Good Passwords for Bad Bots

Password Research Report

Tod Beardsley, Director of Research at Rapid7
Erick Galinkin, Principal Artificial Intelligence Researcher at Rapid7
Curt Barnard, Principal Security Researcher at Rapid7

RAPID7

CONTENTS

EXECUTIVE SUMMARY

This report details the types of credentials that are most often used by automated attackers to gain access to systems with SSH and RDP – the two most common protocols for remote access. These protocols are widely used for managing virtual machines in the cloud and thus, with the growing popularity of both cloud deployments and remote work, it is important to know how opportunistic attackers are targeting these systems. We find that the most common usernames are defaults that are built into operating systems and applications such as “root,” “administrator,” and “mysql.” However, the most commonly attempted passwords tend to be the well-known bad passwords: “123456,” “password,” “admin,” or simply no password at all!

While there are many password lists out there, we use rockyou2021.txt – a well-known password list used by pentesters and attackers. Notably, we found that of the nearly 500,000 unique passwords observed in our honeypots, this “rockyou set” contained practically all of them (99.997%). We conclude from this observation that online credential attackers are not generating truly random passwords, but are instead working entirely off of lists of guessable passwords.

Enterprise IT administrators can defend against these attacks by:

- Ensuring that default passwords for SSH and RDP servers, including those shipping with IoT and cloud solutions, are changed prior to deployment.
- Auditing SSH and RDP endpoints for default passwords with the help of the open-source Defaultinator database of default credentials.
- Encouraging a corporate culture of randomly-generated, strong passwords using commonly available password management solutions.
- Routinely scanning their internet presence from an external point of view to discover SSH and RDP endpoints using Doppler, Rapid7’s free-to-customers attack surface management (ASM) solution.

INTRODUCTION

With the increasing adoption of both remote work and cloud infrastructures, the number of people accessing corporate information systems across the internet has skyrocketed. Many of these systems leverage Remote Desktop Protocol (RDP) and Secure Shell (SSH) for interaction and management. As a result, the “walled garden” approach that once allowed companies to secure their perimeters and force employees to work only on corporate networks has faded, and the number of assets that employees connect to from untrusted networks has jumped. As with so many things in security, the addition of convenience and complexity has made the task of protecting these systems far more challenging.

In 2016, Rapid7 published the Attacker’s Dictionary, which looked at the RDP and found 221,203 connection attempts from 119 countries. In this exploration, we noted that by and large, attackers are not conducting truly random brute force attacks, but rather conducting dictionary attacks that are assumed to have a higher likelihood of success.

This report follows up and expands on that previous report, exploring not only RDP, but also connections to our SSH honeypots. We consider a year’s worth of username and password data gathered from Rapid7’s Project Heisenberg RDP and SSH honeypots between September 10, 2021 and September 9, 2022. During this time, we observed tens of millions of connection attempts to our honeypots. This captured 215,894 unique IP source addresses and 512,002 unique passwords across our RDP and SSH honeypots. Of those, 213,972 unique source IPs and 497,848 unique passwords were observed in the SSH honeypots. 2,030 unique source IPs and 22,690 unique passwords were observed in RDP.

This report is primarily concerned with two questions:

1. What has changed in RDP since 2016?
2. How does the most complete, most well-known dictionary used by attackers (the rockyou set) compare to the corpus of passwords in our honeypots?

