SYSPEACE

Prevents brute force attacks on Windows Servers

The Fight Against Hacking Attacks and Cybersecurity Threats

White Paper V01

Abstract

Today's work environment is entirely different from what it used to be a decade ago. Remote work culture and sophisticated cybersecurity threats are at the forefront of the minds of all businesses. Even as hacking attacks have been around for decades, it is unlikely to vanish anytime soon.

Already, remote work environments, the rise of mobile devices, and workforce solutions have created avenues for these attacks. The rise of botnets, scalable grids and cloud architectures, rapid adoption of artificial intelligence, and machine learning simplify and prioritize brute force processes. Therefore cyber-attacks are more sophisticated, elusive, and targeted than ever before.

It is paramount that all organizations take on a proactive stance against brute force attacks. One sure thing is that no organization, small or big, is immune from a devastating attack. This White paper explains brute force in detail, the shocking vulnerability in our security protocols. We will also offer insights on the timeline of 2020's significant brute force attacks and what is yet to come. In the end, we will provide the best solutions against brute force attacks.

Discover battle-tested brute force protection strategies using advanced technology, focusing on detection, prevention, or remediation.

Sweden HQ

Treetop Innovation AB
Hästholmsvägen 28
SE-131 30 Nacka
Sweden

New York, USA

295 Madison Avenue,
12th Floor
New York, NY, 10017
USA

Phone: 1-646-569-9114

Ottawa, Canada

Constitution Square
340 Albert Street, 13th Floor
Ottawa, Ontario
Canada K1R 7Y6

Phone: 1-613-686-3060

Table Of Contents

SYSPEACE

Prevents brute force attacks on Windows Servers

Problem Statement

Every minute, $2,900 000 is lost to cybercriminals, and top companies pay $25 per minute because of cybersecurity.[1]

Cybercrime has been rising at a blazing speed and is expected to grow further because of the unprecedented growth of technology and the increased number of connected devices. 2020 broke all previous records regarding the sheer number of cyber-attacks on individuals, businesses, and the government. Currently, cybercrimes grew by over 600%, with cyber-attacks such as malware, phishing attacks, DDoS attacks[2], man-in-the-middle attack, ransomware[3], and brute force attacks taking the lead.[4]

The sophistication of threats is rising at an alarming rate owing to the application of emerging technologies such as 5G, artificial intelligence, and machine learning, especially from higher tactical cooperation from state actors and hacker groups. A 2020 State of the Software Supply Chain report showed that cybercriminals now have 'next gen' supply chain attacks, which grew by 420% in just 12 months.[5] Therefore, every business must take proactive measures against hacking attacks. However, creating a robust security blueprint demands an in-depth understanding of all kinds of hacking attacks and cybersecurity threats.

Background: Hacking and Brute Force Attacks

A hacking attack on any computer or computer network is an attempt to alter, disable, destroy, steal, expose, or gain information using unauthorized access. Hacking attacks have been rising within the last decade, with malware attacks, brute force attacks, credential stuffing, and phishing attacks as the most common types.

Brute force attacks primarily focus on computers and other devices on networks to capture usernames, email addresses, passphrases, and PINs. Unlike many other cyber-attacks, brute force attacks do not depend on complex or sophisticated methods.

Attackers do not also have to look for vulnerabilities in the security system. They don't search for backdoors, control, or command functionalities. They merely rely on the psychology of humans and the use of weak and guessable credentials.

Hackers are attracted to brute force attempts because many businesses fail to take all necessary endpoint security precautions. Even when we have suitable security measures protecting databases and networks, our security measures are not working if employees log into these systems using unsecured laptops and routers.

Brute Force Attack Versus Other Cyber-Attacks

Over 80% of breaches caused by hacking involve brute force or using lost or stolen passwords.[6]

A brute force attack is a method of attempting to crack the username and password of accounts using a trial-and-error basis. This attack system is very old but still as effective and popular among hackers.

Brute force is a numbers game, and although the attacker is unlikely to gain access at the first, second, and third attempt, with enough attempts, it might happen.

For instance, many people use passwords with eight characters; usually, a combination of alphabetic and numeric characters, which means 62 possibilities for a given character in a password chain, and 62 options for every character results in 2.18 trillion possible combinations for an eight-character password which is plenty of combinations for a cyberattacker to try.

However, a hacker trying to hack an eight-character password using one attempt per second and go through all possible combinations would require seven million years and an unbelievable amount of computational power. Even 1000 combinations per second results require seven thousand years: therefore, making brute force attacks in the past not nearly as effective.

