BEYOND IDENTITY

Whitepaper

RANSOMWARE: PREVENTION IS THE NEW RECOVERY

BEYOND IDENTITY

Contents

BEYOND IDENTITY

Executive summary

Ransomware is an increasingly serious problem that is no longer only limited to the biggest organizations. Over the past several years, attackers have increasingly turned to smaller targets, many of which haven't changed their security posture in response to modern threats.

In the first three months of 2021, nearly 300 firms were targeted, demanding ransoms totalling $45 million.[1] With platforms like Ransomware-as-a-Service (RaaS) making it extremely easy to launch attacks, the problem will only worsen. With ransomware recovery costs skyrocketing, preventing these attacks in the first place should be a priority for organizations large and small.

We propose eliminating the password altogether. The source of most ransomware attacks is compromised credentials. Even with longer, more complicated passwords and authentication flows that utilize one-time passwords or push notifications, passwords remain insecure. Beyond Identity's platform replaces the password with unhackable cryptographic credentials that are tied to the device. This takes away attackers' most common vector, eliminating the risk of password-based attacks. It also prevents lateral movement, how ransomware attackers often inflict the most damage by jumping from system to system once they are inside an organization.

"An ounce of prevention is worth a pound of cure." Benjamin Franklin, 1736 - *On Protections of Towns from Fires*

In the earliest days of the American Colonies, life wasn't easy. With resources tight, most cities dealt with what was in front of them at any given moment, including city services like fire safety. There were no fire hydrants, stations, or first responders.

In a large (and growing) city like Philadelphia, this was asking for trouble. After visiting Boston, Benjamin Franklin became so enamored by the city's organized fire response that he brought the idea home to Philadelphia. With Franklin's help, Philadelphia created one of the most advanced fire fighting systems in the world at the time.

But dedicated firefighters were only a solution for live, active fires in colonial Philadelphia. From regulating chimney sweeping to adopting better building codes, Philadelphia made the extra effort to not only fight but prevent future fires, too.

Today's cities aren't as concerned with fires, but businesses within are getting ravaged by ransomware. It may be because we are still doing the digital equivalent of building our houses out of flammable, easy-to-light wood: modern cyber threat response is much like Philadelphia's fire protocols in the early 1700s: we react to dangers on an ad-hoc basis, often with no centralized effort.

We must build our applications and services like "fireproof" homes. The first line of defense against ransomware is transitioning your authentication processes to a passwordless, credential-based system.

[1] https://www.brighttalk.com/webcast/18267/516290

BEYOND IDENTITY

The expanding ransomware problem

$847K
Average ransom across all ransomware families in 2020

22 Days
Average Downtime, Q3 2021

44%
Attacks on medium-sized businesses

Ransomware has quickly become one of the most common attack vectors, and a new incident occurs approximately every 11 seconds.[2] Security firm Coveware estimates that the ransomware resulted in an average of three weeks of downtime as a direct result of attacks.[3] The 2021 Unit 42 Ransomware Threat Report reported an average ransom of $847K in 2020 and that Maze, a ransomware gang, had ransom demands in 2020 that averaged $4.8 million.[4]

Ransomware attackers have dramatically expanded the reach of their attacks in the past several years. Some of this movement might have to do with the attention (both in the media and from law enforcement) focused on ransomware due to April 2021's Colonial Pipeline attack. Large companies raced to avoid being the next victim and have stepped up their defenses.

Small and mid-sized businesses aren't moving as quickly. The lack of focus on cyber security isn't necessarily negligence: these smaller organizations don't often have the massive IT budgets or personnel that the big corporations do, and many still operate on the outdated premise that hackers are looking for the "big fish."

That couldn't be further from the truth. Coveware found that in Q3 2021, 44% of all ransomware attacks targeted businesses with 101-1,000 employees, precisely the organizations that have been much slower to adjust their security posture.

While larger businesses might have the funds to pay off an attacker if they're unable to recover their encrypted and stolen data on their own, a ransom demand would cause significant financial disruption for smaller firms, or put them out of business altogether.

[2] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
[3] https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
[4] https://unit42.paloaltonetworks.com/ransomware-threat-report-highlights/

The true cost of recovery

Recovering from a ransomware infection is expensive. Including all the factors that go into recovery—the cost of downtime, excess man hours for recovery, device and network repair and replacement, lost revenue opportunities, and the ransom paid—Sophos found that the average cost to recover was nearly $1.85 million in 2020,[5] double what it was the year before.

