

# Why Network Security Is Still Important in the Cloud Age



**Marc Laliberte**

Director of Security Operations

**Real Security**  
for the **Real World**

# Who Am I?



## Marc Laliberte

Director of Security Operations

*LinkedIn: /in/marc-laliberte/*

*BlueSky: @itsmarc.me*

- 14 years at WatchGuard
- Leader @ WatchGuard of:
  - Security Operations
  - Threat Research
  - Product Security

**How many of you rely on cloud services like  
Microsoft 365, Salesforce, or Azure?**

**Keep your hand up if you no longer have an office or home network.**

# MGM Resorts breached by 'Scattered Spider' hackers: sources

By Zeba Siddiqui and Christopher Bing

September 14, 2023 1:13 AM GMT+2 · Updated September 14, 2023



# Most Cloud Breaches Aren't Cloud Breaches

# ShinyHunters, Lapsus\$ & Scattered Spider

Live Nation / Ticketmaster 560M Users + Card Details 1.3TB  
by ShinyHunters - Tuesday May 28, 2024 at 06:02 PM

[Owner] ShinyHunters



Bossman

ADMINISTRATOR

Posts: 31  
Threads: 7  
Joined: May 2023  
Reputation: 1,187

05-28-2024, 06:02 PM

#1

Live Nation / TicketMaster

### Data includes

560 million customers full details (name, address, email, phone)  
Ticket sales, event information, order details.  
CC detail - customer, last 4 of card, expiration date.  
customer fraud details  
much more

Price is \$500k USD. One time sale.

### Folder / Table Size

Folder size

390G	./processed
149G	./csv
47G	./sales_ord_deluxe_hdr/3
49G	./sales_ord_deluxe_hdr/7
48G	./sales_ord_deluxe_hdr/4
44G	./sales_ord_deluxe_hdr/5
43G	./sales_ord_deluxe_hdr/8
47G	./sales_ord_deluxe_hdr/2
46G	./sales_ord_deluxe_hdr/9