Nevertheless, today's hackers can access automated cracking tools backed by many innovative technologies, making an enormous number of combinations per second possible. This means attackers can now attempt thousands of combinations in seconds, and in a matter of months, can decrypt a weak encryption hash using exhaustive key search brute force attack.

Organizations usually seek to improve security by setting up two-factor or multiple-factor authentication, putting the website behind a web application firewall (WAF), installing a virtual private network (VPN) gateway to broker all RDP connections outside their local network and encrypting data on devices used for work. Organizations also include digital security training for employees as their measures against security threats.

However, all these are futile against hacking, and brute force attacks since VPN connections, WAF, and firewalls only serve to make freeway to the log-in prompt that hackers can exploit freely.

Types of Brute Force Attacks

Dictionary attack
Attack using words and combinations from a dictionary of possible words and tests usually from other breaches.

Simple or traditional brute force attack
An Attacker attempts an unlimited number of combinations to access local files. The higher the scale of the attack, the higher the chances of success.

Hybrid brute force attack
It combines different brute force attack types, such as traditional brute force and dictionary attacks.

Reverse brute force attack
This kind of attack switches the method of guessing passwords for using a generic list of passwords to try and find usernames.

Credential recycling
The attacker uses stolen passwords and usernames from sites and services to hijack other applications and services.

Rainbow table attacks
Rainbow table attacks do not target passwords. Instead, it involves a pre-computed dictionary of plaintext passwords and their corresponding hash values. When a user enters a password, it changes to a hash value. If the hash value inputted password matches the stored hash value, the user authenticates. Therefore, hackers use this dictionary to uncover which plain text passwords give rise to a specific hash and expose them.

The Impact of a Successful Brute Force Attack

Research shows that it only takes one data breach to create diverse adverse implications for any business.[7] Hackers often use brute force attacks during initial reconnaissance and infiltration. They can easily automate brute force attacks and even run them parallel to maximize their chances of cracking credentials. However, that is not where their actions stop.

They can:

- ruin website reputation,
- launch a DDoS attack,
- infect websites with activity-tracking malware, which is subsequently sold to advertisers,
- gain personal data and valuables,
- spread malware to cause disruptions, and
- hijack the system for other malicious purposes.

Once they gain access to a system, attackers will attempt to move laterally to other systems, gain advanced privileges, or run encryption downgrade attacks. Their end goal – is simply endless.

Top 10 most valuable information to cyber criminals	Top 10 biggest cyber threats to organizations
1. Customer information (17%)	1. Phishing (22%)
2. Financial information (12%)	2. Malware (20%)
3. Strategic plans (12%)	3. Cyberattacks (to disrupt) (13%)
4. Board member information (11%)	4. Cyberattacks (to steal money) (12%)
5. Customer passwords (11%)	5. Fraud (10%)
6. R&D information (9%)	6. Cyberattacks (to steal IP) (8%)
7. M&A information (8%)	7. Spam (6%)
8. Intellectual property (6%)	8. Internal attacks (5%)
9. Non-patented IP (5%)	9. Natural disasters (2%)
10. Supplier information (5%)	10. Espionage (2%)

Figure 1 - EY Global Information Security Survey 2018 - 2019 [8]

The True Cost of Brute Force Attack – Password Security

The effectiveness of Brute Force attack is really about the password and other credentials attackers can access. Compromised passwords are arguably highly dangerous than exploits like denial-of-service (DoS), which can disable systems, but our responsiveness to the situation may mitigate the effects. Compromised passwords, in contrast, allow the hacker to take over a person's identity. This means they can access customer information, trade secrets, customer information, and passwords to other critical systems.

Hackers can use passwords also to read emails of a company executive. Suppose the company data breach involves customer information. In that case, the costs can be high, first in terms of hefty fines, secondly damage to the company's reputation and subsequent loss in sales, customers, and lots more.

For instance, data breaches can lead to a loss in stock prices. Research showed a 0.43% expected drop in share price following a breach.[9] Furthermore, breaches involving credit card and social security numbers register a more notable negative impact on share prices than leaks with less sensitive information such as email addresses. Nevertheless, internet businesses (social media, e-commerce, etc.) endure long-term effects in share price (although financial organizations endure an immediate decline).

In the Numbers

Hacking attempts brings about a myriad of adverse impacts. Here are some statistics corroborating the need to prevent them.

Global Cybercrime Damage Costs:

$6 Trillion USD a Year.*
$500 Billion a Month.
$115.4 Billion a Week.
$16.4 Billion a Day.
$684.9 Million an Hour.
$11.4 Million a minute.
$190,000 a Second.