The Rockyou Set

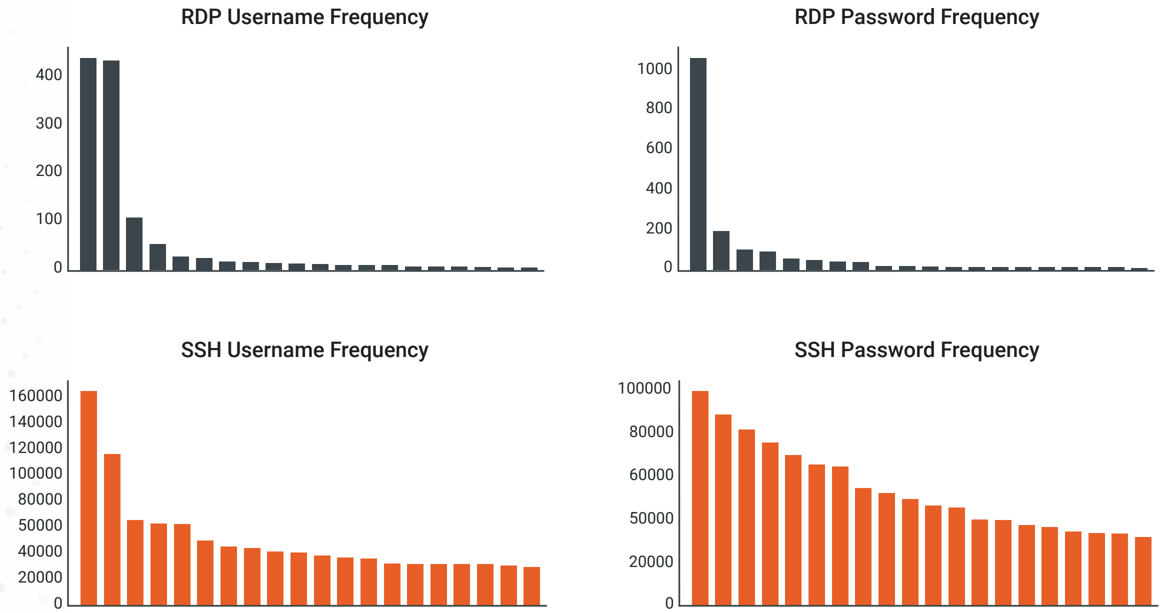
RockYou was a company that developed widgets and plugins for social media sites. Back in 2009, RockYou was hacked and the attackers found that passwords for the various user accounts were stored completely unencrypted. This resulted in the release of 14,341,564 passwords – the original "rockyou.txt" that is included with Kali Linux, a penetration testing-focused distribution of Linux. In the years since that release, many more lists of passwords have been compiled. This culminated in the release of rockyou2021.txt – an approximately 92 GB text file containing about 8.4 billion passwords that have been contained in leaks and dictionaries over the years, which we'll refer to as "the rockyou set." Though it is not included by default in Kali Linux, this updated version of the rockyou set has become a go-to source for all kinds of credential-related attacks, as many users continue to create and reuse passwords rather than using a password generator or password manager. We use the rockyou set as a source of passwords that attackers can trivially generate and try, to see if there is some evolution beyond the use of a password list.

FINDINGS

Overall, the distributions of SSH and RDP usernames show a marked preference for administrative accounts. Ignoring case, the three most popular usernames for RDP are "administrator," "user," and "admin," while the three most popular usernames for SSH are "root," "admin," and "nproc." The password lists for SSH and RDP differ, but classics like "admin," "password," "123456," and the empty string – no password at all – dominate the lists. Interestingly, we also find that there is a similar shape to the distribution of the lists – the first one or two entries dominate all the others, and then rapidly drop off. This is because many attackers are simply opportunistically trying a small handful of usernames and passwords, then moving on. In many cases, we see a single IP trying a single username and password – some of these IP addresses that try a single username and password (like 'root:root' or 'admin:admin') have been observed many times and are likely doing this in an automated way, possibly as part of a botnet.

A noteworthy observation is that in both protocols, the distribution of passwords follows an approximately exponential distribution; that is, passwords that are observed more frequently are observed exponentially more frequently than the less common passwords. The distribution is somewhat similar when it comes to usernames except that the two most common usernames in each protocol are huge outliers relative to the other attempted usernames.

Distribution of Usernames and Passwords (Note different Y axis)



RDP Username Frequency

RDP Password Frequency

SSH Username Frequency

SSH Password Frequency

Outliers and Defaults

Each protocol has two usernames that are huge outliers in terms of their frequency. For RDP, those usernames are "Administrator" and "administrator." Noting that usernames in RDP are case-insensitive, this is actually only one username, making it even more of an outlier in terms of frequency. This is likely due to the fact that RDP typically runs on Windows systems and the default local administrator account – the first account created during installation – is named "administrator."