This doesn't even take into account future losses. Successful ransomware attacks have effects that victimized businesses contend with for years. Data privacy is increasingly a concern for both consumers and regulators alike, and in a Beyond Identity survey it was found that almost 70% of online consumers have stopped using a service because of a publicized breach.[6]

A 2021 Cybereason study found that two-thirds of business respondents suffered "significant" revenue loss, and 53% reported damage to their brands. Then there's the regulatory trouble: governments worldwide are increasingly focusing on data privacy. The two biggest efforts, the EU's GDPR and California's CCPA, put the onus on the organization to protect the data it collects from its users. A ransomware attack puts control of this sensitive data in the attacker's hands, and the organization may be subject to civil penalty for their negligence.

The increase in ransomware attacks, the shift in who the attackers are targeting, and the exploding cost of recovery from ransomware infections all call for preventive measures to be put in place, regardless of organization size.

Ransomware's cost beyond recovery

25% of businesses were forced to close either temporarily or permanently

32% of C-Level executives were out of job either through resignation or termination

29% of businesses were forced to eliminate jobs

[7]

[5] https://www.beyondidentity.com/blog/lost-value-in-customer-authentication-frustration-study
[6] https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
[7] https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf

Current ransomware techniques

RDP
Remote Desktop Protocol

Horizontal Integration

RaaS
Ransomware-as-a-Service

Phishing

In order to successfully prevent ransomware attacks, understanding their source is vital. While 2020 was a trying year for all of us, it also reshaped the ransomware threat landscape: the fast transition to work-from-home (WFH) across many industries played right into attackers' hands.

Organizations no longer have the control they did over the environment or devices users connect with. Attackers know this, and vulnerabilities in remote access protocols are one of the most common points of entry.

The pandemic also changed how the attackers themselves operated. Groups no longer produce the entire ransomware product from start to finish. Experts are pointing to an increase in SaaS-like operations that significantly reduce coding needs for people carrying out the attack, making it even easier for anyone to execute these attacks.

Remote Desktop Protocol (RDP): A common point of entry

WFH tested organizations' remote access policies like never before. Before the COVID-19 lockdowns, just one out of every 25 workers carried out their job remotely. Even with the lockdowns long gone, a recent Mercer study[8] found that 70% of organizations it polled planned to transition, or are using, a hybrid model for work.

Most of these workers will connect using Remote Desktop Protocol (RDP). RDP is a Windows feature that allows users to remotely connect to and control a remote system. While it was most commonly used in IT support environments, RDP is now commonly used in cloud computing environments to manage assets and log into virtual machines.

Since RDP is a primary target for attackers, organizations must make sure they have a handle on their remote access policies and enforcement procedures. A successful RDP break-in gives the attacker an instant seat in the organization and can obtain and view data up to the access level of the compromised account.

Setting up secure remote sessions and enforcing policies is a challenge for many smaller organizations, which don't have the funds to hire IT admins or the expertise to implement robust security policies. However, the lack of assertiveness from large enterprises in preventing these break-ins is far more concerning: they can afford to take proactive steps by hiring additional security personnel, setting better boundaries via solutions and tools like authentication and encryption, and strengthening network monitoring.

[8] https://www.hrdive.com/news/most-us-employers-with-flexible-work-plans-choose-hybrid-work-mercer-says/603304/

Horizontal integration: A team effort

Supply-chain-dependent industries come in two forms: horizontally and vertically integrated. Vertically integrated companies control all aspects of the supply chain, from the production, transport, and sale of its goods. A horizontally integrated company doesn't own the entire supply chain, but it controls a segment of it. This allows the company to specialize, and in theory, develop a better product.

Ransomware attackers are increasingly following a horizontally integrated model. Gone are the days where the attacker wrote the code, researched and found the target, executed the attack, and collected the ransom. Today's ransomware attacks are largely a team effort, with much of the work outsourced to various groups and services specifically set up to serve the attacker's technological needs.

This approach reduces coding time exponentially. The attacker can outsource much of his or her work to other criminals who are experts in certain fields necessary for a successful attack. This is where RaaS comes into play.

Ransomware-as-a-Service (RaaS)

The rise of RaaS is behind the dramatic increase in ransomware attacks in recent years, as well as the uptick in attacks among small and medium-sized businesses. When attackers had to do all the work the focus was on the most significant return, hence why ransomware attackers looked for larger targets. With RaaS, that's no longer necessary.

RaaS enables occasional and professional hackers alike to initiate their ransomware attacks without buying or designing the ransomware themselves. It's one of the most common models in cybersecurity today because it dramatically simplifies the attack process.

RaaS has made it so easy to launch ransomware attacks that a disgruntled ex-employee can do it easily. While these one-off attacks remain rare, experienced attackers are using RaaS to attack more targets in less time.