Call IT helpdesk to reset MFA tokens



Convince SaaS admins to install malicious plugins



Phishing links to steal SSO credentials and MFA codes

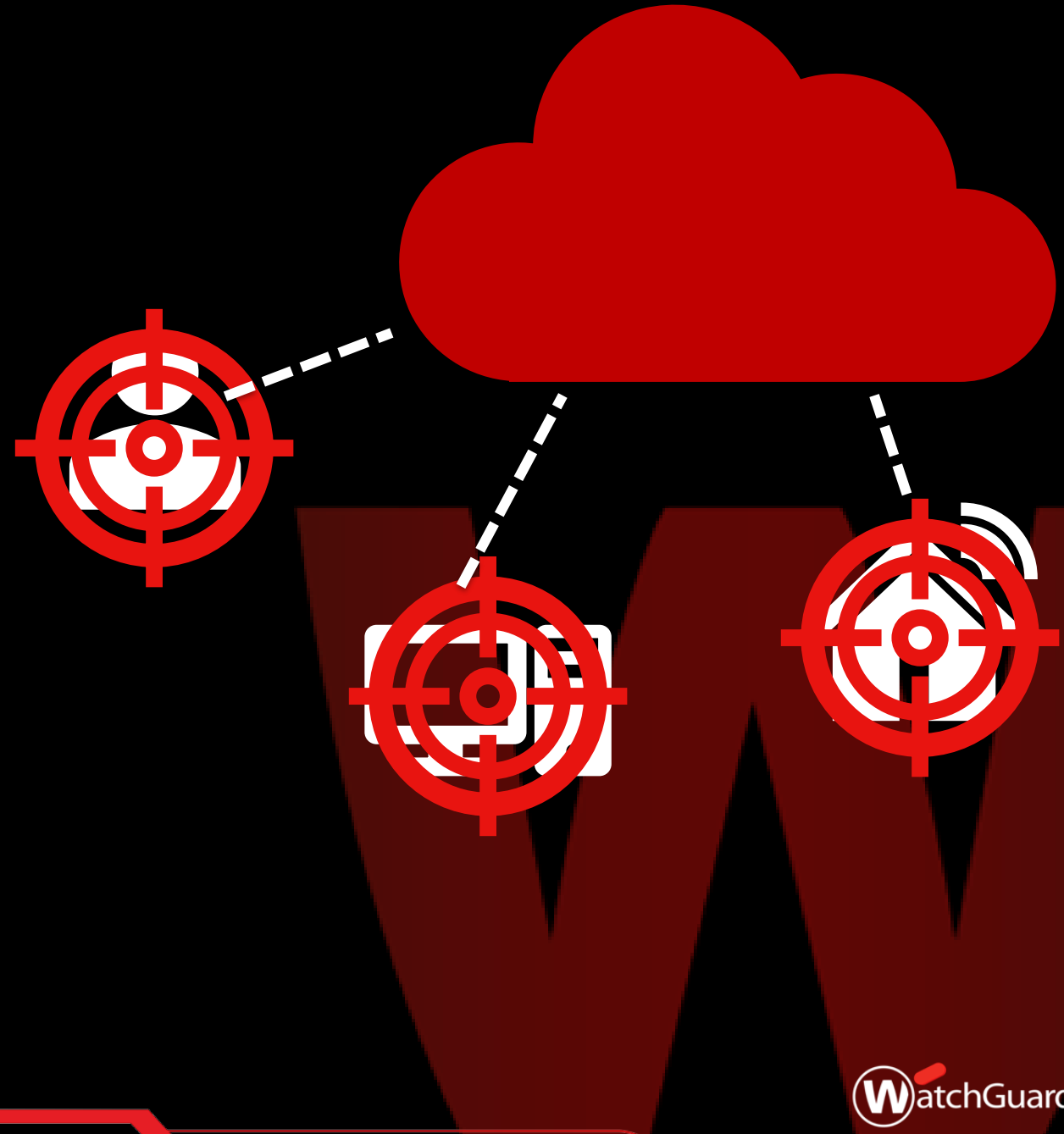
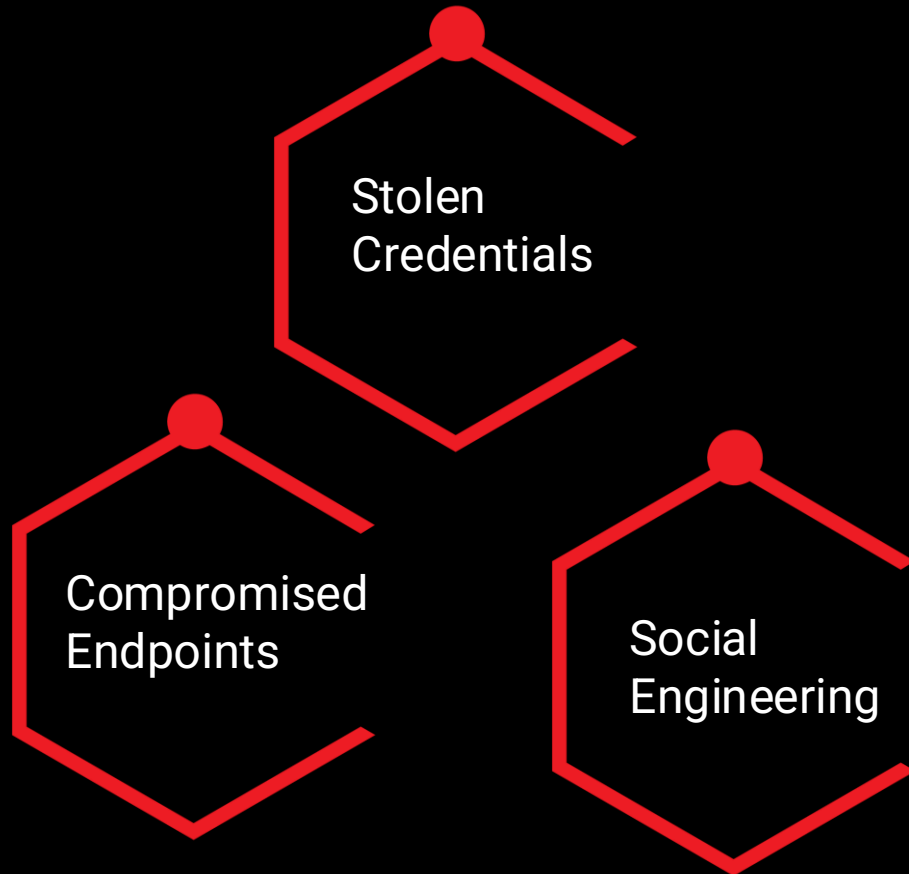


