lessons all C-Staff Need to Know about Security

George Just
CRO





The infographic features a central white rounded rectangle with a large grey arrow pointing towards it from the top and bottom. Surrounding this central element are ten white rounded rectangles, each containing the name of a cyber attack. These are connected to the central area by dashed lines of varying colors (teal, grey, yellow, red, blue). The attacks listed are: DoS Attack, Ransomware, Phishing, DNS attack, SQL Injection, log4j, Man in the Middle, Compromised Machine, Spear Phishing, and Malware.

Cyber attacks remain #1 global threat to organizations

DoS Attack

Ransomware

SQL Injection

DNS attack

Phishing

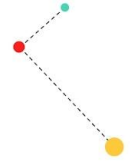
log4j

Man in the Middle

Compromised Machine

Spear Phishing

Malware



Every 11 seconds

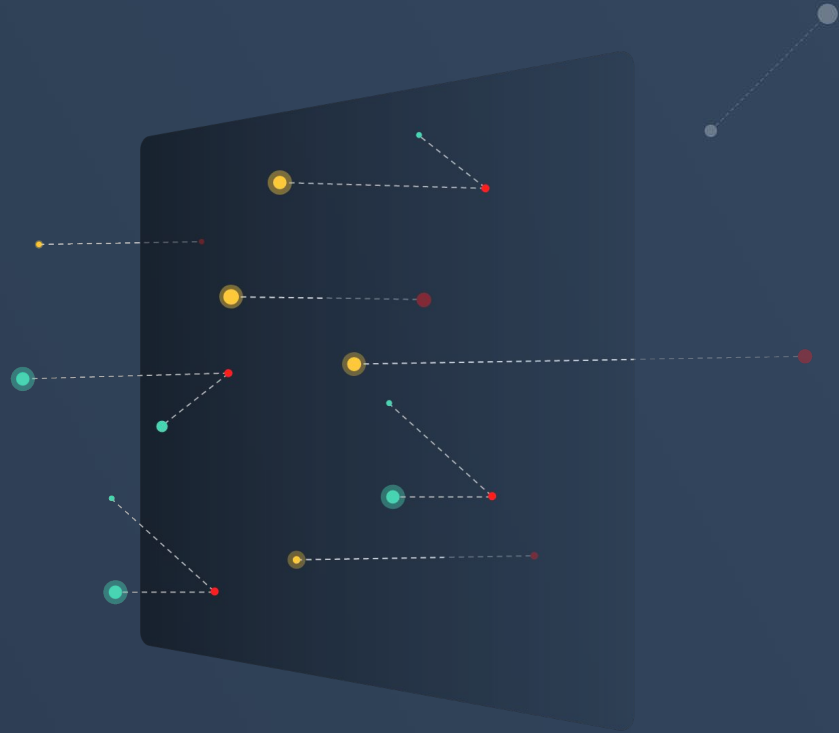
a business is **breached** by a ransomware attack that has **passed through** the security stack.



Existing security controls and tools do provide coverage, but **most are reactive**

Threat actors are still finding ways to slip through the cracks and penetrate your network.

Once they're in, they're in.

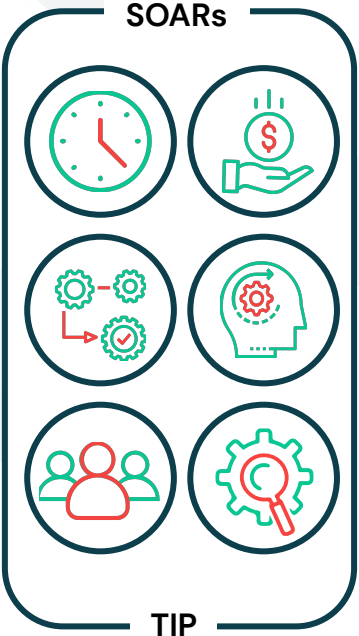


The current model for consuming cyber intelligence is too complex, expensive and most importantly ineffective

Multitude of data feeds, millions of threats



Need Resources (time, money, systems, skill, staff, etc.) to Manage & Optimize Feeds



Difficult to incorporate external feeds into NGFWs



Can only block hundreds of thousands of indicators (not hundreds of millions), blocking can cause latency



Gaps in Cyber Protection





NGFWs don't play nicely with threat intelligence

1

Total indicator capacity limits

2

List size limits (#, size, etc.)

3

Limited integration options

Taking Action with Threat Intel Remains a Key Challenge

- Lack of action remains a key reason why threat intel programs struggle.
- Putting threat intel into action is manual, repetitive, and cumbersome.
- Scalable enforcement is one of the missing pieces of an incomplete threat intel management puzzle.

The Conversations All C-Staff Need to Be Having

1

I know where my vulnerable networks areas are and how my security stack fills those gaps.

2

All successful cyber attacks have breached a firewall. I know they are not a one-stop-shop against threats.

3

I have access to readily available threat intel that instantly updates and protects my network

The Conversations All C-Staff Need to Be Having

4

I'm aware of cyber attacks within my industry that affect my partners and competitors. These are not siloed attacks – so I could be next.

