



# New Dark Web Scan in WatchGuard Cloud

# Agenda

- The Threat of the Dark Web Is Real
- Educating Your Customers About Their Own Vulnerabilities
- Introducing Dark Web Scan, Available in WatchGuard Cloud
- Selling More with Dark Web Scan Data
- Key Things to Know About User Privacy
- FAQ
- Partner Resources

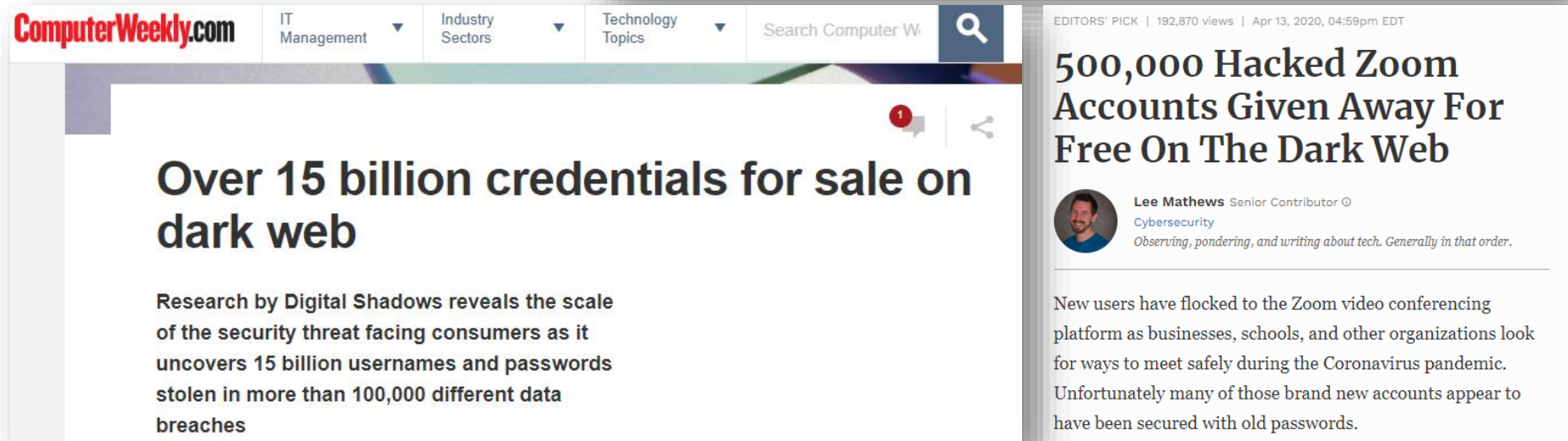
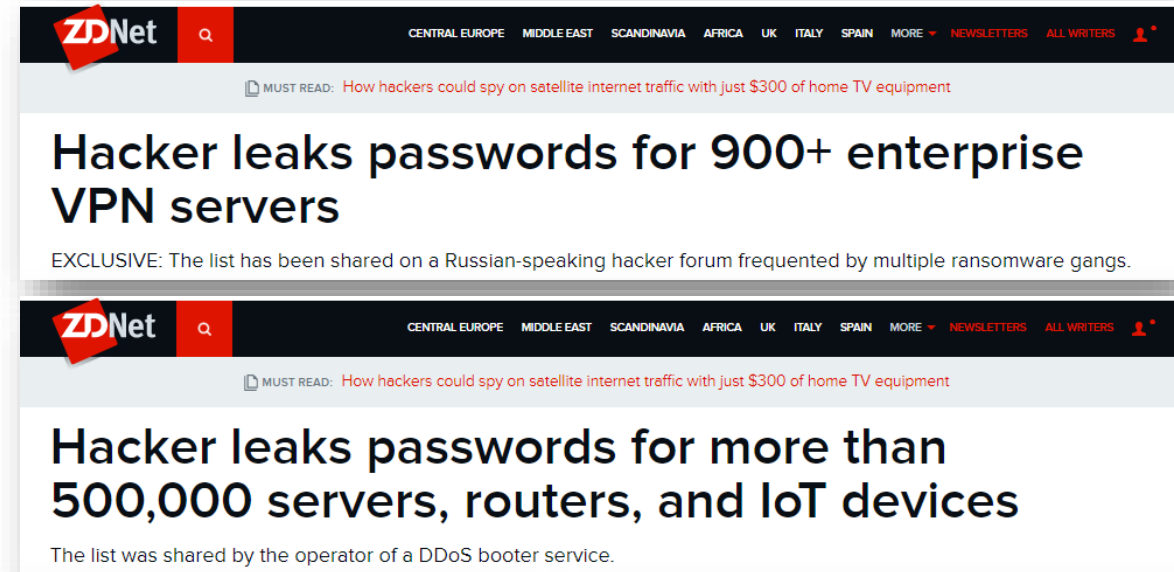