Compromise VPN credentials without MFA

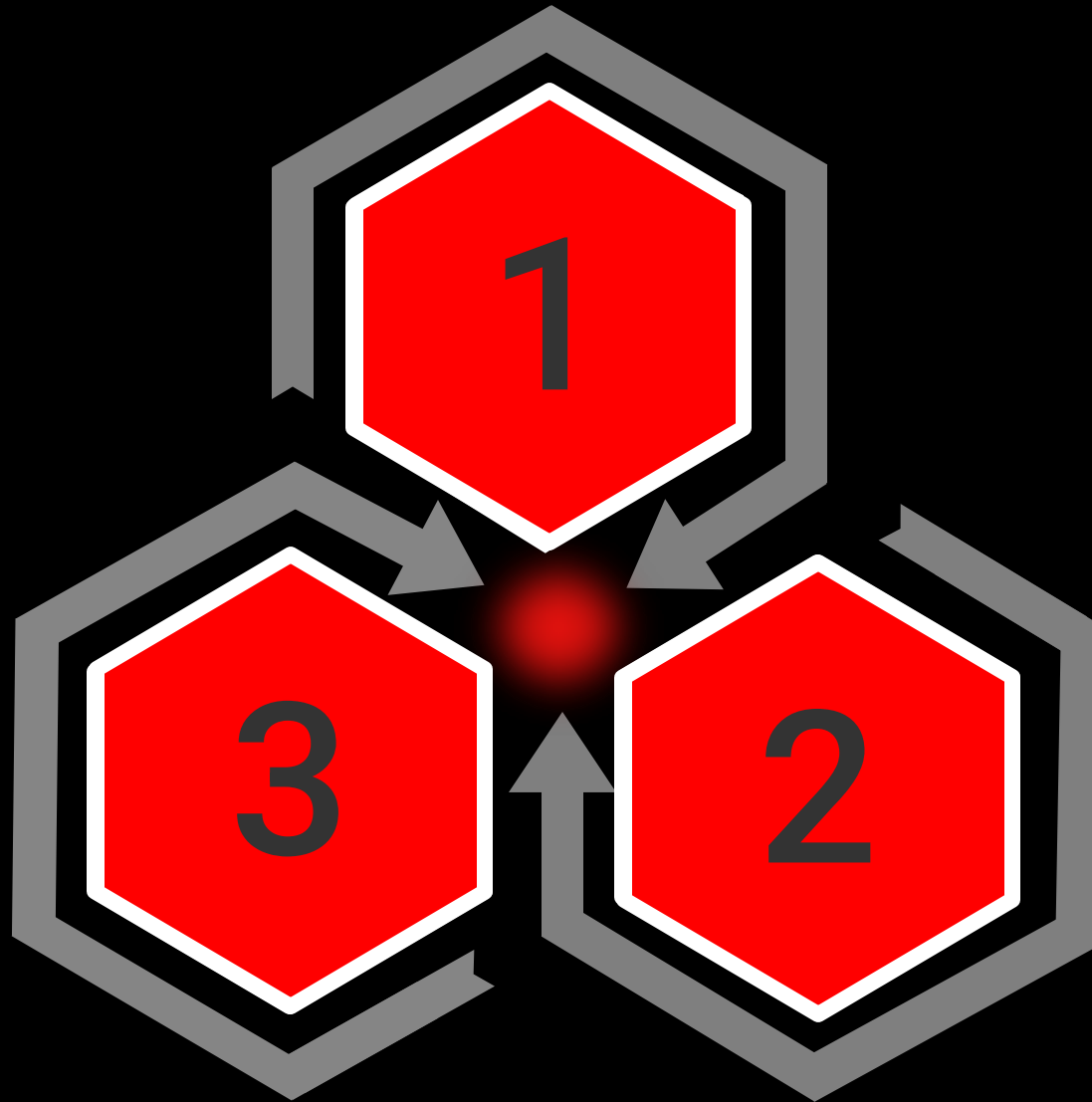


Pay employees for their session cookies

# Most Breaches Involve...



# We're At a Cybersecurity **Turning Point**



**Traditional network boundaries no longer define where data lives or threats come from...**

- Employees are accessing sensitive information from mobile devices and public internet connections.
- Applications and workloads are moving to the cloud.
- Powered by AI and automation, cybercriminals can scale attacks, adapt faster, and exploit more before defenders can respond.

**The old network security playbook is no longer sufficient.**

# SMBs Are a Primary Target

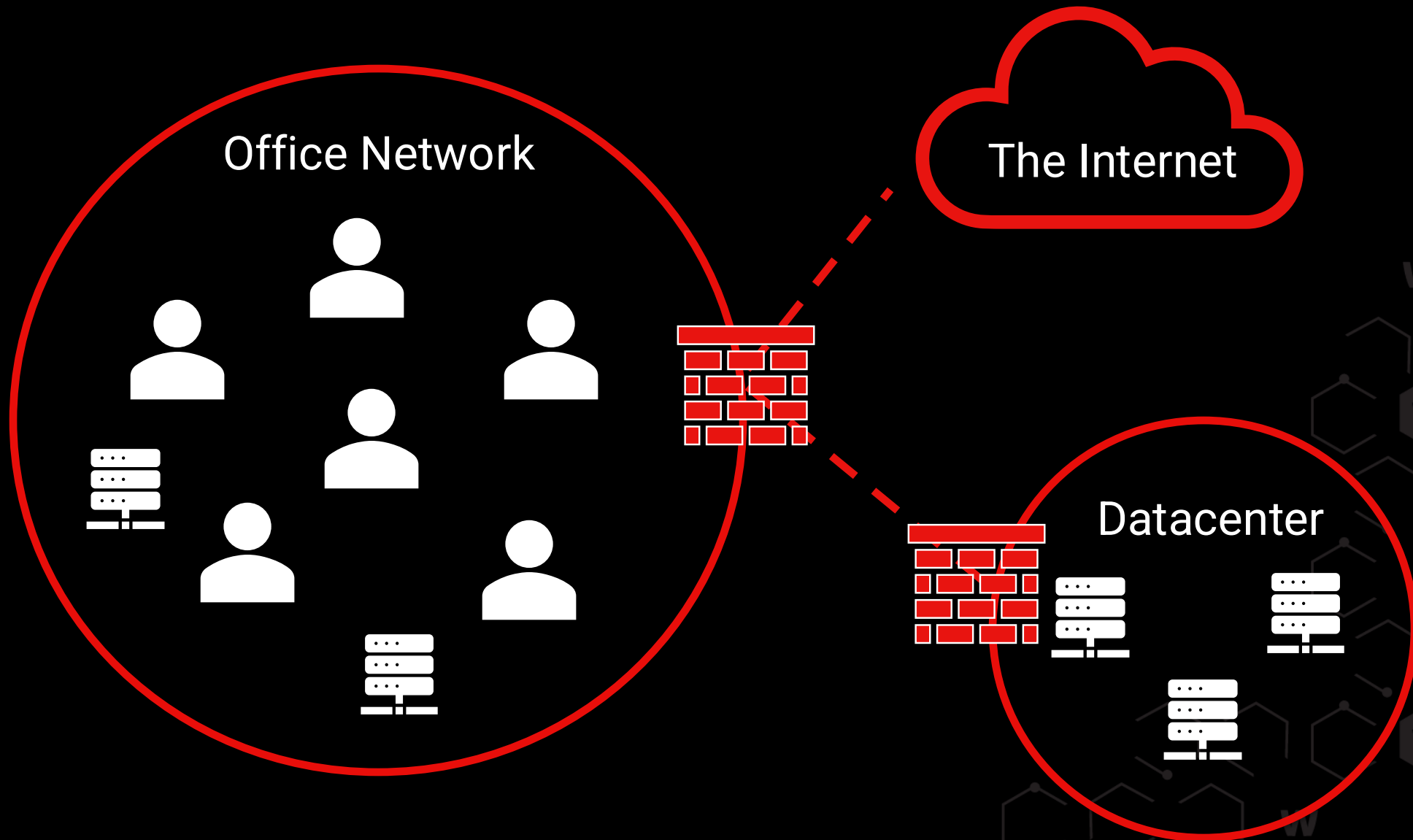
→ **61%** of cyberattacks target SMBs specifically.  
- BlackFog