* Source: Cybersecurity Ventures

- Malicious hackers are now attacking computers and networks at the rate of one attack every 39 seconds.[10]
- The average cost of a breach in the US costs $8.64 million.[11] Across the globe; the cost is $6 trillion a year.
- 63% of network intrusions are the results of comprised usernames and user passwords
- Over 40% of global log-inn attempts are malicious due to the growth in bot-driven credential stuffing attacks.[12]
- About 62% of data breaches not involving misuse, physical action, and error involved stolen credentials, phishing, or brute force.[13]

ROI calculation:
The Cost of Hacking Attacks

Due to the rising sophistication of hacking attacks, cybersecurity budgets are increasing rapidly to meet this threat effectively. However, understanding the actual cost of attacks on the organization is highly important.

As adopted by CSO Online[14], let us create a hypothetical situation of the budget required to protect the front-end of a medium-sized e-commerce website. We will not also consider the higher level of advanced hacking and brute force attacks becoming more prevalent.[15]

First, we consider what an annual loss would look like using the Annual Loss Expectancy and following the CISSP®-ISSMP® guideline:[16]

Annual Loss Expectancy (ALE) = (Number of Incidents per year) X (Potential loss per incident)

We will set the number of incidents per year to 12, estimating one serious intrusion attempt per month. We can apparently go higher, especially for financial, healthcare, and retail industries where the stakes are higher.

However, estimating potential loss is a lot trickier. This would require considering both tangible and intangible costs. Tangible costs would be actual money spent on repair and containment. In contrast, intangible costs include operational disruption, stock options drop, compromised assets, lost business reputation, increase customer turnover, and lost business revenue.

Naturally, the intangibles lead to a higher loss on any enterprise. They are especially threatening for smaller businesses, but they are also more challenging to calculate[17] and highly unique to every business.

However, we would try to consider an average cost per breach using evidence from a reputable source. A new report from IBM and the Ponemon Institute suggests that the average price of a data breach in 2020 is $3.86 million.[18]

On many occasions, it's easy for management to question such an enormous amount since; the company may be inherently smaller. However, for SMBs, we will use a different figure from another reputable source. According to Security Magazine[19] , the average cost of a data breach is about $36,000 to $50,000, with $38,000 as the average.

Hence, in the case of the e-commerce website, we will consider $38,000 as the average and can identify what these losses would include:

- cost of e-commerce website being unavailable during recovery and audit,
- cost of third party experts to investigate and remediate the breach,
- cost of customer database and other sensitive information exposure, and
- cost of compliance and legal fines.

Naturally, it's easier to calculate the cost of paying third-party experts and some compliance costs. However, in July 2019, the Marriot hotel chain paid a $124 million fine for GDPR compliance failures for a breach that initially cost $28 million that was also mostly covered by the company's insurance. The whopping fine, which was paid out of pocket, would significantly cost disruption in business growth.[20]

Some other costs, such as the cost of a lost record, may be easy to calculate, currently at $146 per record, with customer PII records as the most expensive type of record to lose and the most involved in 80% of breaches. Now that we have ideas about different breaches in different situations, let's continue with the modest cost of $38,000, which we will directly input into the ALE formula.

ALE = (Number of Incidents per Year) X (Potential Loss per Incident)

ALE = 12 X $38,000 = $456,000

Therefore, this would be the amount a small business could potentially lose if it does nothing to protect only its front-end. Protecting the front-end would also usually require a) firewalls, b) anti-virus, c) security vulnerability scanning, and d) real-time monitoring, amongst others.

Taking a cue from CSO Online, we could estimate the overall cost of using all four solutions to be $40,000 per year. Now we go back to our equation and calculate ROI using the official guide to CISSP®-ISSMP®:

ROI: (ALE/Cost of Protective measures) X 100%

ROI = ($456,000/$40,000) X 100% = 1140%

However, even with the vast ROI, we must not forget that cybersecurity is not just a reflection of earnings regarding loss prevention and risk management but about defending what's most valuable to us. Let's also consider the higher costs of intangibles which have the higher possibilities of crippling a business for good. There is no doubt that we must have robust security protection.