# **The Threat of the Dark Web is Real**



# The Threat of an Underground Malicious Marketplace

- Hackers are constantly finding ways to steal personal data
- Stolen sensitive information like email accounts (username and passwords), ends up for sale in one of the black markets on the dark web



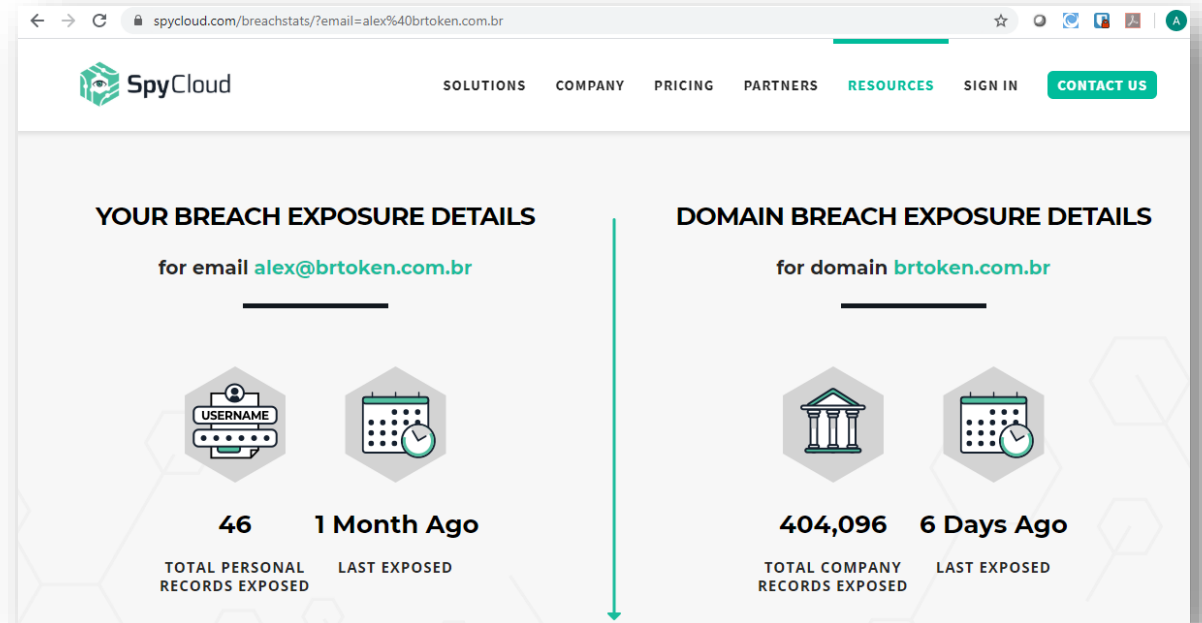
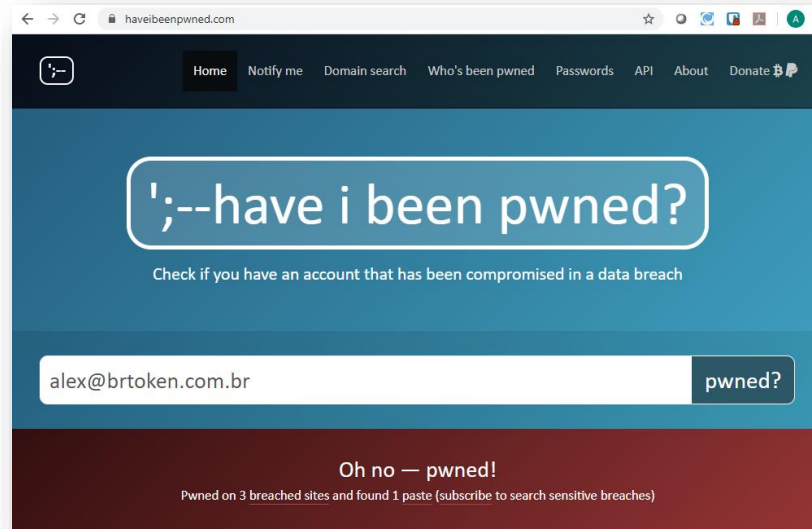
# What It Means for Your Customers