→ **82%** of ransomware attacks target companies with fewer than 1,000 employees.  
- Verizon DBIR

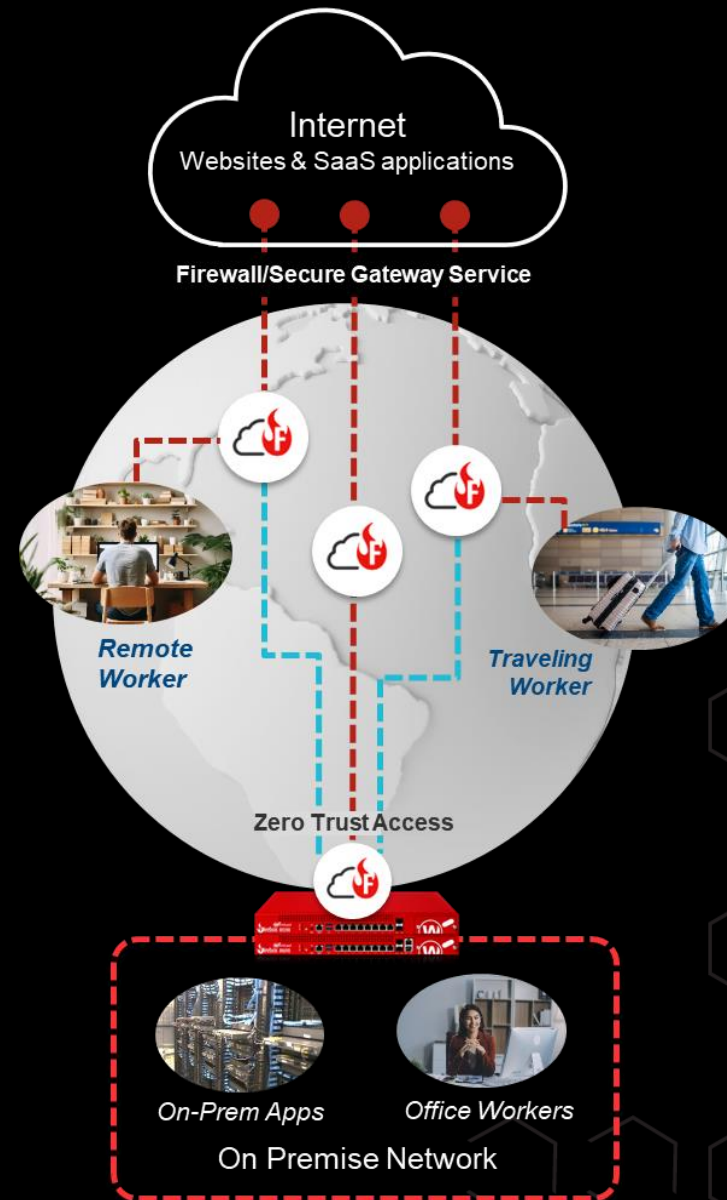
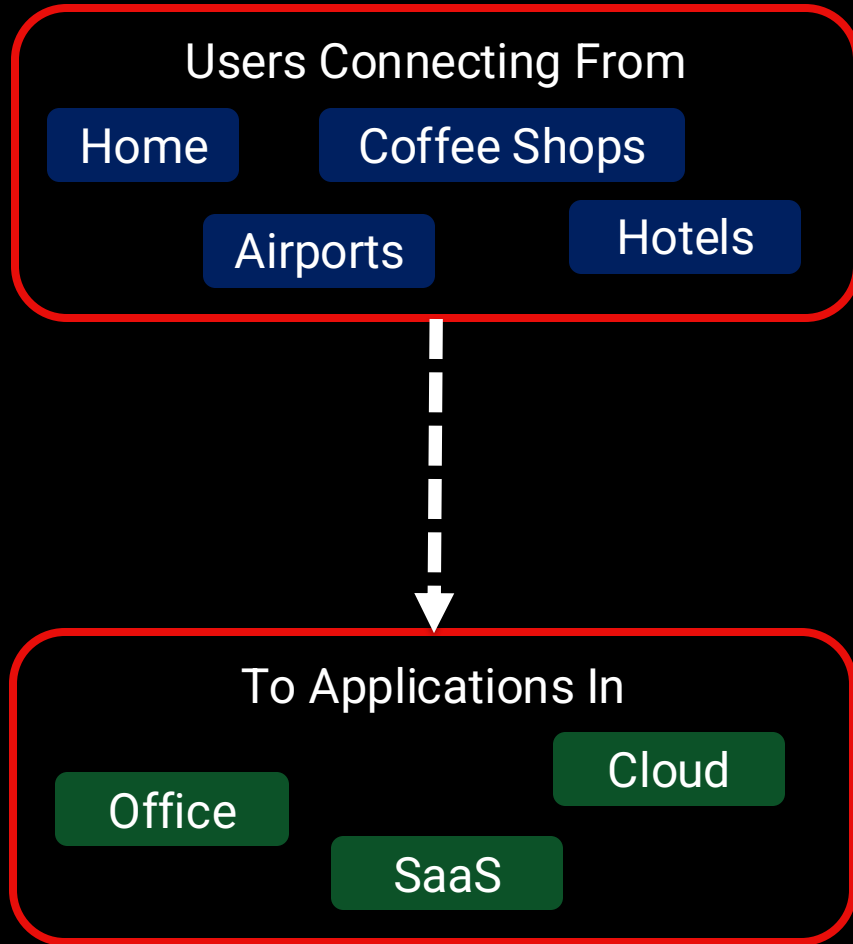
→ Cost of a breach is now **\$1.24m** million for SMBs  
- Verizon DBIR

