

# Keeping SLED Organizations One Step Ahead of Hackers



**Brendan Patterson**  
VP Product Management



# Key Challenges in State, Local Gov. & Education Network Security

- ▶ Phishing
- ▶ Credential Theft
- ▶ Ransomware
- ▶ Inappropriate usage of networks
- ▶ Hacktivism
- ▶ Election hacking

## Did You Know?

80% of state governments say that funding is their top challenge in government information security



## Key Challenge: Outdated legacy technology

- ▶ Hackers are continuing to evolve and perfect their attack methods
- ▶ Legacy solutions are easily one of the most prevalent factors impacting the efficacy of SLED cybersecurity protection
- ▶ Cybersecurity is not well funded in SLED
- ▶ Organizations need to be more proactive in their security postures





## Phishing by the numbers

**91% OF CYBERATTACKS START WITH A SPEAR-PHISHING EMAIL**

\*Trend Micro Spear-Phishing Report

#1

Top action used in breaches is **stolen credentials**

*Verizon Data Breach Investigations Report 2018*

81%

Total number of breaches that leveraged **either stolen and/or weak passwords**

*Verizon Data Breach Investigations Report 2017/2018*

1.4B

Number of **hacked/leaked passwords** found in a file on the dark web

*Forbes, December 11, 2017*

PASSWORD

\* \* \* \* \*



# WatchGuard Password Research



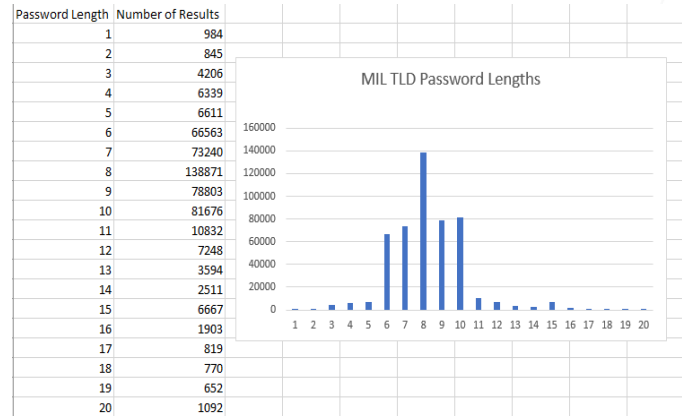
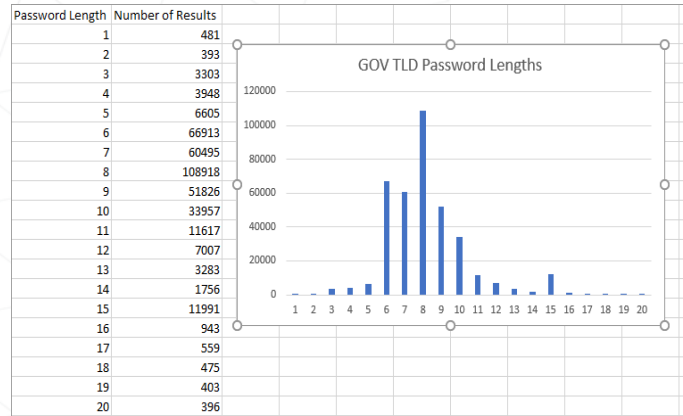
Do government and military organizations use password security best practices?