- Alert IT teams so they can take action
  - Assess existing security measures
  - Improve strategies to protect employee credentials and applications
  - Reset employees' passwords
  - Enable MFA to prevent cyber criminals from accessing important data with stolen information



# Dark Web Scanning

- Breached databases are available in several places and can be accessed by anyone
  - Check if your email or domain address has been part of a known, public breach
  - Know if your password from a service might have been exposed



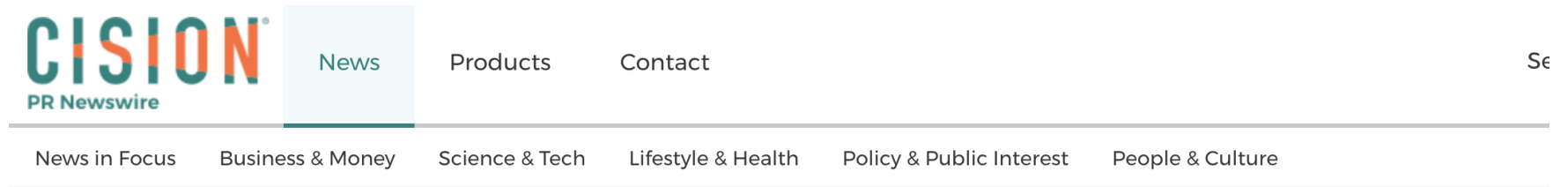




# **Educating Your Customers About Their Own Vulnerabilities**

# Small Businesses At Risk

- 63% of businesses reported an incident involving the loss of sensitive information about customers and employees in the past year.



