



An A.P.P.L.E. a Day Keeps Ransomware at Bay

CYBERSECURITY | FEDERAL



We've all heard the adage, "an apple a day keeps the doctor away."¹ It dates back to the early 19th century when it was believed that eating healthy foods, like apples, would decrease the need for doctor visits.

In much the same manner, we believe that applying the security mechanisms represented by the acronym A.P.P.L.E. — authenticate, patch, protect data, limit privilege and enable anti-malware — as a component of your cybersecurity hygiene will protect your enterprise. To be more specific, to keep ransomware at bay, you need to A.P.P.L.E. every day.

Let's take a closer look at each of A.P.P.L.E.'s cyber defense mechanisms and why they're important to your security capabilities.

Table of Contents

- 01** The rotten apple – ransomware
- 02** Authenticate
- 03** Patch and update
- 05** Protect data
- 06** Limit privilege
- 07** Enable anti-malware
- 09** Conclusion
- 10** About the authors
- 11** Sources



The rotten apple – ransomware

According to the Federal Bureau of Investigation, “ransomware is a type of malicious software, or malware, which prevents you from accessing your computer files, systems or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.”²

Viruses, trojans, breaches and malevolent actors are enough to send shudders down the spine of even the most stalwart CISO. Even more disconcerting is the rise of ransomware attacks. As many as 70% of businesses worldwide report being the victim of ransomware attacks in 2022.³ Globally, one out of 40 organizations were impacted by ransomware attacks, a startling increase from previous years, that many experts attribute to the war between Russia and Ukraine, where cyberattacks are an increasingly effective weapon.⁴

We’ve all seen the headlines and have been affected in some manner by ransomware. The Colonial Pipeline attack impacted 45% of the fuel supplies on the East Coast of the United States, crippling airline travel and other transportation and causing supply chain challenges, gas shortages, price gouging and more.⁵ There were less publicized attacks in 2022, but for those companies and individuals affected

by ransomware, it didn’t lessen the hurt. Chicago Public Schools, Microsoft Exchange, Samsung, MacMillan and Cisco – just to mention a few – were impacted.

Fortunately, government agencies are faring a bit better than their private sector counterparts, reporting an approximately 45% attack rate.⁶ Still, the numbers provide no comfort because they continue to rise. Each year, NTT’s Digital Forensics and Incident Response team produces a “Global Threat Intelligence Report” to track the latest in cybersecurity. The 2022 report saw an astronomical rise in ransomware: 240% growth, up from 7% in 2019.⁷

Ransomware demands are clear. Pay up or lose valuable data, access and assets. The growing trend is for victims to pay up, with 62.9% of victims giving in to the demands.⁷ Cyber experts caution that paying ransom doesn’t guarantee full recovery and that data is often corrupted or lost. Even worse, yielding to demands and paying ransom can encourage a second round of demands. In a worldwide survey of security professionals, 80% of the organizations that paid were subject to a second attack.⁸

As Benjamin Franklin said, “an ounce of prevention is worth a pound of cure,” and that’s certainly true when it comes to

cybersecurity hygiene. That’s where A.P.P.L.E. comes in. A combination of authenticating, patching, protecting data, limiting privilege and enabling anti-malware can help protect your organization.

The physical invasion of Ukraine began on February 24, 2022; cyber operations began much earlier. Before the invasion, Whispergate, a data-wiping malware, targeted multiple industries in Ukraine, including government, non-profit and IT organizations. In January 2022 attackers likely aiding Russian strategic objectives defaced nearly 70 Ukrainian government websites. These defacements warned Ukrainians to “expect the worst.” In mid-February, DDoS attacks targeted Ukraine’s armed forces, defense ministry, public radio and the two largest national banks, crippling services for hours.

– NTT, “2022 Global Threat Intelligence Report”

Authenticate

Just as there are different varieties of apples, — Macintosh, Red Delicious and Fuji, among others, — there are different authentication types to protect from ransomware. The most common form is a username/password combination. But passwords alone do little to protect organizations and individuals from ransomware.