- Leaked .gov passwords = 380,077
- Leaked .mil passwords = 503,878



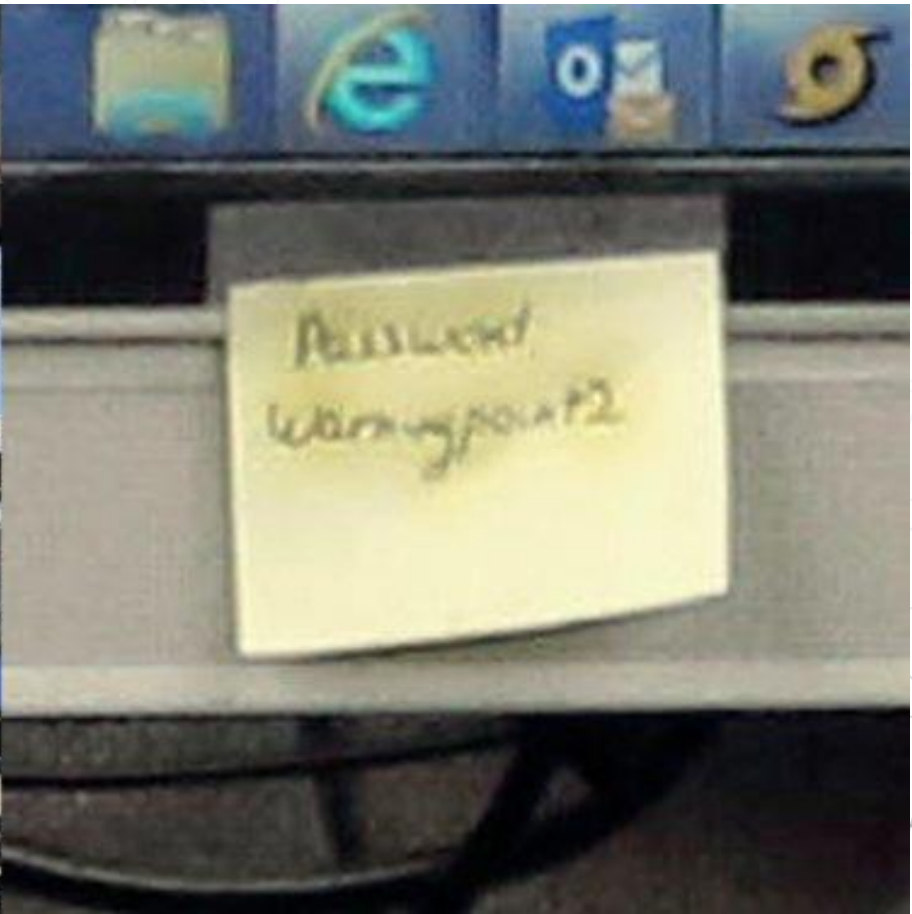
Combined, only **.07%** of these addresses used **one of the 50 most common passwords.**

**Marc Laliberte**  
Sr. Security Analyst  
WatchGuard



## Most, however, didn't use sufficiently long passwords

# Hawaii – Emergency Management



## Ransomware was on decline, but ...

### SECURITY

# Over a Month On, Baltimore Still Grappling with Hack Fallout

*The city has been slowly getting its operations and systems back online after a cyberattack in early May, but debate over the administrative response to the attack is still causing controversy.*

BY LUCAS ROPEK / JUNE 17, 2019



## RECOVER FROM A \$52,000 RANSOMWARE SCARE



# Hacktivist launch more cyberattacks against local, state governments

<http://www.kpax.com/story/38487006/hacktivist-targeting-montana-government-computers>  
<http://www.dispatch.com/news/20180226/hacktivist-group-takes-down-state-websites-telephones>  
<https://www.pbs.org/newshour/nation/hacktivist-launch-cyberattacks-local-state-governments>



# Key Challenge: Election Hacking

- ▶ Election system with more than 10,000 unique jurisdictions
- ▶ Responsibility of security often falls to local officials who are not up to date on the latest security threats

**MOTHERBOARD**  
TECH BY VICE

## Exclusive: Critical U.S. Election Systems Have Been Left Exposed Online Despite Official Denials

The top voting machine company in the country insists that its election systems are never connected to the internet. But researchers found 35 of the systems have been connected to the internet for months and possibly years, including in some swing states.

By [Kim Zetter](#)

Aug 8 2019, 10:55am [f Share](#) [t Tweet](#)

# WatchGuard Internet Security Report

Based on opt-in threat feed containing malware and network attack data from tens of thousands of Fireboxes around the world.