For SSH, the two usernames that stand out are "root" and "admin" – a logical choice for attackers, as most Linux distributions ship with a user named "root," and "admin" is a common default user, especially for routers and IoT devices.

It is very common for malware, especially malware that targets IoT devices such as Mirai, to spread by attempting to authenticate with a device's default credentials. While recent variants tend to rely more heavily on incorporating exploits for publicly disclosed vulnerabilities, it is still possible to identify new sets of devices being targeted by these malware campaigns by mapping the credentials observed to a list of known defaults. It's for this reason that we developed Defaultinator, an open-source tool for searching through default credentials.

While the rockyou set does contain many common default passwords, it's important to note that a malicious actor using this credential file does not indicate that they are specifically targeting individual devices; however, the presence of so many default credentials in this popular data source should be enough reason to be vigilant about eliminating default credentials from devices you control.

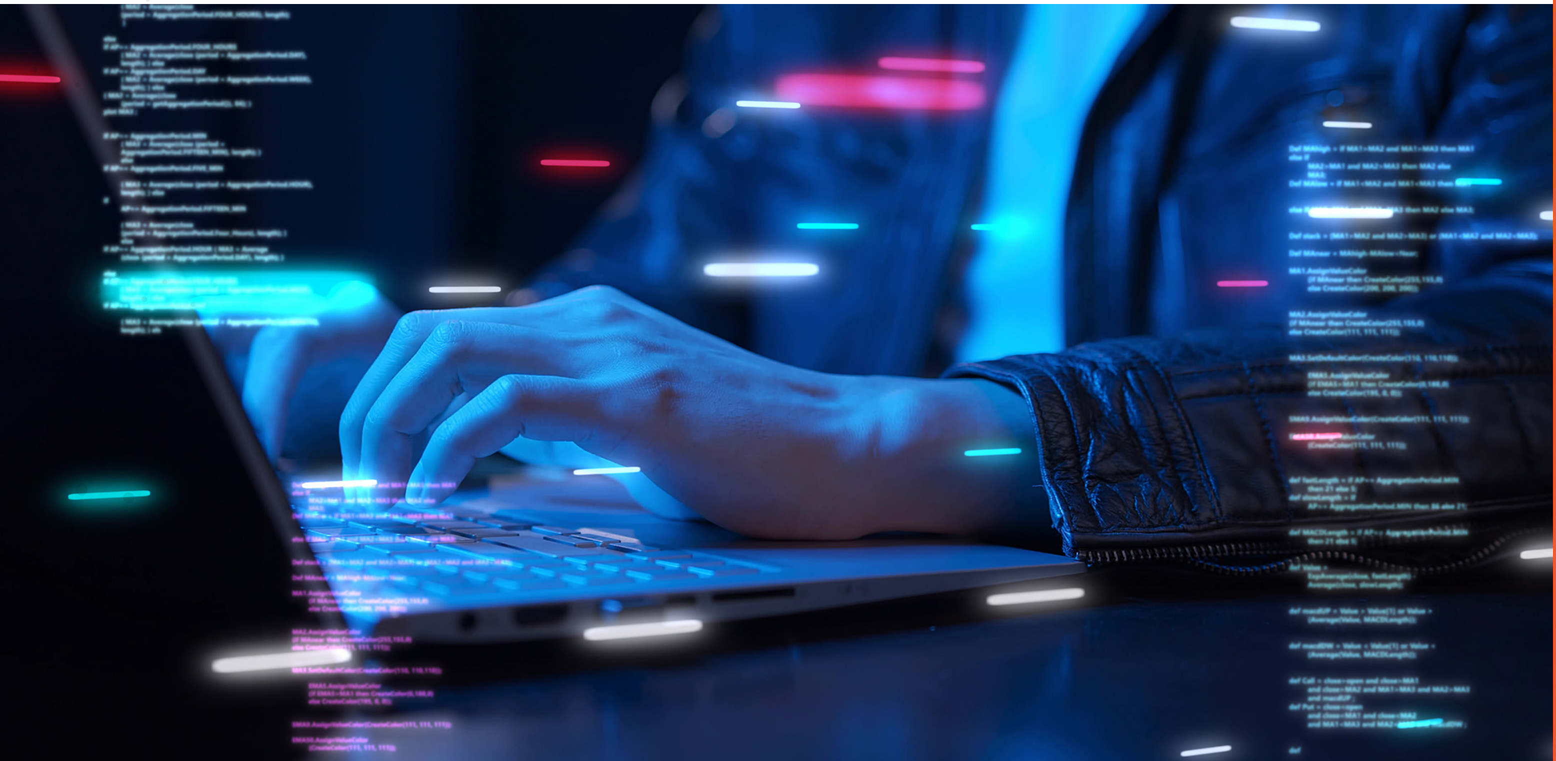
Secure Shell (SSH)