→ **83%** of SMBs are unprepared financially to recover from a cyberattack.  
- Cybersecurity Magazine

# The Fundamentals Didn't Change - The Environment Did



# The New Era of Connectivity



# Where does most of your business risk exist today?

In Your Data

In Your Applications

In Your Users

In How They All Connect

# Where does most of your business risk exist today?

In Your Data

In Your Applications

In Your Users

In How They All Connect

An employee opens their laptop at home, logs into Microsoft 365, downloads a file, and shares it with a vendor

The User Involved

**Is this really the right user?**

The Device Involved

**Is this device really safe?**

The Application Involved

**Is this connection normal?**

The Data Involved

**Should this data be accessed or shared?**

# Remote Workers Are Vulnerable

Security Training Just Scratches the Surface; More Protection Is Possible

67% of data breaches are linked to remote and hybrid workers

Infostealer Malware is now the #2 technique used after phishing.

65% of stolen credentials are up for sale on the dark web the same day

60% of all cybersecurity incidents involve human error

Social engineering remained the #1 cause of breaches 15 years in a row.

## Strong Authentication (MFA)

99.9% of account compromise cases could have been prevented with MFA.

-Microsoft Research



**Real Security**

for the **Real World**

ROADSHOW

# Targeting Remote Employees

Real Security  
for the Real World

Microsoft Bing

watchguard vpn

ALL SEARCH SHOPPING IMAGES VIDEOS MAPS COPILOT MORE

Copilot Search

watchguard-vpn.net  
https://watchguard-vpn.net

### Download WatchGuard Mobile VPN with SSL

WatchGuard Mobile VPN ver27 mod30 with SSL is designed for fast, encrypted access to business resources from any location. Whether you are working from a home office or on the move, you can download WatchGuard VPN and...

21:35 WatchGuard  
MFA: Protect your SSL VPNs  
Configure the WatchGuard SSL (TLS) V...  
YouTube · WatchGuardWest · 21.4K views · Apr 4, ...

WatchGuard  
**Firebox SSL**  
Server: 203.0.  
 Use  
User name: j.smit  
Password:  
 Automatically rec  
Conn

### Download, Install, and Connect the Mobile VPN with SSL Client

1. Client Computer Requirements. For information about which operating...
2. Download the Client Software. You can download the client from the...
3. Install the Client Software. After you download and install the client softwar...
4. Connect to Your Private Network. Specify the Client Connection Settings....
5. Other Connection Options. Two other connection options are available in...

### How do I uninstall WatchGuard mobile VPN with SSL client?

The WatchGuard Mobile VPN dialog box opens with information about the client software. Exit (Windows) or Quit (macOS) Disconnect from the Firebox and shut  
watchguard.com

### Download, Install, and Connect the Mobile VPN with SSL

This topic describes how to install the Mobile VPN with SSL client. This topic also describes how to connect to a private network.