## The Firebox Feed includes:


- Gateway AntiVirus
- Intelligent AV (IAV) - machine-learning AV
- APT Blocker - sandbox malware detection
- Intrusion Protection Service (IPS) – network
- DNSWatch - a DNS filtering service

## Top 10 Gateway AntiVirus Malware Detection

COUNT	THREAT NAME	CATEGORY
3,728,249	Mimikatz	Password Stealer
1,300,282	Win32/Heim.D	Win Code Injection
746,048	CVE-2017-11882	Office Exploit
337,330	HTML-PowerShell	Win Code Injection
299,762	Adware.MAC	Adware
297,672	Linux/Flooder	Generic Linux DDoS Tool
291,988	Generic.Application.CoinMiner.1.8BFB0BA6	Cryptominer

Malware	Percentage Change (+/-)	2019 Q1 Volume	2018 Q4 Vo
Mimikatz	+73.2%	3,728,249	2,152,48
Heim.D	+388.8%	1,300,282	266,013
CVE-2017-11882	+58.6%	746,048	470,279
Linux/Flooder	+15.3%	297,672	258,167
CoinMiner	-42%	291,988	503,510
MAC.OSX.AMCleaner	-18.4%	231,888	284,162
Win32/Heur	-25.8%	230,466	310,625

# Malware Trends



The **Firebox Feed** recorded threat data from

**42,372**

participating Fireboxes

a **12%** increase in the number of Fireboxes reporting year over year.



Our **GAV** service blocked

**18,107,580**

malware variants

a **62%** increase quarter over quarter.

YoY we increased by **6.6%**.



**APT Blocker** detected

**5,308,364**

additional threats

QoQ we saw a **39.4%** increase YoY we decreased

by **21.33%**



**IntelligentAV** blocked

**469,035**

malware hits

**18%** of

of total GAV hits on supported models



**35.89%**  
OF MALWARE WAS  
**ZERO DAY**



**64.1%**  
OF MALWARE WAS  
**Known Malware**

# Regulations

---

## PCI-DSS and HIPAA



### Built-in Reports

Management and visibility solutions can provide compliance reports

### MFA

Requirement 8.3.2, added in v3.2, mandates MFA for admins accessing the CDE

### VPNs/Encryption

Protected health data must be encrypted during transit

### MFA

Standard 164.312 (d) requires verification of users of electronic protected health info



# CJIS Compliance for Police



## 13 Policy Areas

### Management & Logging

CJIS defines the events that shall be logged, and log contents

### Multi-Factor Authentication

CJIS requires unique identities, advanced authentication, and secure password/PIN attributes

### Firewall/UTMs and VPNs

CJIS mandates security to include patch management, intrusion detection, malicious code protection, spam and spyware protection, security alerts and advisories

### Wi-Fi Management & Security

CJIS requires you to enable all security features

1. Information Exchange and User Agreements
2. Security Awareness Training
3. Incident Response
4. Auditing and Accountability
5. Access Control
6. Identification and Authentication
7. Configuration Management
8. Media Protection
9. Physical Protection
10. System and Communications Protection and Information Integrity
11. Formal Audits
12. Personnel Security
13. Mobile Devices

# CIPA for Schools and Libraries

**Who?** K-12 schools and libraries using E-Rate discounts

**What?** Must operate "a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are obscene, child pornography, or harmful to minors".

**When?** During any use by minors. The law also provides that the school or library "may disable the technology protection measure concerned, during use by an adult, to enable access for *bona fide* research or other lawful purpose".

## Content Filtering

Restricts content that can be viewed by category; override features are available





# Additional Sources of Funding or E

## E-rate

The E-rate program provides discounts on certain services at classrooms and libraries to receive Internet connections. The of the cost of eligible services depending on level of poverty. To be eligible to receive discounts, a school or library must r general elementary schools, secondary schools, and public <https://www.fcc.gov/consumers/guides/universal-service-pro>

**GSA IT Security** <https://www.gsa.gov/technology/>

**PEPPM Technology Bidding Program**

<https://www.peppm.org/>

**NCPA Cooperative Purchasing** <http://www>

**MNIT Cybersecurity Program (Minnes**

The program allows Counties to get a free firewall if they ag Capitol. The capitol then runs a SIEM and log scanning ser see an anomaly they contact the county to note a potential k <https://statescoop.com/minnesotas-five-year-plan-addresses>

WatchGuard – All Products

(Make selections from the drop-down menus below to search for specific items)

Product Search:  Category: ALL Status: Submitted OR Active Show Sub-Products: YES FY: 2015 and after