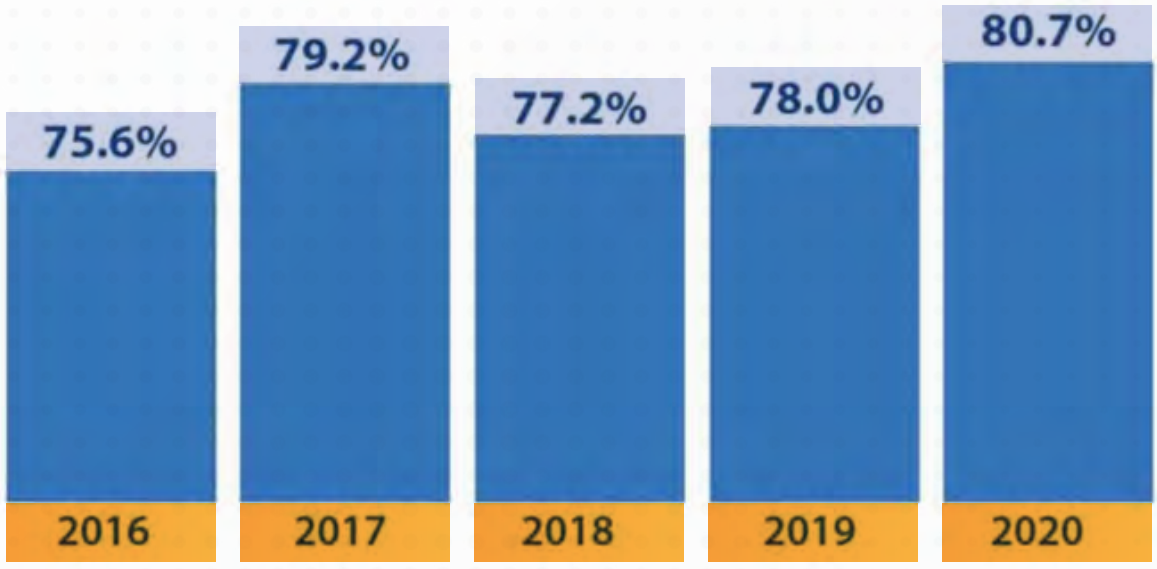


Figure 1 - Percentage compromised by at least one successful attack by year (CyberEdge Group 2020 Cyberthreat Defense Report)

Firewalls and Anti-Virus
Are Not the Answers

Because of the COVID-19 pandemic, the shift to remote work has also created more tempting opportunities for brute force attacks. This is because server and network administrators have been forced to log in to vital systems remotely. They often also lack all the extra layers of protection that their enterprise systems and offices would have provided. Attackers attempt to exploit the Windows remote desktop protocol (RDP) used by network administrators to manage Windows systems remotely. This is why remote work during the COVID-19 increased data breach to cost around $137,000.[21]

In April 2020, Kaspersky reported that the number of brute force attacks on Remote Desktop protocols (RDP) increased by 400 percent in March and April.[22]