## Ponemon: Cyberattacks on SMBs Rising Globally, Becoming More Targeted and Sophisticated

English ▼

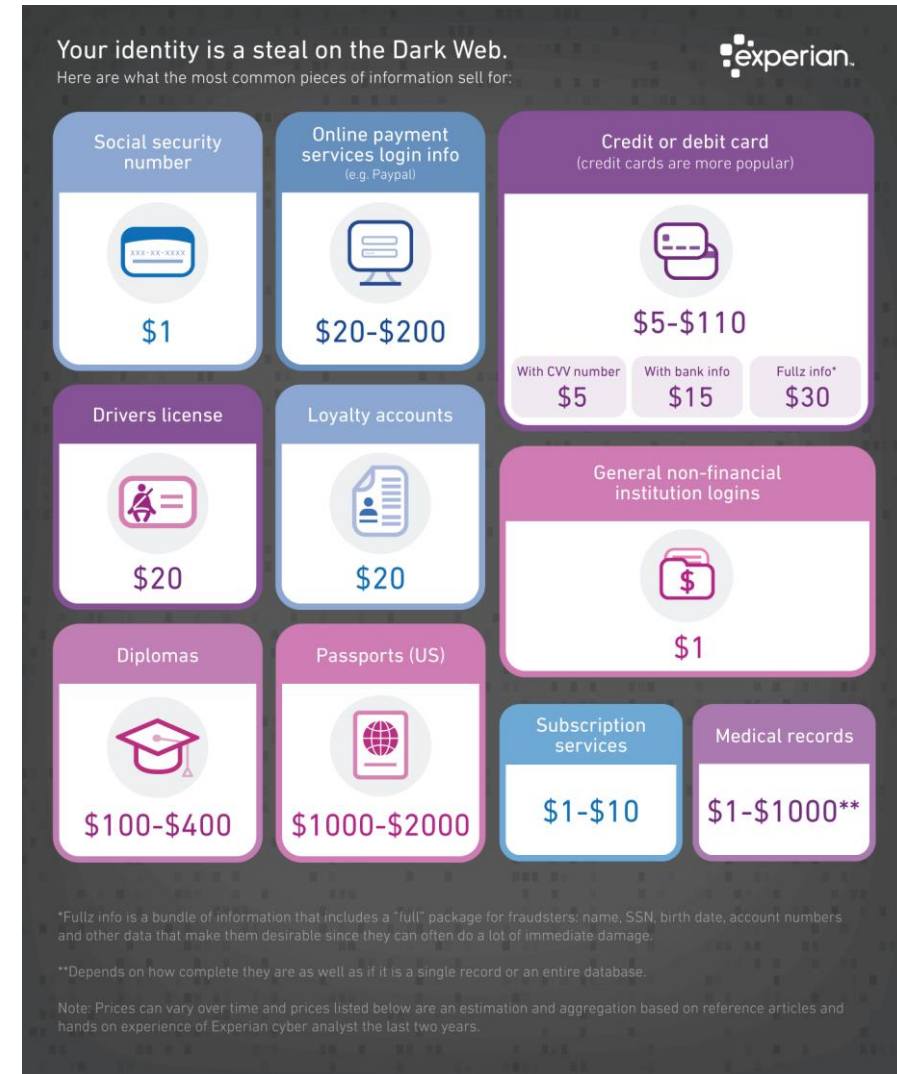
66% of SMBs globally reported a cyberattack within the past 12 months, 76% in the U.S





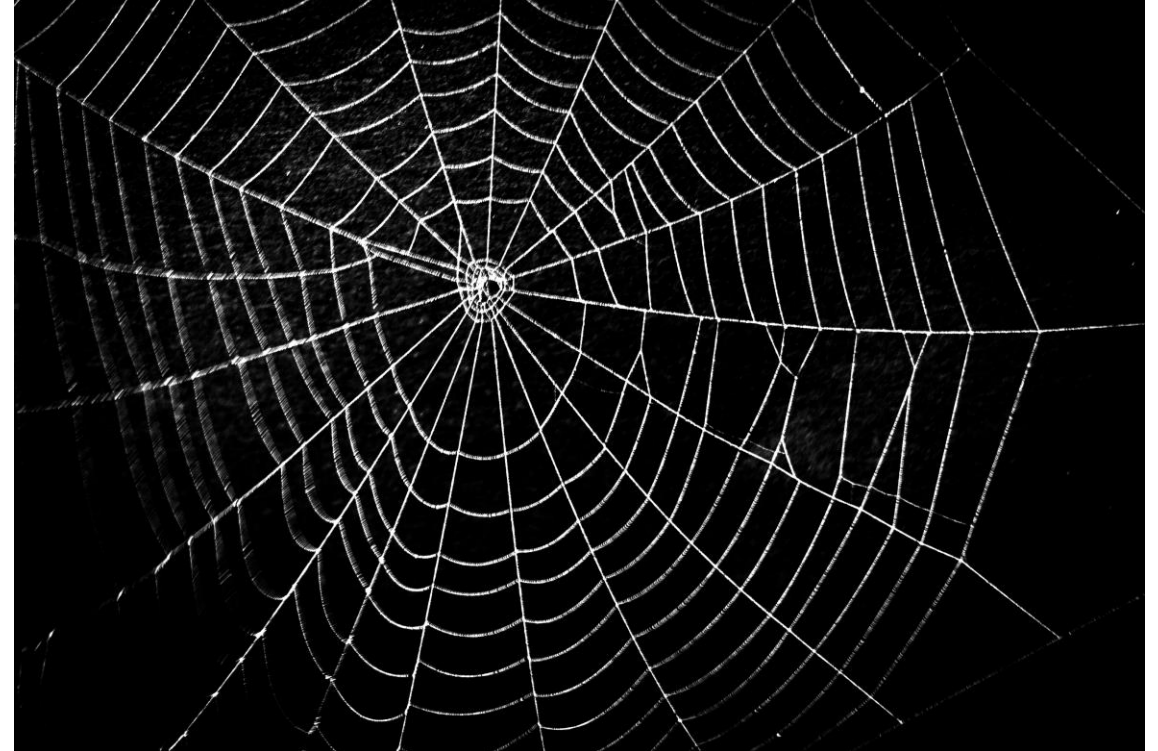
# The Price of Stolen Data on the Dark Web