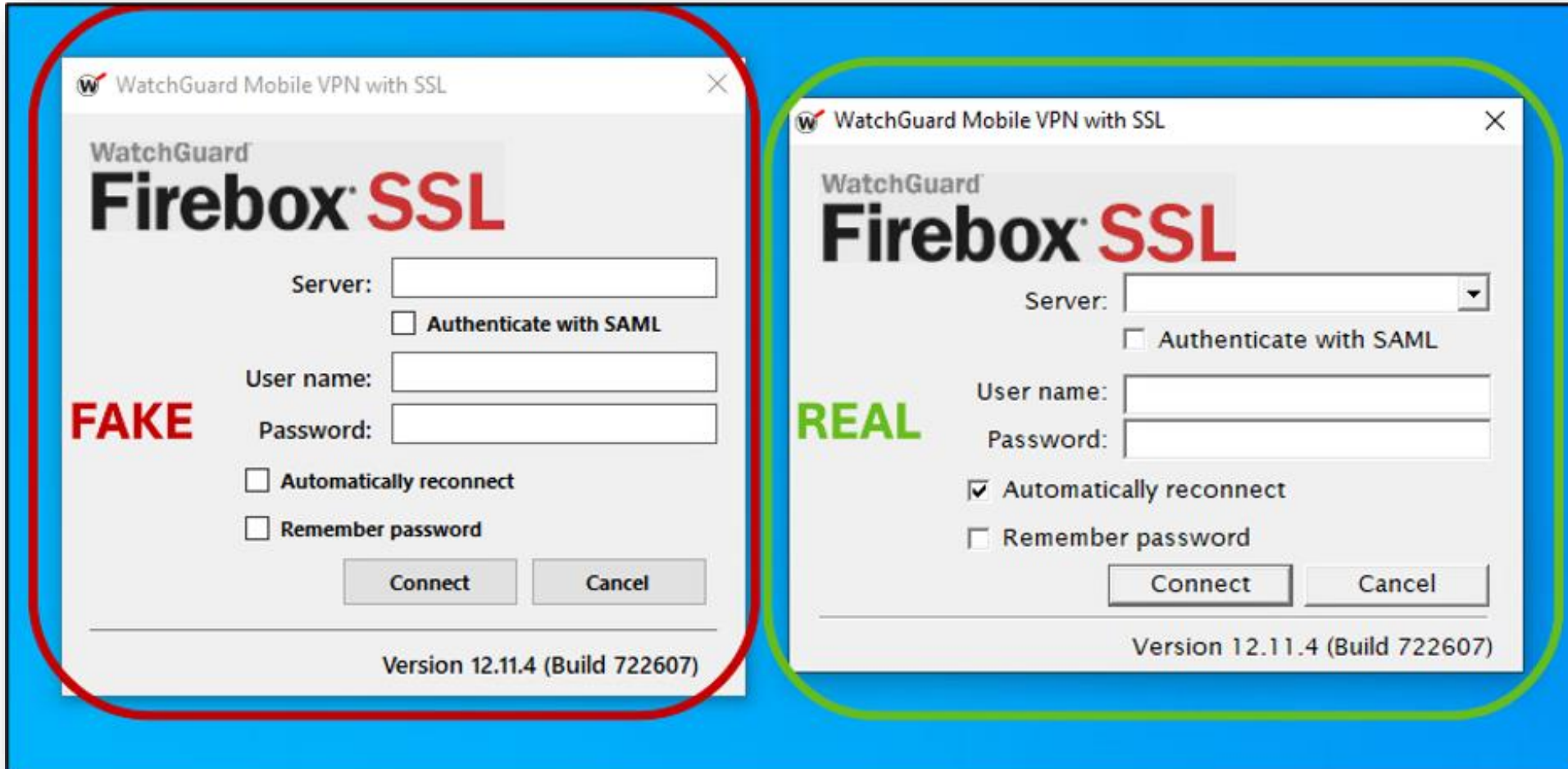
WatchGuard Technologies

Best settings for WatchGuard VPN    Compare WatchGuard SSL VPN clients    WatchGuard VPN client troubleshooting



# Can You Spot the Difference?

Real Security  
for the Real World



# Accelerating AI Threats and Defenses

## 2005 – Smarter Antivirus

- Early machine learning makes antivirus smarter. 2010

## 2010 – Stuxnet Wake-Up Call

- Nation-state attacks prompt behavior-based detection.

## 2014 – DARPA Cyber Challenge

- AI competes to detect and patch vulnerabilities.

## 2016 – AI in Endpoint Security

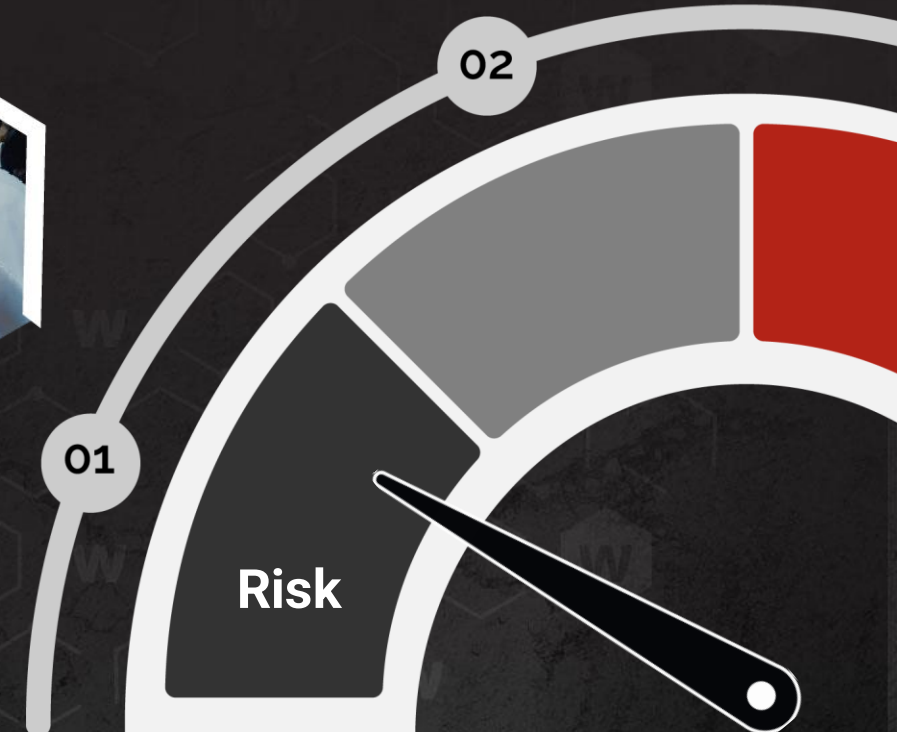
- Predictive EDR launched by major AV vendors