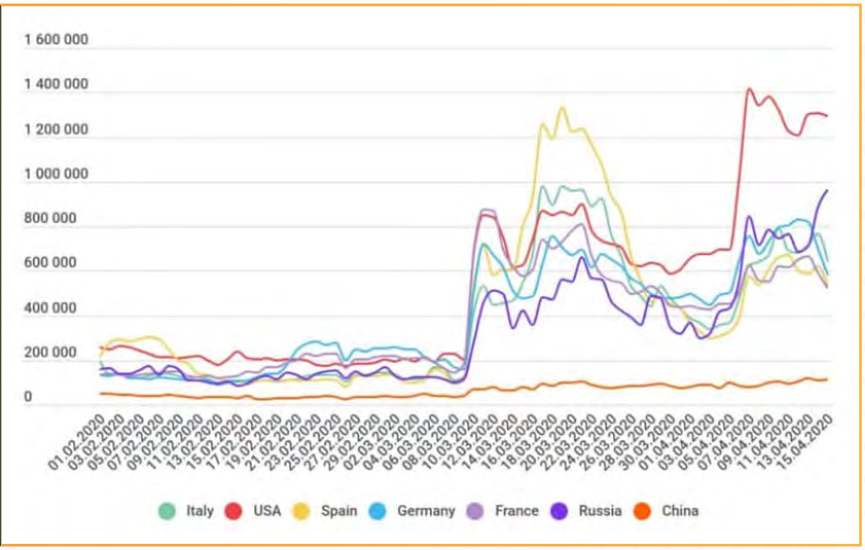


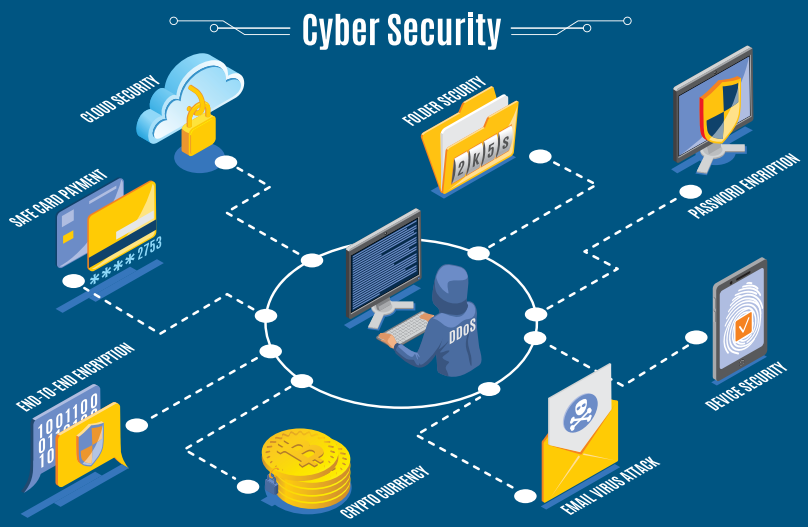
Figure 2 - Source – Kaspersky [23]

However, even with robust firewall and virus solutions, we often use vulnerable and guessable passwords, which is the driving force behind the success of many brute-force attacks.

Paired with the vast number of automated tools attackers use for brute force attacks, warfare gets complicated. As said earlier, they now have tools that can allow them rapidly every possible password alongside workaround programs that can crack wireless modems, identify weak passwords, work against computer protocols (like MySQL, SMPT, FTP, and Telnet), translate words into leetspeak, and run all possible combinations of characters. Some of these tools can pre-compute rainbow tables for known hash functions, which speeds up the process of brute force attacks.

Therefore, it is paramount to implement brute-force-oriented solutions to combat brute force attacks and mitigate all negative influences. To cover what firewalls and anti-virus cannot.

How to Mitigate a Brute Force Attack



Catching and neutralizing a brute-force attack in progress is an excellent measure but preventing the attack from happening in the first place is the best. Once attackers have access to a network, they are much harder to find. They can work undetected for a long time.

Protection against brute force is vital for protecting company data and valuables to avoid hackers hijacking systems for malicious activity.

The first step to protecting our passwords and entire networks from the brute force is to take precautions by reinventing our behavior and network security systems.

For users and IT specialists alike, we need to implement these actions with strict adherence.

Operational strategies and policies

- **REAL-TIME MONITORING:** Active monitoring is critical to catch a Brute force item. We must be on the lookout for odd log-in locations, excessive log-in attempts, and other anomalous behavior that shows something suspicious is happening. For Windows servers, enable logging of failed log-in events and monitor the event log.
- **VPN GATEWAYS:** Even as placing websites and other connected devices and applications behind firewalls is not enough, they are just as important. However, we need to take a step further to invest in VPN gateways. This gateway will broker all RDP connections outside the local network and encrypt data on devices used for work.
- **LIMIT EMPLOYEE ACCESS:** Take steps towards implementing a zero-trust cybersecurity strategy to ensure that only people within our network have access.
- **PASSWORD EDUCATION:** e need to educate our people about safe password practices. We should also provide tools that can help them save their complex, hard-to-remember passwords and keep track of them. The best passwords should be about 127 characters and are called passphrases.[24] This training should extend beyond passwords to every crucial detail about digital security.
- **MULTI-FACTOR AUTHENTICATION:** Consider setting up two-step and multi-step authentication to help fight brute force attacks.

Backend preparation

- **HIGH ENCRYPTION RATES:** We need to ensure that passwords for systems are encrypted with the highest encryption rates possible (e.g., 25-bit encryption), which would make them more challenging to crack.
- **USE AN IP DENY LIST (GLOBAL BLACKLIST):** Check out lists of known attackers that are constantly updated and use these lists to block out unsuccessful log-in attempts.
- **SALT THE HASH:** Administrators often randomize password hashes by adding random strings of numbers and letters (known as salt) to the password itself. This string would be stored in a different database and retrieved and added to passwords before hashed. Salting the hash ensures that users can use the same password with different hashes.
- **MAKE THE ROOT USER INACCESSIBLE VIA SSH** by editing the sshd_config file. Set the 'PermitRootLogin no' and 'DenyUsers root' and options.