- Installing malware
- Stealing customer and employee information
- Stealing intellectual property
- Transferring funds
- Deleting files or information
- Threatening you with ransomware
- Modifying sensitive information



# Can Solution Providers Save the Day?

- The Dark Web Scan is a free WatchGuard Cloud tool that can be used as a an AuthPoint Sales Tool
- No credential breaches today? How about tomorrow?
- Users might have been breached with personal emails, and could use same password for corporate account
- AuthPoint is an effective way to protect your credentials – and find out if someone stole your password!





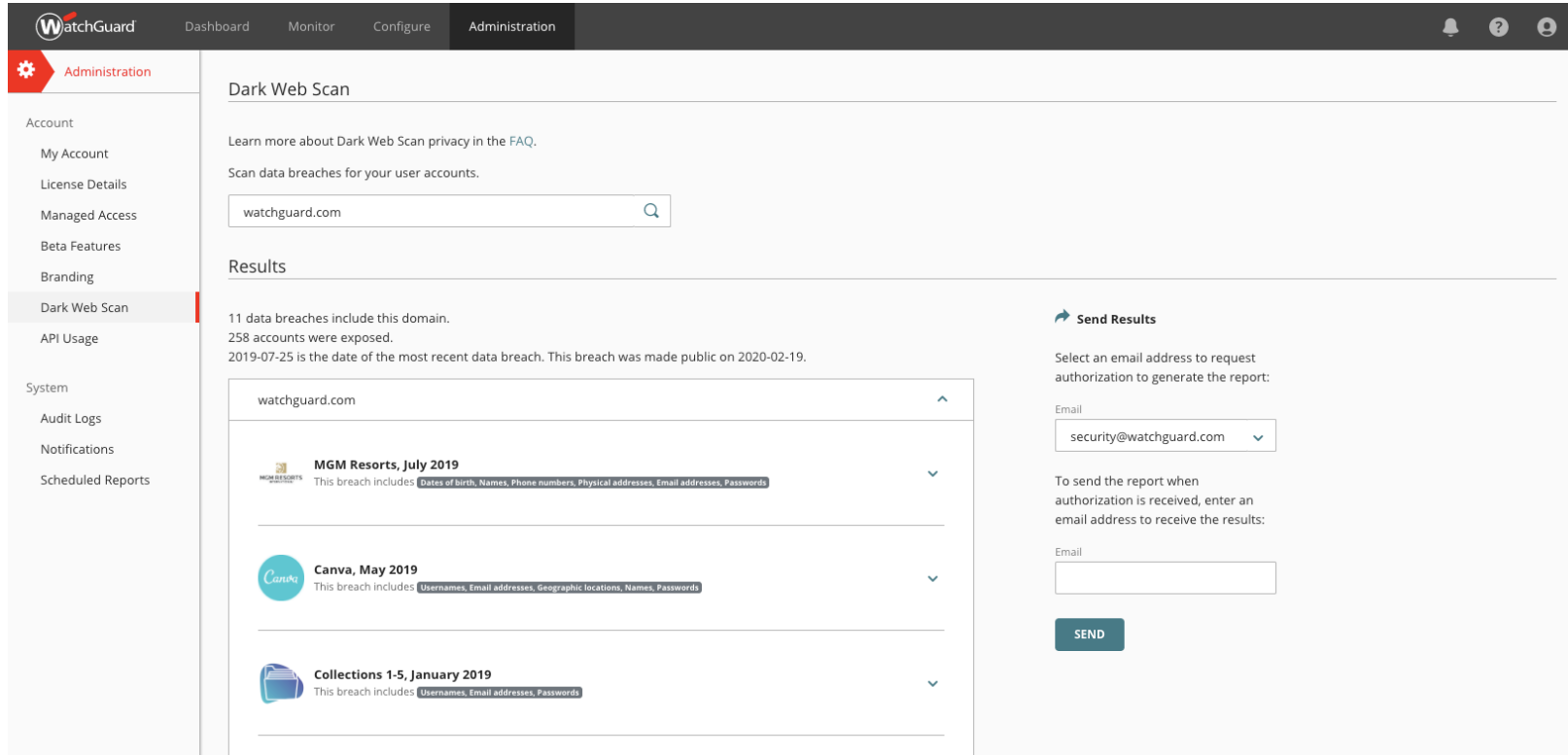
# **Introducing Dark Web Scan Available in WatchGuard Cloud**