Of the 497,848 passwords observed in our SSH honeypots, by far and away, the passwords "123456" and "password" dominated the other entries. These, among other common default passwords, are an easy way for attackers to connect to a system. As mentioned in our discussion of the rockyou set, these passwords are easily guessable, and an attacker with any level of skill would easily be able to access a system with these passwords.

When we remove the rockyou set from our list of observed passwords, only 14 of the 497,848 passwords remain. All 14 of those remaining passwords contain the IP address of the honeypot and were observed only one time.[1]

While the rockyou set does contain a huge number of passwords, it's far short of the total universe of possible passwords. For example, a list of all possible passwords which are exactly seven characters long, built from all 95 possible printable ASCII characters, would be about 70 trillion (95^7) passwords long.

[1] The presence of these 14 passwords that contain IP addresses is pretty puzzling. After all, our honeypots are on dynamic IP addresses, so it would be odd for someone to intentionally set a static password to include a dynamic IP address. We're not sure if this is a feature of a particular device that an attacker was seeking out, or if this pattern of "<password><IP address>" is a programming error on the part of this particular scanner. The latter seems more likely.



This is a full four orders of magnitude larger than the entire roughly eight billion in the rockyou set, and doesn’t even consider six-, eight-, or 10-character passwords. If any automated attacker were spraying truly random passwords, it would have been obvious.

Below are the top 20 usernames and passwords attempted against SSH. So “root” is the most common username, followed by “admin” and ending with “minecraft” as the 20th most common, while “123456” is the most common password and “P@ssw0rd” is the 20th most common.

TOP 20 SSH USERNAMES

1. root
2. ubuntu
3. guest
4. hadoop
5. admin
6. postgres
7. support
8. ftp
9. nproc
10. oracle
11. mysql
12. nagios
13. user
14. ftpuser
15. testuser
16. deploy
17. test
18. git
19. user1
20. minecraft

TOP 20 SSH PASSWORDS

1. 123456
2. nproc
3. test
4. qwerty
5. password
6. 123
7. 12345678
8. 1qaz2wsx
9. 1234
10. root
11. 123456789
12. 123123
13. admin
14. ’ ’ (the empty string)
15. admin123
16. abc123
17. 12345
18. 1
19. admin1
20. P@ssw0rd

497,848

Remote Desktop Protocol (RDP)

RDP has long been a preferred target for threat actors. A number of breaches in the past several years are attributable to weak RDP authentication. Password spraying, brute force, and credential reuse on RDP are frequently cited by penetration testers as ways to gain initial access to a target. Moreover, in the past six years, a bevy of RDP-related vulnerabilities – CVE-2019-0708 (BlueKeep) most notorious among them – have cropped up, offering even more reasons for attackers to look for systems that have RDP's default port 3389 open.

One password that stands out among our top 20 is "AuToLoG2019.09.25" – searching for this exact string doesn't turn up much, but a number of malware samples with the "AuToLoG" string written into them crop up. The samples are classified as generic trojans by most antivirus vendors but appear to have RDP credentials hardcoded into them. This password, incidentally, is the only password that is not in the rockyou set.