While RaaS providers handle the details of the execution of the attack once inside, getting the initial information necessary to access company resources is well-documented.

Step 1: Find out how to get in

In this first step, the attacker searches for vulnerabilities in the target organization through penetration testing. However, instead of the legitimate use of pen testing, the attacker is looking for a way in.

With ransomware, the most common method is through the RDP. However, other less-common entry points warrant close monitoring. These include:

- **Third-party managed service providers (MSPs):** Some organizations outsource their IT needs to third parties. MSPs are an attractive target because you only have to compromise one organization to get access to several. They often use the same remote tools that hackers target in individual companies, with high (if not root) access to the organizations they serve. Organizations using MSPs must closely monitor these accounts for suspicious activity and are at the MSP's mercy as to whether or not they follow good security practices.

- **Remote employees:** Remote employees are another common point of vulnerability. Some workers often have excessive access rights, significantly increasing the impact of a data breach or ransomware attack if they are compromised. The risk here to organizations is poor security practices on the part of the employee. Organizations often don't have strict bring-your-own-device (BYOD) policies and can't accurately monitor what might be installed on their devices, such as malware, when the employee is accessing company resources.

- **Remote access tools:** Employees and MSPs use remote access tools regularly, i.e., RDP, VNC, etc. It is becoming increasingly common for attackers to specifically target these tools as a means of entry into an organization's network. If compromised because of leaked passwords or other vulnerabilities in these tools, hackers can easily take control.

- **Using the Shodan browser:** Shodan is a search engine for devices on the internet. It has become popular because it enables hackers to find anything from webcams to routers accessible on the internet. With the rise of Internet of Things (IoT) devices, Shodan is becoming more valuable to attackers looking for a way into an organization's network.

- **Remote Access Ports:** These are the main entry points, and hackers know all of them. If you have any business with these services on your network, you need to ensure that your firewalls are up to date and configured accordingly.

Step 2: Outsource the attack

Before RaaS, the attacker would take the time to write the code necessary to set up the attack. This part of the process is by far the most labor-intensive and may take days, weeks, or months to complete.

RaaS changes that. The attacker finds a RaaS provider on the dark web and chooses from a list of available payloads they want to use against their target organizations. When that's finished, all it takes is one click to deploy the attack against their targets.

RaaS providers might charge a monthly, annual, or on-demand rate just like a SaaS company would, or they might demand a portion of any ransom collected in return for its services.

The ransomware attack can then be monitored across multiple computers in real-time through a RaaS dashboard. Like a SaaS product, these dashboards offer a birds-eye view of the platform, and they receive reports on when payments are received and decrypt keys sent. It allows attackers to monitor the status of an attack and manage attacks on multiple victims simultaneously.

As a result, ransomware attacks have become much more efficient, explaining the dramatic increase in incidents over the last several years as RaaS providers evolved and "full service" offerings became widely available.

These days, attacks are launched with literally a click of the mouse.

Phishing remains a problem

Phishing techniques remain a popular method to gain access to organizations when RDP isn't an option. RaaS-based attacks employ phishing methods to access target organizations with the hope that users will open a malicious link or attachment. Even with years of efforts to educate the public about what they should and should not open in an email, attackers are still managing to trick some with well-crafted spoofs.

A new threat: data disclosure

Traditional ransomware methods involved encrypting or locking up the victim's data and then demanding a ransom. In the past several years, this has begun to change. Attackers are increasingly adding threats of data disclosure to their ransom demands, especially where any leaked data could be potentially damaging.

While the exact reasons for this switch are unknown, one possibility is that attackers are increasingly finding victims less willing to pay the ransom.[9] The FBI recommends that victims don't pay the ransom, and many companies are at least making some effort to protect themselves from hacking attacks.

[9] https://www.fbi.gov/news/stories/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise

With the victims' valuable data and the threat to sell or disclose it if they don't pay up, the attackers regain the upper hand. Last year, Coveware found that nearly half of the ransom demands included a threat to disclose data[10] if the ransom wasn't paid. But while organizations might be engaging these cybercriminals more often as a result of these threats, the promises to "delete the data" aren't being honored, and in some cases, are used to extort the same victim at a later date.

We believe the changes in the ransomware techniques used along with the rapidly increasing number of attacks demonstrate the need for a solution that strikes at the core of what makes a ransomware attack successful: the password.

How to avoid becoming the next victim

A majority of hacks are a result of vulnerabilities in the authentication process, most commonly a compromised username and password. Taking the password out of the process and replacing it with a more secure method, such as cryptography, seems like a no-brainer.