Technical solutions to hinder an ongoing attack

- **ACCOUNT LOCKDOWN AFTER EXCESSIVE LOG-IN ATTEMPTS:** A temporary lockout or using short lockout timers may be convenient for users, but that convenience can become a vulnerability. Consider using a complete lockout that requires users to contact the support, especially after several failed log-ins and short lockout.
- **USE DELAY AFTER REPEATED LOG-INS:** We can further slow down the attacker's efforts by adding time gaps between log-in attempts. This lag time, alongside real-time monitoring systems, can help provide ample opportunities to stop the attack as quickly as possible.
- **CAPTCHA AFTER REPEATED LOG-INS:** Consider manual verification using captcha. However, don't forget that captcha alone is not practical since there are now bots around the system.

Although using the methods we outlined seems to offer some relief, they are not enough. Some of these techniques we outlined above can and have been compromised in the past by these perpetrators. A good example is locking accounts. Account lockout for an hour or until manually unlocked by an administrator can be abused by the attacker to cause a denial of service (DoS) by locking out many accounts. Attackers can also cause a diversion by locking out many accounts and overwhelming the support team with calls. Attackers with targeted individuals using a slow attack can be ready to wait a few hours until they hit the jackpot.

Perpetrators can launch wide-scale attacks by trying single passwords on several thousand servers. This method will ultimately prevent the trigger for that account lockout and cleverly bypass such a defensive mechanism. Powerful accounts such as the administrator accounts can be used to bypass the lockout policy[25] – the list is endless!

Who Can Help You?

Therefore, we need to actively implement dedicated access control, a brute-force protection solutions offered by seasoned professionals to protect valuable assets from brute force attacks.

There are only a handful of companies offering reliable server protection for brute force attacks and specifically.

The right solution should actively monitor patterns of failed log-in attempts, discern the difference between attacks and legitimate user log-ins to offer the best solution against brute force attempts. The best solution should be:

- **EFFECTIVE**
  Dedicated to brute force protection to be used as part of a puzzle to a bigger cybersecurity umbrella.
- **SCALABLE**
  The right solution should be tailored to every organization's specific need to ensure you only pay for what you need. That way, you can enjoy a security solution that grows and scales with your changing business needs.

What To Look For In Companies That Can Help You?

Only around 21% of security professionals think their current security controls are adequate.[26]

- **DEDICATION –** They should offer references to help gauge their expertise, reliability, responsiveness, and performance. This also includes having the proper industry-standard credentials and qualifications to ensure that their dedication to helping their clients have the best protection against brute force is authentic.
- **LONG-TERM SUCCESS –** The best brute force protection firm should have years of experience on top of a portfolio of services to meet their customer needs. They should offer evidence of customer success through case studies, which shows precisely how they have backed their customers with proven results. They should also desire to work with your organization as a partner for years to come.
- **BATTLE PROVEN TECHNOLOGY –** Top-rated security agencies should have battle-tested tools. They should have relevant examples of 'war stories' encompassing all current trends and provide details on how their technological tools and solutions can help protect against brute force attacks.

- **PROFESSIONAL AND ACCURATE SUPPORT –** Technical issues are inevitable. They should offer cybersecurity experts as active support personnel to provide all the guidance and directions you need. If they lack interpersonal or technical skills, there is a greater danger of financial losses, cyber-attacks, and damage to your reputation. They should provide detailed guidelines on their products, why they use them, and how they will integrate them with our systems. They should also help us understand if any products have overlapping features or gaps that might create vulnerabilities for dangerous threats. They should be knowledgeable of past, current, and potential future threats, alongside technological solutions to combat such threats. To be effective, they should have leading security experts who stay up-to-date on attackers' latest trends and techniques.

- **REAL-TIME MONITORING TO OBSERVE PATTERNS**

  Internet-facing servers – global threat from other entities.

  Brute force protection actively observes log-in attempts across all global users to develop behavioral profiles of users and detect threats. At the same time, analyzing perimeter activities from VPN, DNS, and web proxy, alongside data, email, and active directory behavior to continuously learn and adapt to behaviors specific to the organization. The proper brute force protection should expand your field of vision.

  Servers within the company – internal threat from employees and "secured" remote PC:s that use VPN to connect to the company network.

  Brute force protection tools can build a behavioral profile of all system accounts (insider) while analyzing perimeter activities from VPN, DNS, and web proxy, alongside data, email, and active directory behavior to continuously learn and adapt to behaviors specific to the organization to detect suspicious activities on time. It would also systematically pull back permissions to sensitive data, helping augment your privileged management solutions for more effective control over the activity of privileged users.

Conclusion

There is no doubt that brute force is unlikely to vanish anytime soon. It is becoming more apparent that brute force attacks will only become more prevalent and effective. In the rapidly evolving digital environment we live in, this growth will only be a few years.[27] Therefore the future of our organization rests on being able to act now. We need to stay on our toes and clear-eyed about fighting this menace.