# Scan Known Data Breaches from the Cloud

- Subscriber Account
  - Scan any email address
  - Scan company domain associated with user account
- Service Provider Account
  - Scan any email address
  - Scan any company domain, except for public ones (google.com; apple.com; microsoft.com, etc.)
  - Send personalized dark web reports to authorized admins and users



# Show prospects the importance of protecting credentials with MFA



The screenshot displays the WatchGuard Administration console. The left sidebar contains navigation links for Account, System, and various reports. The main content area is titled 'Dark Web Scan' and shows a search for 'watchguard.com'. Under the 'Results' section, it states that 11 data breaches include this domain, with 258 accounts exposed. A table lists three specific breaches: MGM Resorts (July 2019), Canva (May 2019), and Collections 1-5 (January 2019). Each entry includes a brief description of the exposed data. To the right, there is a 'Send Results' section with a dropdown menu for email selection (currently showing 'security@watchguard.com') and a 'SEND' button.

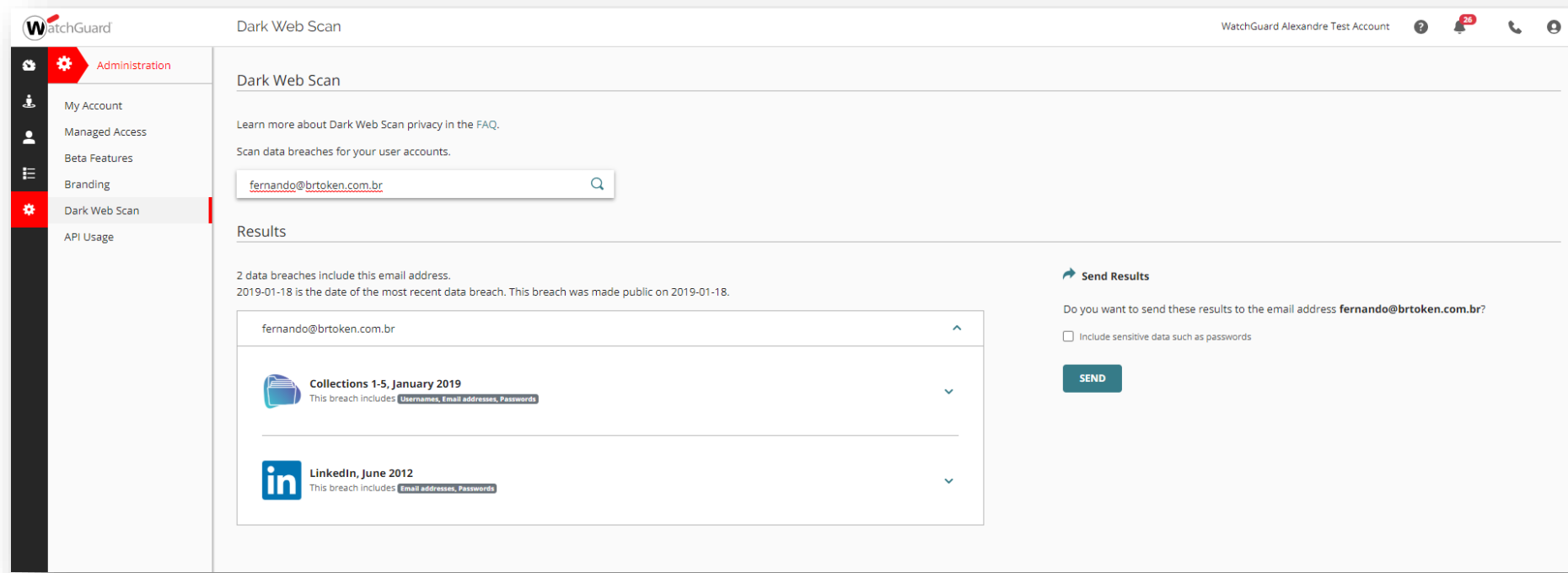
Breach Name	Date	Exposed Data
MGM Resorts	July 2019	Dates of birth, Names, Phone numbers, Physical addresses, Email addresses, Passwords
Canva	May 2019	Usernames, Email addresses, Geographic locations, Names, Passwords
Collections 1-5	January 2019	Usernames, Email addresses, Passwords

- Full domain scan including a non-sensitive information report
- Partner will see a list of breaches - with password exposure - that involved the searched domain
- Option to send the full report by email to someone from the same domain



# WatchGuard Dark Web Scan – Single Email Check

- Subscriber accounts can check their own domain
- Single email check available for anyone
- Optional: Send report by email with stolen passwords (first characters)



# Personalized Domain Reports

## Dark Web Scanner Results

Report generated 2020-05-11 18:12:47 UTC