Product Name	Name	Description	SVC Category	Price	%Elig	Status
AP120	Access Point 120	Remote wireless AP - 1 x 1 GBE, dual radio 2.4/5GHz, 5.150-5.250GHz, 3.250-3.300GHz, 5.475-5.725GHz, 5.725-5.850GHz (802.11 a/b/g/n, 802.11n, 802.11g, 802.11a, 802.11ac, 802.11n)	IC	\$320.00	90%	Submitted
	WGA12701	WatchGuard AP120 with 1 yr Standard Support	Bundle-IC/BA/IC	\$320.00	90%	Submitted
	WGA12703	WatchGuard AP120 with 3 yr Standard Support	Bundle-IC/BA/IC	\$400.00	90%	Submitted
	WGA12721	WatchGuard AP120 with 1 yr Standard Support and WiFi Cloud Subscription	Bundle-IC/BA/IC	\$525.00	90%	Submitted
	WGA12723	WatchGuard AP120 with 3 yr Standard Support and WiFi Cloud Subscription	Bundle-IC/BA/IC	\$605.00	90%	Submitted
	WGA12403	Trade Up to WatchGuard AP120 and 3 yr Standard Support - Previous device was not part of E-Rate Program or is beyond the 5-year limitation	Bundle-IC/BA/IC	\$365.00	90%	Submitted
	WGA12483	Trade Up to WatchGuard AP120 and 3 yr Wi-Fi Cloud Subscription and Standard Support - Previous device was not part of E-Rate Program or is beyond the 5-year limitation	Bundle-IC/BA/IC	\$775.00	90%	Submitted
	WGA12443	Competitive Trade In to WatchGuard AP120 and 3 yr Standard Support - Previous device was not part of E-Rate Program or is beyond the 5-year limitation	Bundle-IC/BA/IC	\$365.00	90%	Submitted
	WGA12453	Competitive Trade In to WatchGuard AP120 and 3 yr Wi-Fi Cloud Subscription and Standard Support - Previous device was not part of E-Rate Program or is beyond the 5-year limitation	Bundle-IC/BA/IC	\$775.00	90%	Submitted
	WGWFC191	WatchGuard 1 yr Wi-Fi Cloud Subscription and Standard Support	BM	\$185.00	93%	Submitted
	WGWFC193	WatchGuard 3 yr Wi-Fi Cloud Subscription and Standard Support	BM	\$465.00	90%	Submitted
	WGA12201	WatchGuard AP120 1 yr Standard Support Renewal	BM	\$65.00	80%	Submitted
	WGA12203	WatchGuard AP120 3 yr Standard Support Renewal	BM	\$190.00	89%	Submitted
	WGS556	WatchGuard Ethernet Power Injector	IC	\$60.00	100%	Submitted
	WGS019	Power Supply for WatchGuard AP120/AP122	IC	\$25.00	100%	Submitted
	WGS017	Ceiling Mount Kit for WatchGuard AP120	IC	\$15.00	100%	Submitted
AP320	Access Point 320	Remote wireless AP - 3 x 1 GBE, dual radio 2.4/5GHz, 5.150-5.250GHz, 3.250-3.300GHz, 5.475-5.725GHz, 5.725-5.850GHz (802.11 a/b/g/n, 802.11n, 802.11g, 802.11a, 802.11ac, 802.11n)	IC	N/A	N/A	Submitted
	WGA32701	WatchGuard AP320 with 1 yr Standard Support	Bundle-IC/BA/IC	\$525.00	90%	Submitted
	WGA32703	WatchGuard AP320 with 3 yr Standard Support	Bundle-IC/BA/IC	\$600.00	90%	Submitted
	WGA32721	WatchGuard AP320 with 1 yr Standard Support and WiFi Cloud Subscription	Bundle-	\$710.00	97%	Submitted

# WatchGuard Security Solutions

---

# Essential Security for the Modern Business

## THE WATCHGUARD SECURITY PORTFOLIO



*Network Security*



*Secure Wi-Fi*



*Multi-Factor  
Authentication*

**Build a comprehensive security plan today!**

Visit WatchGuard at booth #404

# EAL4+ / FIPS Compliant UTM Appliances



- CIPA Compliant URL Filtering: [WebBlocker](#)



## Malware Detection Services

- Signature and Heuristics: [Gateway Antivirus](#)
- Artificial Intelligence: [Intelligent AV](#)
- Cloud based sandboxing: [APT Blocker](#)