5

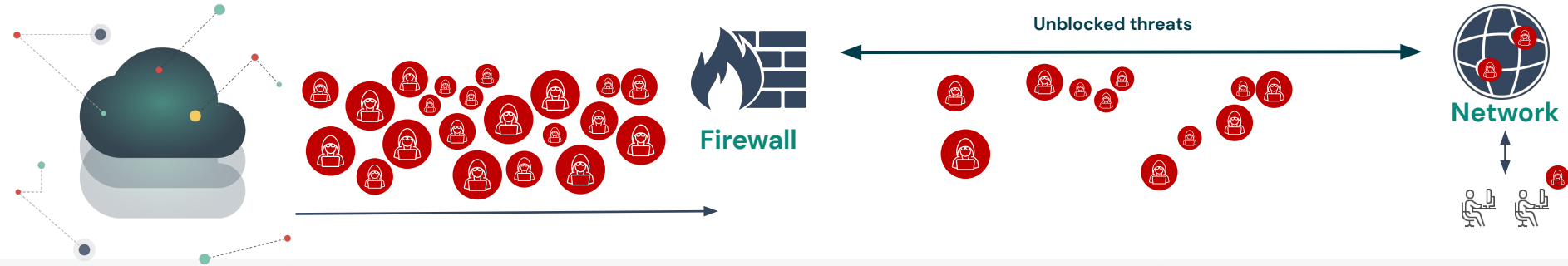
Recent SEC ruling indicated that this is a responsible and could eventually be a punishable act against board members & executives who refuse to take action.

6

The current war abroad has driven awareness towards state sponsored action hitting the private industry – something that hasn't been a priority before.

ThreatBlockr blocks what your security stack cannot

Existing security stack leaves your network vulnerable



ThreatBlockr blocks every threat ... inbound and outbound

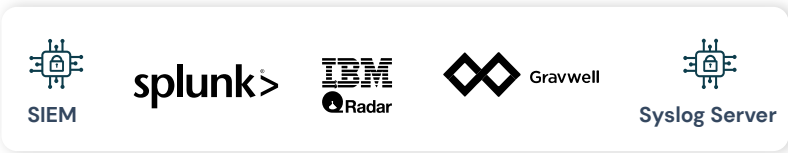


An Active Defense Strategy

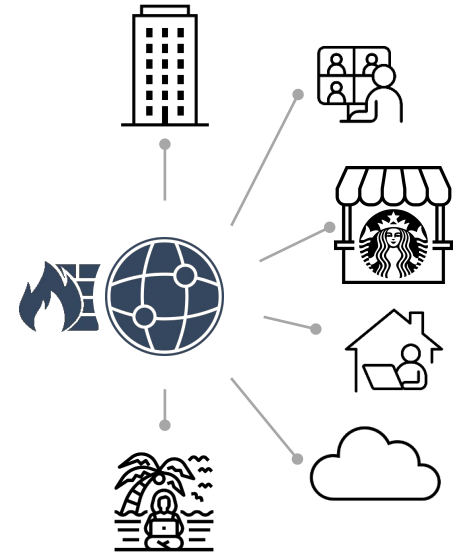
Cyber Intelligence



Access to tens of millions of cyber intelligence indicators



Your Network



THREATBLOCKER

Security blocking and tackling. Automated.

ThreatBlockr + Opkalla



Aggregates



Policies



Curates



Deploys



Updates



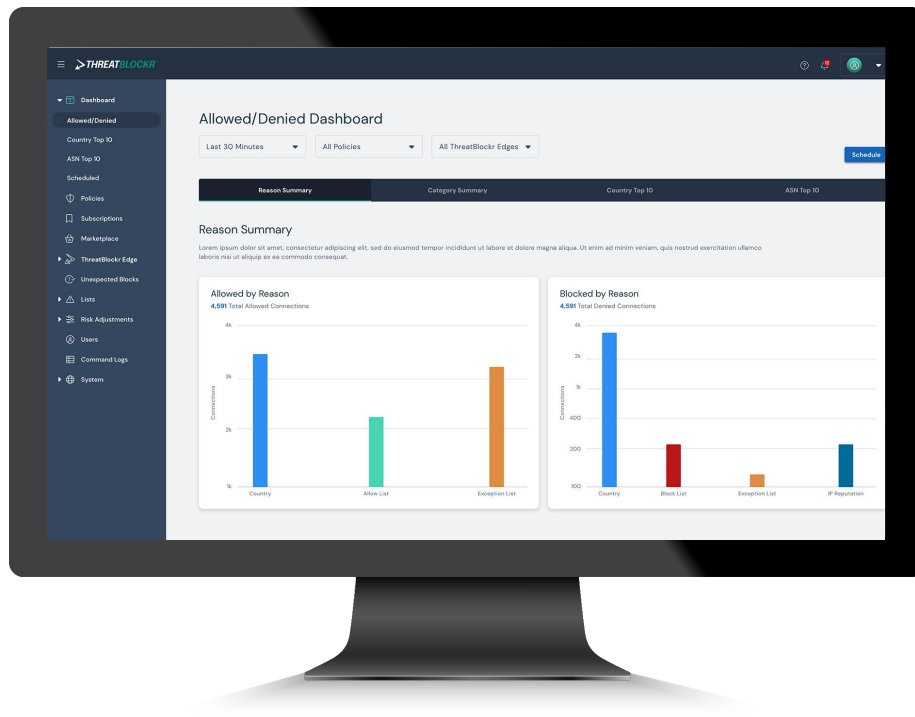
Dashboards & Reports



Blocks



Enforces



With ThreatBlockr, you will:

1

Seamlessly integrate into and enhance your existing security stack enabling an **ideal protected network**

2

Protect your network with **millions of indicators** from over 50 world class sources
- **updated in real time**

3

Mitigate false positives quickly and intuitively using **automation** saving time and resources

An active defense that
blocks every threat
in real time

Filter the noise to **focus on the meaningful**

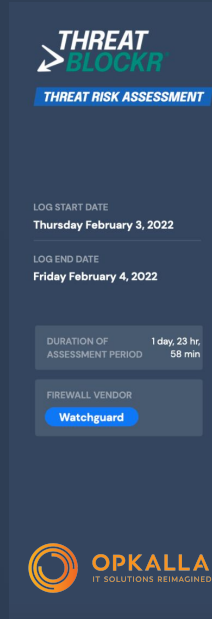
Q & A

Any Questions?

Not Sure Where to Start?

Threat Risk Assessment

Let's do a rapid analysis of your security logs to see how ThreatBlockr would have blocked threats that your security stack missed.



THREAT BLOCKER
THREAT RISK ASSESSMENT

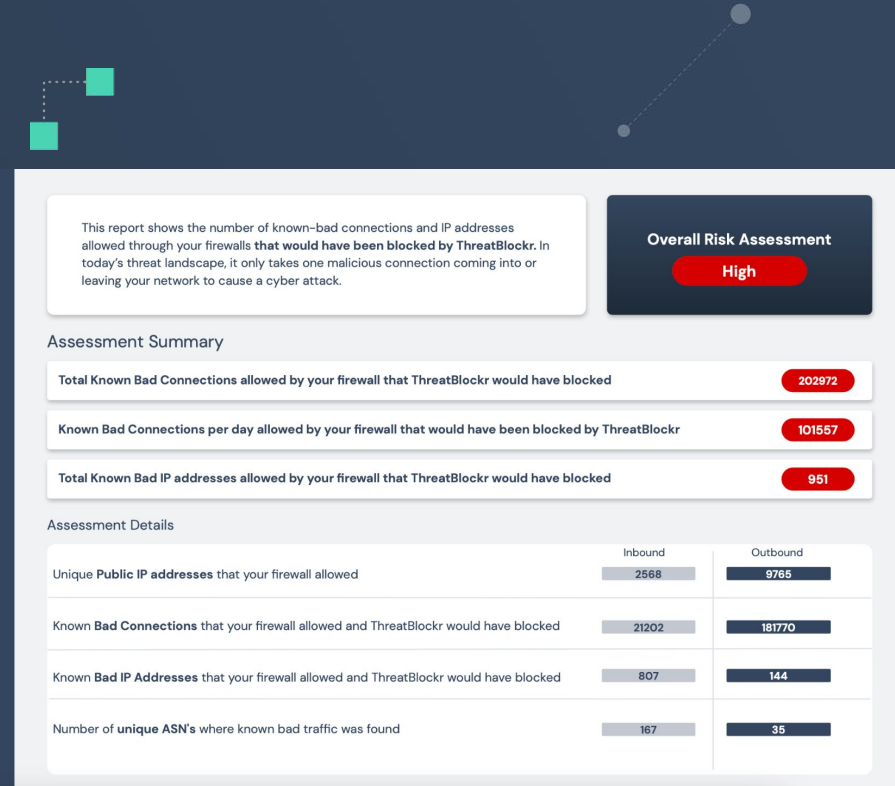
LOG START DATE
Thursday February 3, 2022

LOG END DATE
Friday February 4, 2022

DURATION OF ASSESSMENT PERIOD
1 day, 23 hr, 58 min

FIREWALL VENDOR
Watchguard

OPKALLA
IT SOLUTIONS REIMAGINED



This report shows the number of known-bad connections and IP addresses allowed through your firewalls **that would have been blocked by ThreatBlockr**. In today's threat landscape, it only takes one malicious connection coming into or leaving your network to cause a cyber attack.

Overall Risk Assessment
High

Assessment Summary

- Total Known Bad Connections allowed by your firewall that ThreatBlockr would have blocked: **202972**
- Known Bad Connections per day allowed by your firewall that would have been blocked by ThreatBlockr: **101557**
- Total Known Bad IP addresses allowed by your firewall that ThreatBlockr would have blocked: **951**

Assessment Details

	Inbound	Outbound
Unique Public IP addresses that your firewall allowed	2568	9765
Known Bad Connections that your firewall allowed and ThreatBlockr would have blocked	21202	181770
Known Bad IP Addresses that your firewall allowed and ThreatBlockr would have blocked	807	144
Number of unique ASN's where known bad traffic was found	167	35