References

1. Riskiq (2019). The Evil Internet Minute 2019: https://www.riskiq.com/resources/infographic/evil-internet-minute-2019/ Retrieved 24 May 2021.

2. Help Net Security (2020). 4.83 million DDoS attacks took place in the first half of 2020, a 15% increase: https://www.helpnetsecurity.com/2020/09/30/4-83-million-ddos-attacks-first-half-of-2020/ Retrieved 24 May 2021.

3. Skybox Security (2021). Vulnerability and threat trends report 2021; Cybersecurity comes of age. https://lp.skyboxsecurity.com/rs/440-MPQ-510/images/Skybox-Security-vulnerability-and-threat-trends-report-2021.pdf. Retrieved 24 May 2021.

4. Pacag, Homer (2020). Multiple Phishing Attacks Discovered using the Coronavirus Theme: https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/multiple-phishing-attacks-discovered-using-the-coronavirus-theme/ Retrieved 24 May 2021.

5. Sonatype (2020). State of the Software Supply Chain 2020 Report: https://www.sonatype.com/2020ssc Retrieved 24 May 2021.

6. Patel, Deepak & Pestana, Eric (2020). Q & A: Top threats in 2020 Featuring Research from Forrester. https://www.perimeterx.com/resources/blog/2020/q-a-top-threats-in-2020-featuring-research-from-forrester/ Retrieved 23 May 2021.

7. Mangat, Monia (2020). 89 Eye-opening Data breach statistics for 2020. https://phoenixnap.com/blog/data-breach-statistics. Retrieved 23 May 2021.

8. EY Global Information Security Survey 2018-19 (2019). Is Cybersecurity about more than protection? https://assets.ey.com/content/dam/ey-sites/ey-com/en_ca/topics/advisory/ey-global-information-security-survey-2018-19.pdf Retrieved 23 May 2021.

9. Bischoff, Paul (2021). How data breaches affect stock market prices. https://www.comparitech.com/blog/information-security/data-breach-share-price/ Retrieved 23 May 2021.

10. Cukier, Michel (2020). Hackers Attack Every 39 seconds: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. Retrieved 22 May 2021.

11. IBM Security (2020). Cost of a Data Breach Report 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/en/pdf IBM Security, Retrieved 22 May 2021.

12. Akamai (2017). State of the Internet Security Q4 2017 Report ,https://www.akamai.com/it/it/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, Retrieved 23 May 2021

13. Varonis (2021). 2021 Financial Data risk report, https://info.varonis.com/hubfs/docs/research_reports/2021-Financial-Data-Risk-Report.pdf. Retrieved 23 May 2021.

14. Kolochenko, Illia (2015). How to calculate your ROI and justify your cybersecurity budget, https://www.csoonline.com/article/3010007/how-to-calculate-roi-and-justify-your-cybersecurity-budget.html. Retrieved 23 May 2021.

15. Kolochenko, Illia (2015). Modern APTs at your corporate website, https://www.csoonline.com/article/2950049/modern-apts-start-at-your-corporate-website.html. Retrieved 23 May 2021.

16. (ISC)² Inc. /Steinberg, Joseph (editor) (2015). Official (ISC)², Guide to the CISSP-ISSMP CBK. 2nd Edition. CRC Press Taylor & Francis Group. https://www.isc2.org/issmp

17. Schmeidler, Netta (2016). Calculating your cybersecurity ROI, https://blog.morphisec.com/calculating-your-cyber-security-roi. Retrieved 23 May 2021.

18. IBM Security (2020) Cost of a Data Breach Report 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/en/pdf IBM Security. Retrieved 22 May 2021.

19. Khanfar, Marwan (2017). The average cost of a data breach, https://www.curotec.com/insights/cost-of-a-data-breach-2018/#:~:text=According%20to%20Security%20Magazine%2C%20the,able%20to%20absorb%20these%20costs. Retrieved 22 May 2021.

20. Swinhoe, Dan (2021). The biggest data breach fines, penalties, and settlements so far https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html Retrieved 22 May 2021.

21. IBM Security (2020). Cost of a Data Breach Report 2020, https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/en/pdf IBM Security. Retrieved 22 May 2021.

22. Gewirtz, David (2020). COVID cybercrime: 10 disturbing statistics to keep you awake tonight: https://www.zdnet.com/article/ten-disturbing-coronavirus-related-cybercrime-statistics-to-keep-you-awake-tonight/ Retrieved 22 May 2021.