Furthermore, tying these credentials to the user's device allows you to always know who and what device is requesting access. This prevents logins from unknown devices that may or may not be secure, and confirms the user is who they say they are.

In contrast, all the username and password tells you is that whoever is requesting access has provided the correct credentials. While careful monitoring of user behavior and Multi-Factor Authentication (MFA) helps to provide a greater degree of certainty that logins are legitimate, only device-linked credentials can provide complete certainty of identity.

Efforts to protect your organization should not end there: just because passwordless authentication is enabled does not mean you're completely immune from attack. You must monitor the security posture of anyone requesting access, and make authentication and authorization decisions based on risk level.

Risk-based access controls allow you to enforce company security policies on devices you own as well as any personal device your users may use to access company resources. With remote work exploding in popularity, corporate networks must treat any device or user the same no matter who they are or what device they use. Each login is a potential threat, and with insider attacks also a growing problem, your next attack could come from within your organization.

There are solutions available which allow you to secure your corporate network using the principles we've laid out in this paper, and Beyond Identity offers such a platform.

[10] https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report

Introducing Beyond Identity

Beyond Identity eliminates passwords altogether, thus eliminating the entry point many ransomware attackers use. Passwordless multi-factor authentication is at the heart of our platform. Traditional MFA relies on passwords, which are fundamentally insecure, but Beyond Identity uses a private encrypted key tied to the user's device instead of the password and requires users to confirm identity with a local device biometric before being granted access.

But Beyond Identity doesn't stop there. Our platform also helps organizations achieve a zero trust security architecture. Before granting access and continuously during the user session, Beyond Identity continuously monitors the security posture of the device connected and provides access only to what the user needs to complete the task. Suspicious logins, unknown device security posture, and lateral movement are easily detected since identity is verified at every step and would stop a ransomware threat in its tracks.

Self-signed X.509 certificates based on industry-standard asymmetric key cryptography replace the password. An entirely cloud-based service, our authenticator operates within an app on the device, and existing SSO solutions easily integrate with Beyond Identity with just a few lines of code. Our platform is both easy to deploy and equally easy to use.

When a user visits a protected application, there is no password field -- all users need to do is click a button to log in. The user has already confirmed their identity through on-device biometrics or PIN codes. Behind the scenes, the app provides the necessary credentials to our authenticator, which can optionally further analyze the login for risk signals, including if the device is jailbroken, its location, security posture, and more.

The result is an authentication solution that is far more protected from attacks. In addition, our policy engine can help you enforce security policies that protect you from internal threats from logged-in users.

Our approach to authentication is entirely private. Nothing about the login is ever shared, even with us, and insecure MFA methods like SMS, push notifications, or e-mail links are now unnecessary. We use industry-proven public key infrastructure (PKI), TLS, and hardware enclaves in a brand new way to finally bring authentication into the 21st century.

There is nothing private about a password, and that password is stored somewhere, whether in a database on your server or a user's computer. Hackers know this. By removing the insecurity passwords bring, you're eliminating the most common entry point: stolen credentials.

Learn More:

How Our Authenticator Works

www.beyondidentity.com/how-it-works/authenticator

Passwordless MFA Solution

www.beyondidentity.com/solutions/passwordless-mfa

Request a Demo

www.beyondidentity.com/demo

About Beyond Identity

Beyond Identity provides the most secure authentication platform in the world. Breaking down barriers between cybersecurity, identity, and device management, Beyond Identity fundamentally changes the way the world logs in by eliminating passwords and providing users with a frictionless multi-factor login experience. Beyond passwordless, the company provides the zero-trust access needed to secure hybrid work environments, where tightly controlling which users and which devices are accessing critical cloud resources has become essential. The advanced platform collects dozens of user and device risk signals during each login, enabling customers to enforce continuous, risk-based access control. The innovative architecture replaces passwords with the proven asymmetric cryptography that underpins TLS and protects trillions of dollars of transactions daily. Customers turn to Beyond Identity to stop cyberattacks, protect their most critical data, and meet compliance requirements.

The company was founded by Jim Clark and TJ Jermoluk, who helped ignite the commercial internet with Netscape and @Home Networks. The dynamic duo assembled an all-star team and created the world's most advanced passwordless identity platform at a time when digital transformation is impacting every business, and cyberattacks have become a top risk. The company raised $105M from premier investors Koch Disruptive Technologies (KDT) and New Enterprise Associates (NEA). Beyond Identity is headquartered in NYC with offices in Boston, Dallas, Miami, and London.

Ready to Have Beyond Identity Solve Your Authentication Challenges?

GET A DEMO

beyondidentity.com | info@beyondidentity.com

BEYOND IDENTITY