'14 DARPA  
Cyber Challenge



'05 Basic  
Machine Learning



# Accelerating AI Threats and Defenses



**'17 Rise of Ransomware Gangs**

03



**'20 AI Arms Race & GPT born**

04

**Risk**

## 2017 – Automation of SOC

- Using ML Across the Stack

## 2019 – Whale Hunting

- \$10Bn in Ransomware damage

## 2020 – Deepfake Attacks Rise

- AI powers phishing, impersonation, and social engineering.

## 2025 – Generative AI in Hacking

- LLMs used by both attackers and defenders at scale.

## 2026 – Agentic Hacking

- Fully autonomous attack campaigns

# Agentic Attacks Are The Latest Challenge

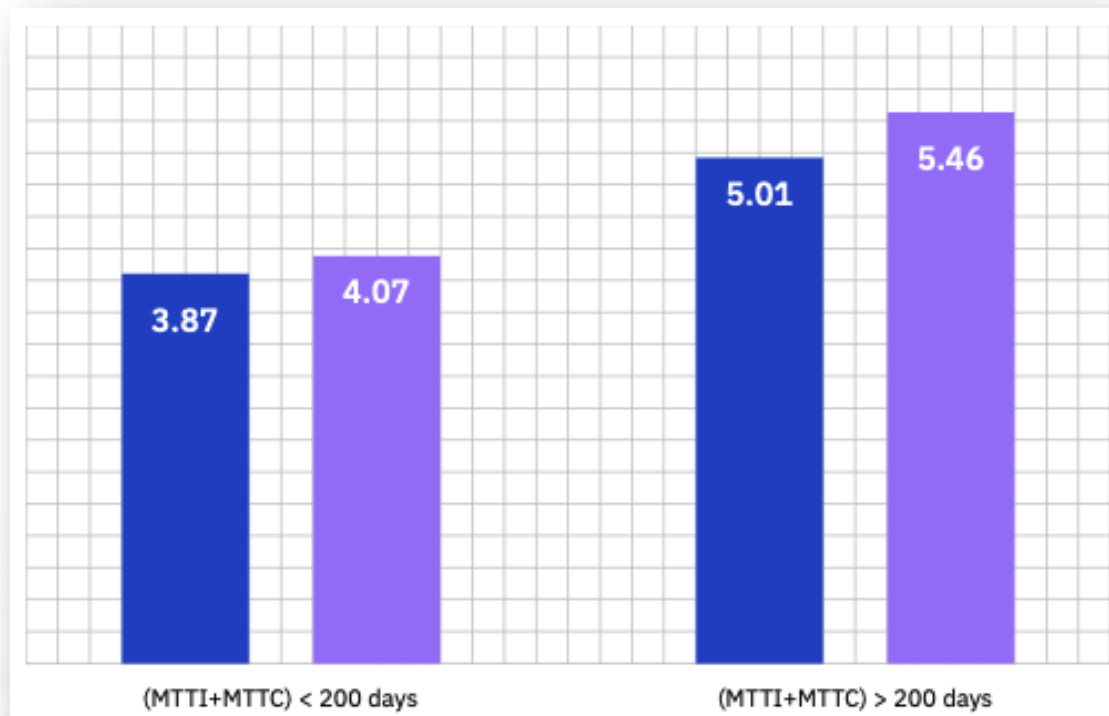


# Detection and Response is Too Slow

276

Days it took to identify and contain a data breach across various environments

Cost of a Breach in Millions



*\*IBM Cost of a data Breach 2025*

# Time to Action on Objective Decreasing

Top ransomware operators have an average dwell time of **less than 24 hours**.

- 2025 Veeam Ransomware Trends Report



ChatGPT 4o ▾

Temporary



Good to see you, Marc.

Ask anything



Search

Deep research



It's not a matter of if, but when.  
There is no silver bullet defense.