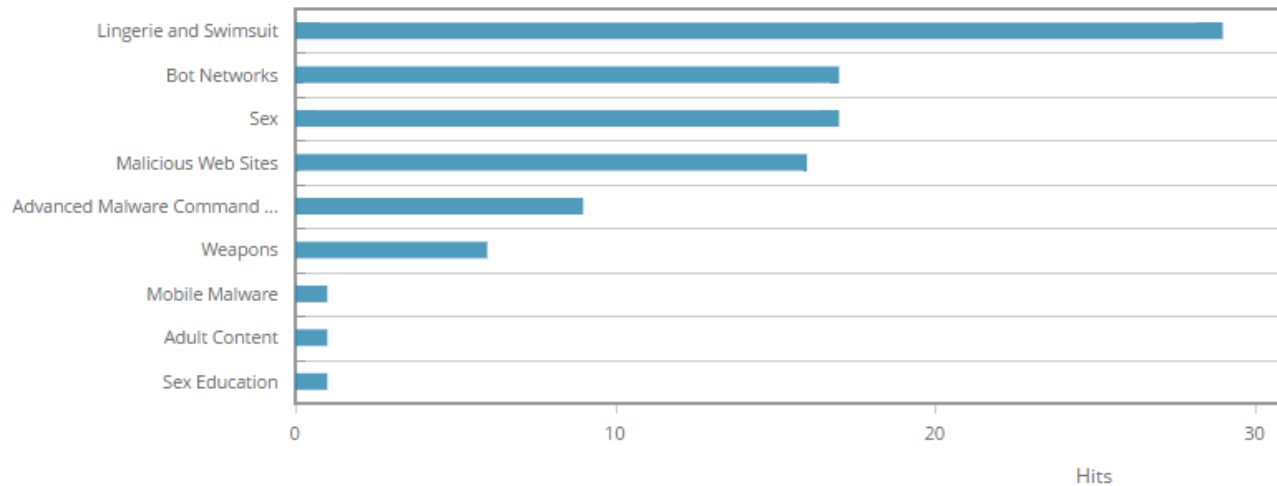


# Web Categorization

Dimension

[Home](#) / [webdemo](#) / Blocked Websites

## Blocked Websites



CATEGORY	HITS ▾
Lingerie and Swimsuit	29
Bot Networks	17

# KCSIE (UK): Monitoring Search Engine Requests

Fireboxes

Yesterday: 2019-07-30

Users

Cyril\_FBv139\_QA\_LTT

Monitor Configure

130 pages 1 25 Per page << Back Next >>

EVENT TIME	AUTHENTICATED USER	HOST	SEARCH ENGINE	QUERY
2019-07-30 00:00:15	None	192.169.2.145	www.bing.com	ad hoc
2019-07-30 00:00:55	None	192.169.2.145	www.bing.com	holiday
2019-07-30 00:01:15	None	192.169.2.145	www.google.co.uk	silent
2019-07-30 00:01:35	None	192.169.2.145	www.google.com	gleaming ripe
2019-07-30 00:01:55	None	192.169.2.145	www.bing.com	second smell
2019-07-30 00:02:16	None	192.169.2.145	www.google.com	middle blush powerful telephone co...
2019-07-30 00:02:36	None	192.169.2.145	www.bing.com	heavy itch trite boring
2019-07-30 00:03:16	None	192.169.2.145	www.google.co.uk	salty middle clear
2019-07-30 00:03:36	None	192.169.2.145	www.bing.com	thoughtless zip
2019-07-30 00:03:56	None	192.169.2.145	www.google.co.uk	seed
2019-07-30 00:04:36	None	192.169.2.145	www.google.co.uk	lazy desire agreement ultra
2019-07-30 00:05:16	None	192.169.2.145	www.bing.com	thoughtless stomach love
2019-07-30 00:05:36	None	192.169.2.145	www.google.co.uk	suck ludicrous stage jazzy
2019-07-30 00:06:16	None	192.169.2.145	www.bing.com	desert curve cluttered pumped hus...

# Educate your users



DNSWatch

W

Oo:

It l:

Pl:

**From:** do-not-reply@Anthem.com  
**Subject:** Because We Care  
**Date:** 1:32 AM EST  
**To:** Joe Robertson <joer@acmemarketing.com>

Dear Anthem Client,

We wanted to make you aware of a data breach that may have affected your personal health information and credit card data. The data which was accessed may impact clients who made credit or debit card payments for healthcare.