TOP 20 RDP USERNAMES

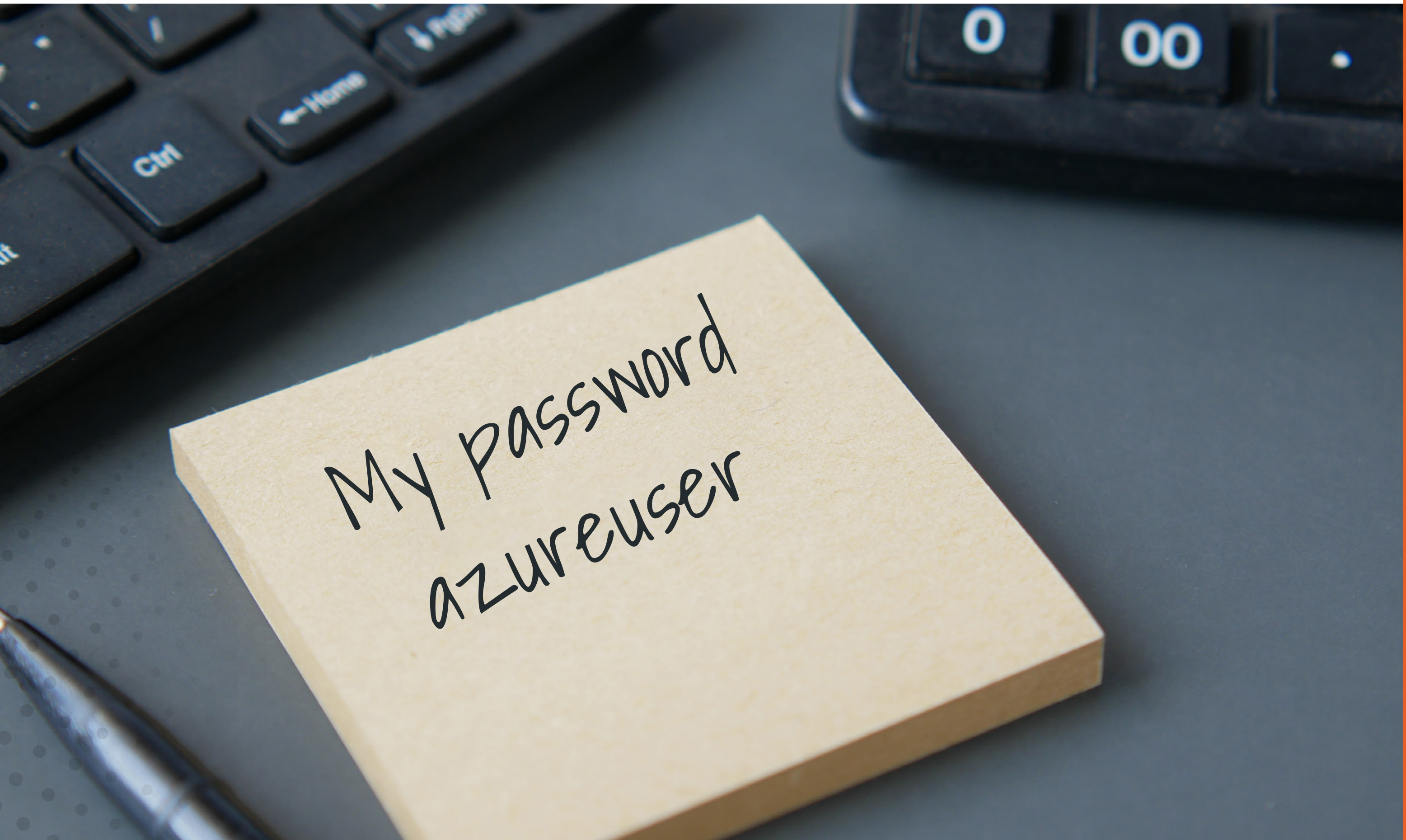
1. Administrator
2. root
3. Admin
4. guest
5. administrator
6. tor
7. Student
8. Administrador
9. user
10. user0
11. C
12. adminGG1
13. admin
14. test
15. Guest
16. rdp
17. 1
18. administrador
19. ‘‘(the empty string)
20. azureuser