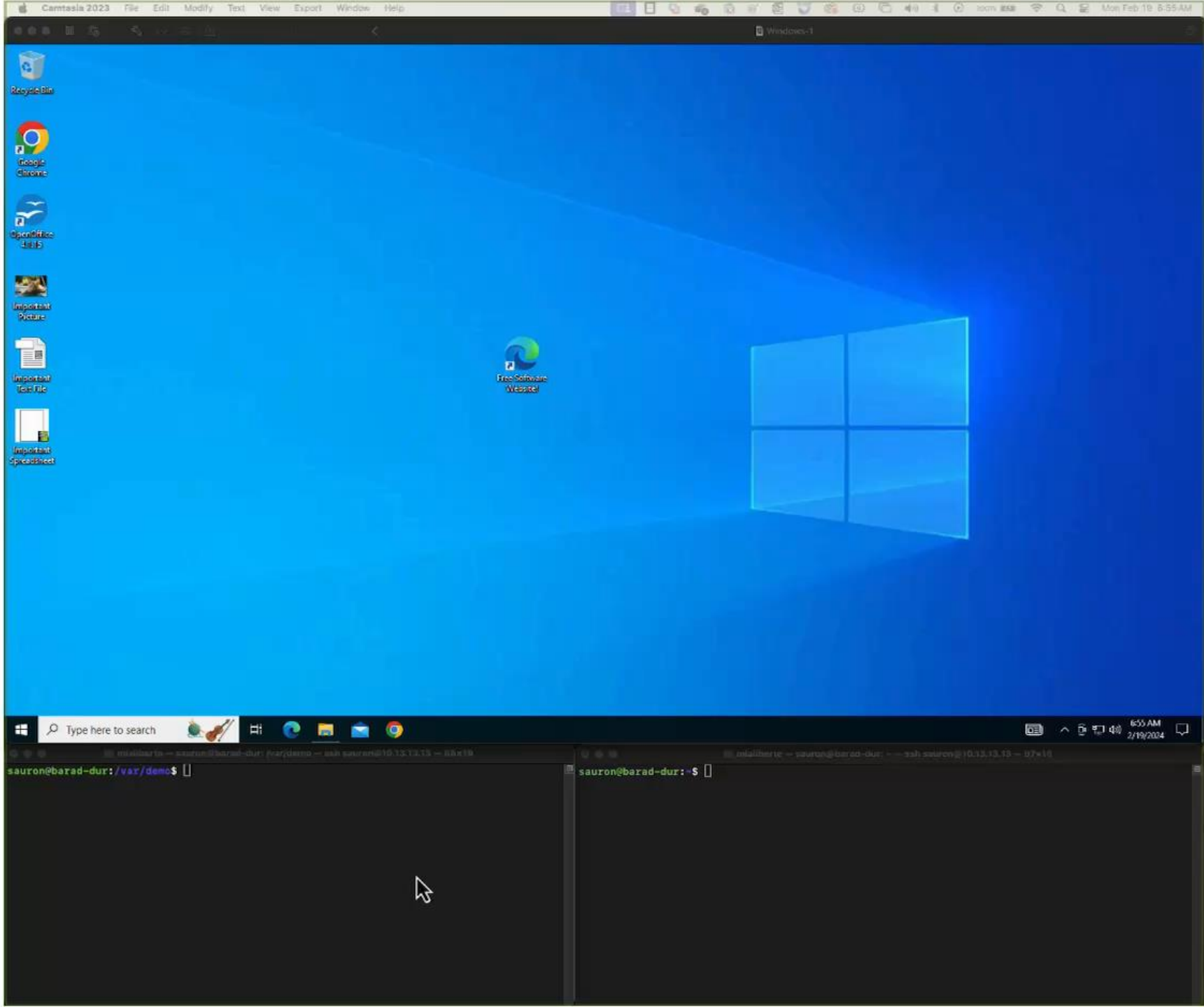
Advanced threats leverage multiple vectors of attack. No **single** defense will protect you completely



MFA effectively mitigates the overwhelming majority of authentication attacks

Advanced **behavior-based**  
anti-malware catches evasive  
threats that signatures miss







EDR quickly **detects** and **contains** threats that traditional endpoint protection misses

ZTNA provides **secure remote access** to private resources without exposing you to hackers



# Only through a layered defense can you achieve **Real Security.**



# Thank You!

LinkedIn: [/in/marc-laliberte/](#)

BlueSky: [@itsmarc.me](#)

WatchGuard Solutions Products & Services Resources Partners News Support Try Now

## The 443 - Security Simplified Podcast

Breaking Down and Simplifying Cybersecurity Headlines & Trends

Cybersecurity Hub | Internet Security Report | Threat Landscape | Ransomware Tracker | The 443 Podcast

### All Podcast Episodes

[The 443 on Apple Podcasts](#) [The 443 on Spotify](#) [The 443 via RSS](#)

#### Episode 290 – The Seattle Kraken Edition

15 May 2024

In a very special episode of #the443Podcast, WatchGuard Director of Security Operations, Marc Laliberte sits down with Seattle Kraken Cybersecurity Engineer, Ryan Willgues to discuss how Ryan got his start in IT, what it's like working for an NHL franchise, how the Kraken have deployed WatchGuard's Unified Security Platform, and much more.

[Start Episode 290 >](#)

#### Episode 299 – CrowdStrike's Incident Report

29 July 2024

Description: This week on the episode, we walk through CrowdStrike's preliminary post incident report to understand exactly what happened during the July 19th outage and what all software vendors can learn from the event. After that, we cover a clever plot that lead to KnowBe4 hiring a North Korean threat actor. We end with some research from Wiz on Artificial Intelligence tenant isolation.

[Start Episode 299 >](#)