Your trust is a top priority for Anthem, and we deeply regret the inconvenience this may cause.

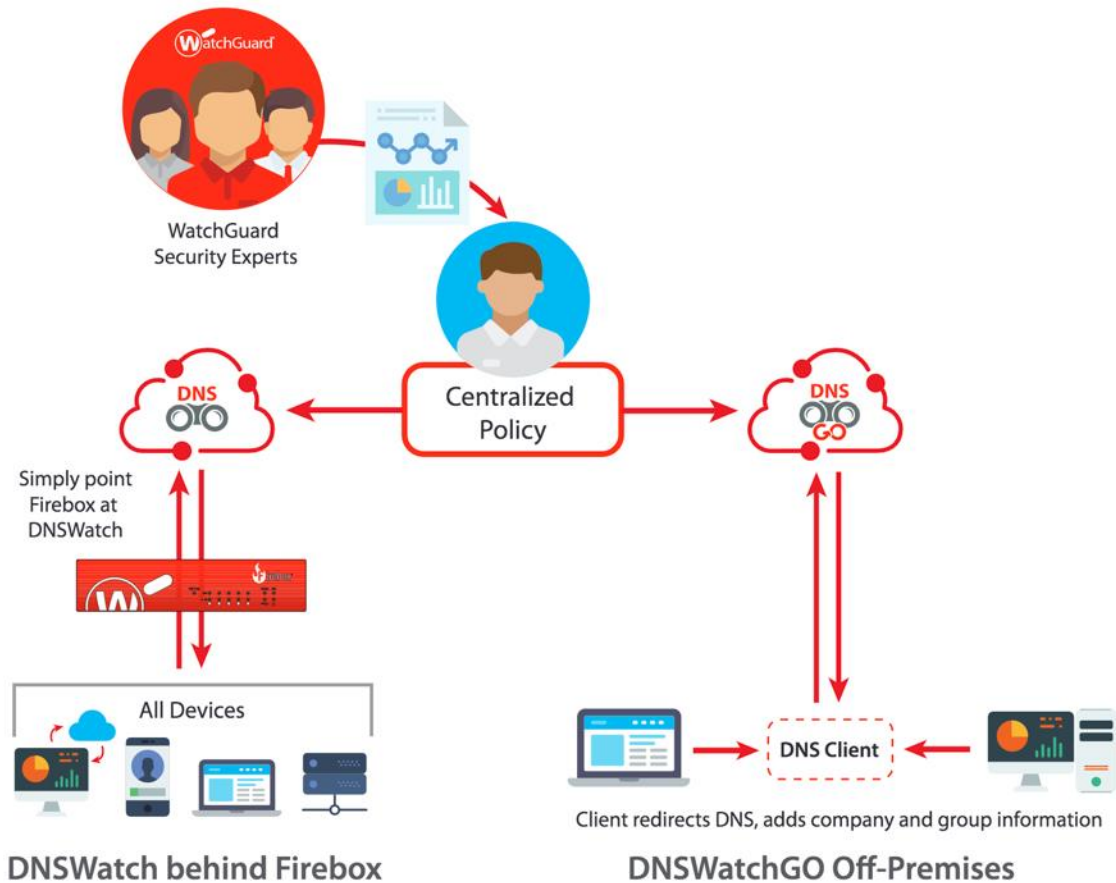
Please accept our sincere apology and a year of free credit card protection.

[Anthem.](#)

[Click Here To Get Your Free Year of  
Credit Card Protection](#)