TOP 20 RDP PASSWORDS

1. ‘‘(the empty string)
2. 123
3. password
4. 123qwe
5. admin
6. Administrator
7. root
8. qwe123
9. 123456
10. administrator
11. Aa123456
12. %username%
13. AuToLoG2019.09.25
14. !
15. admin@123
16. 1q2w3e
17. 1
18. %null%
19. administrador
20. !@#123

Changes from 2016

In 2016's "Attacker's Dictionary," we saw that the top two usernames for RDP were "administrator" and "Administrator," respectively. Though the ranking in 2022 is different, the association of RDP with Windows and the commonality of the "administrator" account on Windows means that these are liable to remain the top two – at least until attackers realize that the usernames are not case sensitive. After that, we see a dramatic drop off to user, admin, and tor. One noteworthy difference between 2016 and 2022 is our 20th most common username: "azureuser." Although Microsoft Azure was launched in 2010, cloud adoption in 2016 was less common than it is today and Azure was not as mature six years ago. As a result, it is not only the operating system and IoT defaults that attackers are beginning to target, but also cloud provider defaults.



RECOMMENDATIONS

This report has shown that in many ways, the landscape of guessing weak passwords to gain access to systems has not changed in a very long time. As a result, many of the recommendations here should feel familiar to readers, but given the number of times we have seen these techniques work against real victims, they clearly bear repeating.

Defeating Default Usernames

Although it is not nearly as effective against targeted attacks, the overwhelming majority of opportunistic attacks used a small number of guessable usernames – root, admin, administrator, and so on. Though it has been advised for a long time, disabling local administrator and guest accounts when possible can serve to shore up some of these weaknesses. This warning is especially important for IoT devices, where it is much easier to forget to change them (when it's possible at all for end users to change them), and for cloud deployments that may be short-lived (but long-lived enough to be guessed at).

Doing Better With Passwords

Users have dozens of accounts for which they need to remember passwords, leading to password reuse. Modern password managers like Bitwarden, 1Password, and LastPass fairly easily alleviate this problem, since they are able to generate random passwords for any number of applications and securely store them in an encrypted vault protected with modern cryptography. In the case where credentials are shared across multiple users – and that is ill-advised, but does happen – those vaults can be securely shared with other users. By using a password manager, you can generate a completely random password – one that isn't in the rockyou set – and have a different one for every website. This way, if one account is compromised, the others remain secure.

Securing RDP and SSH

RDP and SSH are both very commonly targeted by brute force authentication attempts. It's extremely important that best practices are followed when setting up these services. These best practices broadly cover limiting your external exposure and increasing the complexity of the authentication space.

To protect your enterprise from brute force attacks on these services, you may consider using a corporate VPN and restricting all remote connections to only work through VPN authenticated hosts. You may also choose to change the default port for these services. While changing the port falls under "security through obscurity," it would prevent you from being exposed to the vast majority of brute force attempts.

For RDP, the best protection is to restrict access via firewalls and network security groups so that instances with RDP exposed can be accessed only from trusted IP addresses. Using a jump host or a bastion host for cloud deployments is also a good practice in lieu of exposing RDP directly to the internet.

When securing SSH, the most important security measure you can take is to disable password-based authentication in favor of certificate-based authentication. It's also strongly advised to limit the users that have SSH enabled by modifying your sshd_config file. If you follow just these recommendations, you will already be much more protected against online brute force attempts, though there are a few other steps you could choose to take as well. It's generally a good idea to disable SSH for all root accounts. You can also change the number of max login attempts, or even use a plugin such as fail2ban that will automatically block sources that make too many authentication attempts.

External Monitoring

Once you believe your enterprise and cloud infrastructure is buttoned up against opportunistic online brute force attempts, it's always a good idea to verify your external attack surface when it comes to ports 22/TCP and 3389/TCP (SSH and RDP, respectively). After all, you've gone to the effort of checking your exposure today, but new services still pop up in modern networks from time to time. Routinely monitoring your public IP space through external scanning can alert you to (often well-meaning) "shadow IT" operations happening in your organization. Take that opportunity to quickly stop up gaps in your overall security posture.

POWER TO THE PROTECTORS

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attackers methods. Trusted by more than 10,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what’s next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CUSTOMER SUPPORT

Call +1.866.380.8113

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/