### Personalized Report for watchguard.com

Hackers may choose to use the personal data they've stolen themselves, but many find it easier and more lucrative to sell it in one of the black markets on the dark web. Login credentials and other private data can be purchased by anyone with a Bitcoin account. Once stolen, there's no way to prevent your data from showing up on the dark web. The key is to prevent the data breach from ever happening and remove the possibility of attackers successfully authenticating with your stolen credentials.

### Summary

- 8 data breaches for **watchguard.com**
- 192 accounts have been breached
- 2019-07-25 is the date of the most recent breach

## Dark Web Scanner Results

Report generated 2020-05-11 18:12:47 UTC



### Breach Information



#### Collections 1-5

This breach included your Usernames, Email addresses, Passwords.

In early January, security researcher Troy Hunt identified a massive collection of usernames and passwords in plain text, which he subsequently dubbed 'Collection 1.' Shortly after, researchers found Collections 2-5 available on various underground forums on the dark web and not-so-darkweb. These collections contained records from multiple individual breaches over a 10 year timespan.



#### LinkedIn

This breach included your Email addresses, Passwords.

Cyber criminals hacked LinkedIn on June 5th, 2012, making off with 117 million user records including email addresses and hashed passwords



#### MyHeritage

This breach included your Email addresses, Passwords.

On June 4, 2018, MyHeritage's released a statement on their blog notifying their users that an external researcher had found a file on a private server containing the email addresses and hashed passwords of accounts created on the site up to October 26, 2017. The database subsequently appeared for sale on the dark web in 2019.



#### Dropbox


This breach included your Email addresses, Passwords.

In 2012, attackers made off with the email addresses and hashed passwords of over 68 million user accounts. Four years later, Dropbox announced it was forcing password resets for all affected users after finding the breached data available on a database trading community.