23. Securelist (2020). Remote spring; the rise of RDP bruteforce attacks: https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820/ Retrieved 23 May 2021.

24. Lundin, Leigh (2013). "PINs and Passwords, Part 2". Passwords. Orlando: SleuthSayers

25. Esheridan (2020) Blocking brute force attacks, https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks. Retrieved 23 May 2021.

26. Forrester Consulting (2020). How to investigate and mitigate brute force attacks: https://www.armis.com/resources/analyst-reports/forrester-state-of-enterprise-iot-security-in-north-america-unmanaged-and-unsecured-tlp, Armis Retrieved 24 May 2021.

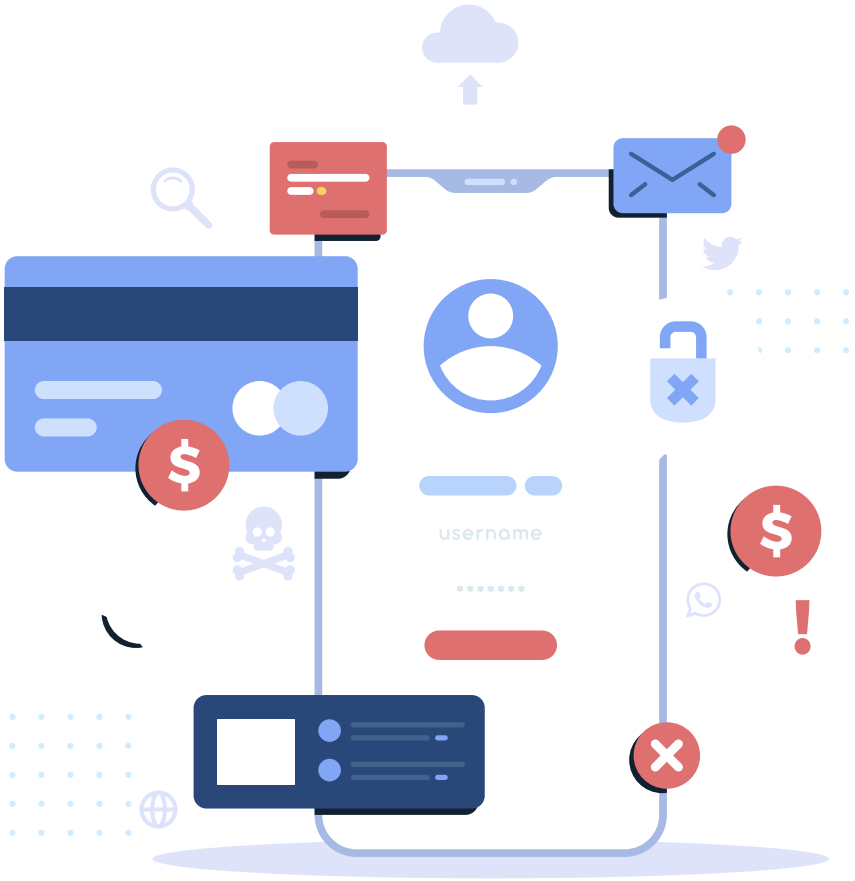
27. Gross, Garrett (2020). State of Enterprise IoT Security in North America: Unmanaged and Unsecured: https://cybersecurity.att.com/blogs/security-essentials/brute-force-attack-mitigation-methods-best-practices. Retrieved 23 May 2021.

Recommended Reading

1. What's the New Cost in the 2020 Cost of a Data Breach (https://securityintelligence.com/posts/whats-new-2020-cost-of-a-data-breach-report/)
2. Security ROI (Fact or Fiction) (https://www.csoonline.com/article/2123096/security-roi–fact-or-fiction-.html)
3. Cybersecurity Statistics (https://purplesec.us/resources/cyber-security-statistics/)
4. Vulnerability and threats trend reports 2021 (https://www.skyboxsecurity.com/trends-report/)
5. The Cost of a Data Breach Report 2020 (https://www.ibm.com/security/data-breach)
6. Remote Spring: The Rise of RDP Brute force attacks (https://securelist.com/remote-spring-the-rise-of-rdp-bruteforce-attacks/96820)
7. State of Enterprise IoT Security In North America: Unmanaged and Unsecured (State of Enterprise IoT Security in North America: Unmanaged and Unsecured: https://cybersecurity.att.com/blogs/security-essentials/brute-force-attack-mitigation-methods-best-practices)

SYSPEACE

Prevents brute force attacks on Windows Servers



www.syspeace.com