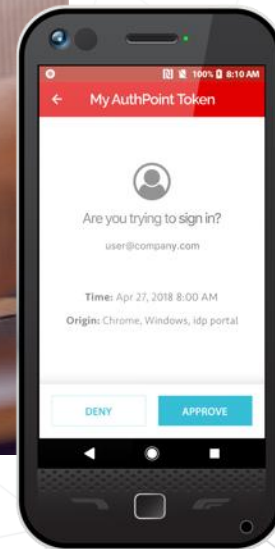
# Off Campus Monitoring

Safeguards even when computer is used away from school





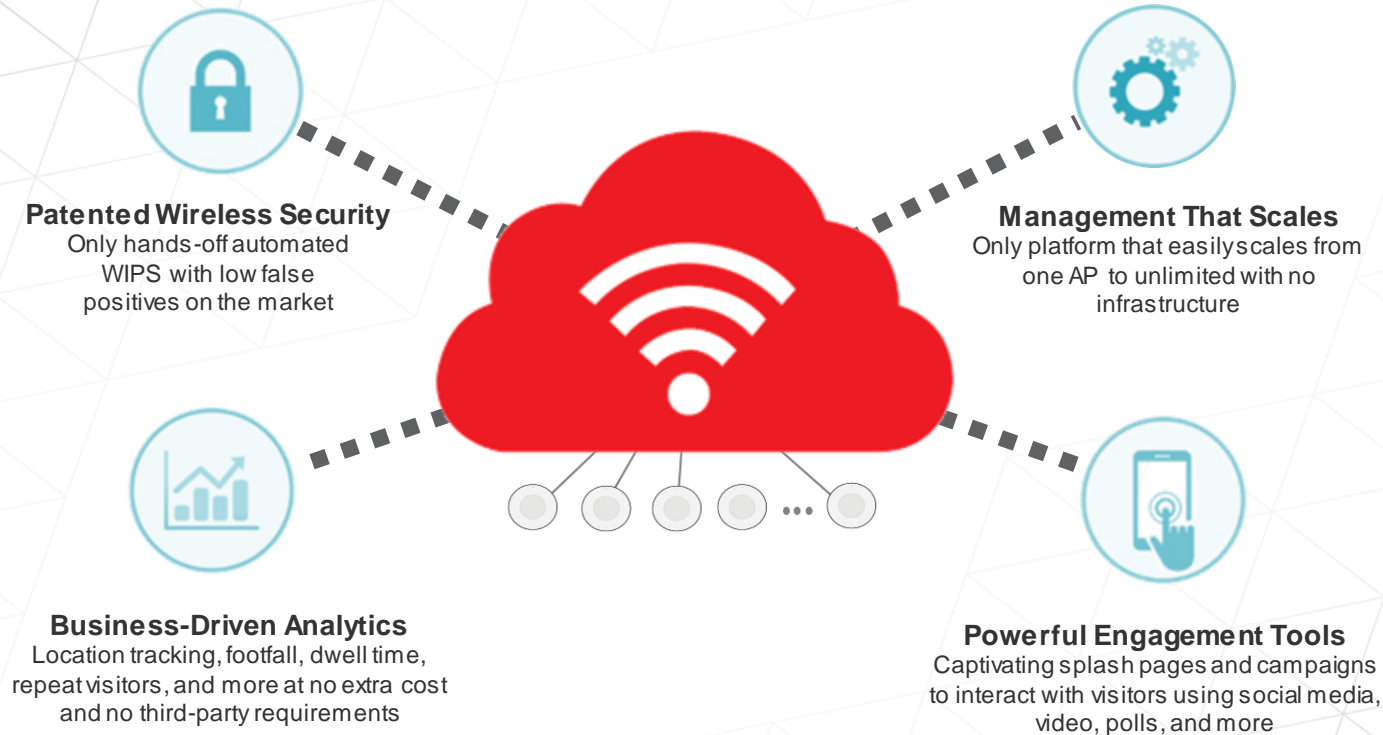
# MFA Protects With More Than Just A Password



## Multi-Factor Authentication Is Essential Protection

By requiring additional proof of identity beyond a simple password, **multi-factor authentication (MFA) is the most important safeguard** to protect your business

# Secure, Cloud-Managed Wi-Fi



# Built-In Ecosystem Integrations



## Key Takeaways

- ▶ Educate users to recognize phishing attempts
- ▶ Password length of 12 or more characters
- ▶ Multifactor authentication everywhere
- ▶ Use advanced security: Signature based detection is no longer effective
- ▶ Apply monitoring and filtering safeguards in education
- ▶ Insist that your customers take a proactive approach to cybersecurity defenses
- ▶ Visit WatchGuard at Booth #404
- ▶ Stay current at [secplicity.org](https://secplicity.org)



**all in**



***Thank You!***