# Personalized Email Reports

Dark Web Scanner Results

Report generated 2020-05-09 12:43:50 UTC



Personalized Report for  
manishbalwada09@gmail.com

Hackers may choose to use the personal data they've stolen themselves, but many find it easier and more lucrative to sell it in one of the black markets on the dark web. Login credentials and other private data can be purchased by anyone with a Bitcoin account. Once stolen, there's no way to prevent your data from showing up on the dark web. The key is to prevent the data breach from ever happening and remove the possibility of attackers successfully authenticating with your stolen credentials.


Summary

- 1 data breaches for manishbalwada09@gmail.com
- 2019-01-18 is the date of the most recent breach


WatchGuard Technologies, Inc. | Page 1

Dark Web Scanner Results

Report generated 2020-05-09 12:43:50 UTC



Breach Information

 Collections 1-5

This breach included your Usernames, Email addresses, Passwords.


In early January, security researcher Troy Hunt identified a massive collection of usernames and passwords in plain text, which he subsequently dubbed 'Collection 1.' Shortly after, researchers found Collections 2-5 available on various underground forums on the dark web and not-so-darkweb. These collections contained records from multiple individual breaches over a 10 year timespan.

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit WatchGuard.com.

WatchGuard Technologies, Inc. | Page 2

Dark Web Scanner Results

Report generated 2020-05-11 18:12:47 UTC



Individual Email Accounts Breached

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Collections 1-5, LinkedIn

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Collections 1-5

manishbalwada09@gmail.com

- Canva

manishbalwada09@gmail.com

- Collections 1-5, LinkedIn, Myspace

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Collections 1-5

manishbalwada09@gmail.com

- Collections 1-5, LinkedIn

manishbalwada09@gmail.com

- Dropbox

manishbalwada09@gmail.com

- Collections 1-5, LinkedIn

manishbalwada09@gmail.com

- Dropbox, LinkedIn

manishbalwada09@gmail.com

- MyHeritage

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Collections 1-5, LinkedIn

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Dropbox

manishbalwada09@gmail.com

- Dropbox

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Collections 1-5, Forbes, LinkedIn

manishbalwada09@gmail.com

- Collections 1-5, LinkedIn

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- LinkedIn

manishbalwada09@gmail.com

- Dropbox

manishbalwada09@gmail.com

- LinkedIn





# **Selling More with Dark Web Scan Data**

# Marketing Tips to Sell More

Raise awareness among existing and potential customers with data from real breaches involving their company domains and employee credentials

- Bring scan results to meetings with prospects
- Offer free personalized dark web reports to your customers
- Host a webinar or live demo to review results with existing or potential customers







# **Important Reminders**

# Reminders

- Follow up with IT teams so they know to look for the confirmation email from WatchGuard Cloud
- For better delivery results, verify the right authorized email address before sending a report confirmation email
- The link in the confirmation email is only valid for one hour
- The only accounts that can authorize report delivery are:
  - [security@companydomain.com](mailto:security@companydomain.com)
  - [hostmaster@companydomain.com](mailto:hostmaster@companydomain.com)
  - [webmaster@companydomain.com](mailto:webmaster@companydomain.com)
  - [postmaster@companydomain.com](mailto:postmaster@companydomain.com)





# Frequently Asked Questions

## FAQ

- Q: Is this a WatchGuard service or is it powered by a third-party provider?
- A: The Dark Web Scan is 100% WatchGuard!
- Q: Can I search for any type of breach?
- A: WatchGuard's Dark Web Scan only shows on publicly available breaches that involve passwords. We don't capture breaches with credit cards, IDs, or other personal data. We also don't purchase breached databases. We only show data related to public breaches.

[Learn more about the WatchGuard  
Dark Web Scan in our FAQ](#)





# Partner Resources

# Partner Resources

## ■ Training Resources

- Watch On-demand demo recording
- Read User Guide
- Watch quick demo for Subscribers
- Read FAQ

## ■ Marketing Resources

- Email templates to reach customers and prospects
- Email signature
- Banner ads
- Pitch deck