Compromised passwords are one of the easiest ways for hackers to gain access to a network. Vulnerable credentials are a gateway to the enterprise. The highly publicized, infamous ransomware attack of Colonial Pipeline was traced to a compromised password. The DarkSide gang targeted Colonial Pipeline's billing system and internal business network, leading to widespread shortages in multiple states. Colonial Pipeline paid the group \$4.4 million in bitcoin to avoid disruption.⁹ The attack on critical infrastructure was linked to an old virtual private network that allowed remote access without requiring multi-factor authentication (MFA).¹⁰

Sadly, many of us are password lazy. We don't appreciate the importance of developing strong, unique passwords. The password responsible for the most data breaches is "123456" — 23.2 million accounts use it.¹¹ Derivations of easily searchable information, such as birthdays, oldest child's name, high school graduation or favorite pet, all make

bad passwords. A word to the wise: Those quizzes on social media asking your astrological sign or first pet reveal nothing about your personality, but they do give hackers clues to decoding your passwords.¹² Humans are creatures of habit. We often have the same password across multiple accounts. It keeps things simple and easy to remember. But this lackadaisical approach to cyber hygiene provides hackers easy entry to your accounts.

If passwords are the first line of defense for authentication, then we need to be smart about them. Another great step is deploying Fast Identity Online (FIDO), a set of open-standard authentication protocols designed to eliminate passwords. FIDO protocols streamline the authentication process through a fingerprint or PIN while leveraging cryptography behind the scenes for protection. The current telework environment means each endpoint — the laptops, tablets and mobile phones employees use to get the job done — is a potential vulnerability. In fact, according to the NTT 2021 Global Threat Intelligence Report, 67% of all attacks were remote access: either web application (32%) or application-specific (35%).¹³ FIDO is one protection that may help CISOs sleep at night.

FIDO instead of passwords is great, but cybersecurity practitioners also stand firm on recommending MFA as an additional line of defense. MFA is now common across most online interactions; it's likely you use it to access your banking information, Amazon account or social media profile. It's a second step to verify identity, which typically involves providing more than one unique piece of information.

The Cybersecurity Infrastructure Agency (CISA), established in 2018, works across public and private sectors and challenges traditional ways of doing business by engaging with government, industry, academic and international partners. CISA defines MFA as "a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify identity for login. MFA increases security because even if one credential becomes compromised, unauthorized users will be unable to meet the second authentication requirement and will not be able to access the targeted physical space, computing device, network or database."¹⁴

Patch and update

Even with strong authentication methods, hackers can take advantage of outdated software and firmware to “escalate” their privilege, move freely within your network and look for opportunities to create havoc. The solution to the problem of outdated software is simple: Make sure all your software — and firmware — is up to date and apply appropriate patches when needed. Devices that handle sensitive information should be first on the update list.

Fortunately, tools are available to scan your trusted network and identify devices with software that needs updating. Staying abreast of the changes in the marketplace is important because installed software could rely on compromised components.

One of the worst cases of this is the recent Log4j vulnerability, about which CISA issued a dire warning in early December 2021.¹⁵ Among the millions of systems that use Log4j software exists a JavaScript vulnerability called Log4Shell. The frequently used open-source library software records a variety of software functions in these systems. Even prominent technology vendors, including Cisco, IBM and VMware, have products with the vulnerable code.¹⁶

“Logging” is a basic function in most software, and as a result, Log4j is everywhere.¹⁷ Popular games like Minecraft, as well as the most widely used business tools from Microsoft, and other security and software development tools — not to mention Apple iCloud — use Log4j software, giving hackers a huge target.

Large technology companies can expedite patches to protect web servers and prevent exploitation, but it takes many organizations longer to patch systems. And because Log4j is often bundled as part of other software packages, it’s tough for even the most diligent IT teams to know if and where they might have a problem.

An internet comic from xkcd depicts a project much like an Log4j deployment (see Figure 1).¹⁸ Think of it as an incredibly useful open-source project supported by a relatively small group of developers. When something goes wrong, the software is generally “patched.” But with Log4j, the fix requires coordination throughout the software supply chain and involves many facets of software development and distribution. So, the fix isn’t easy. As a result, some believe we’ll see Log4j troubles for many years to come.

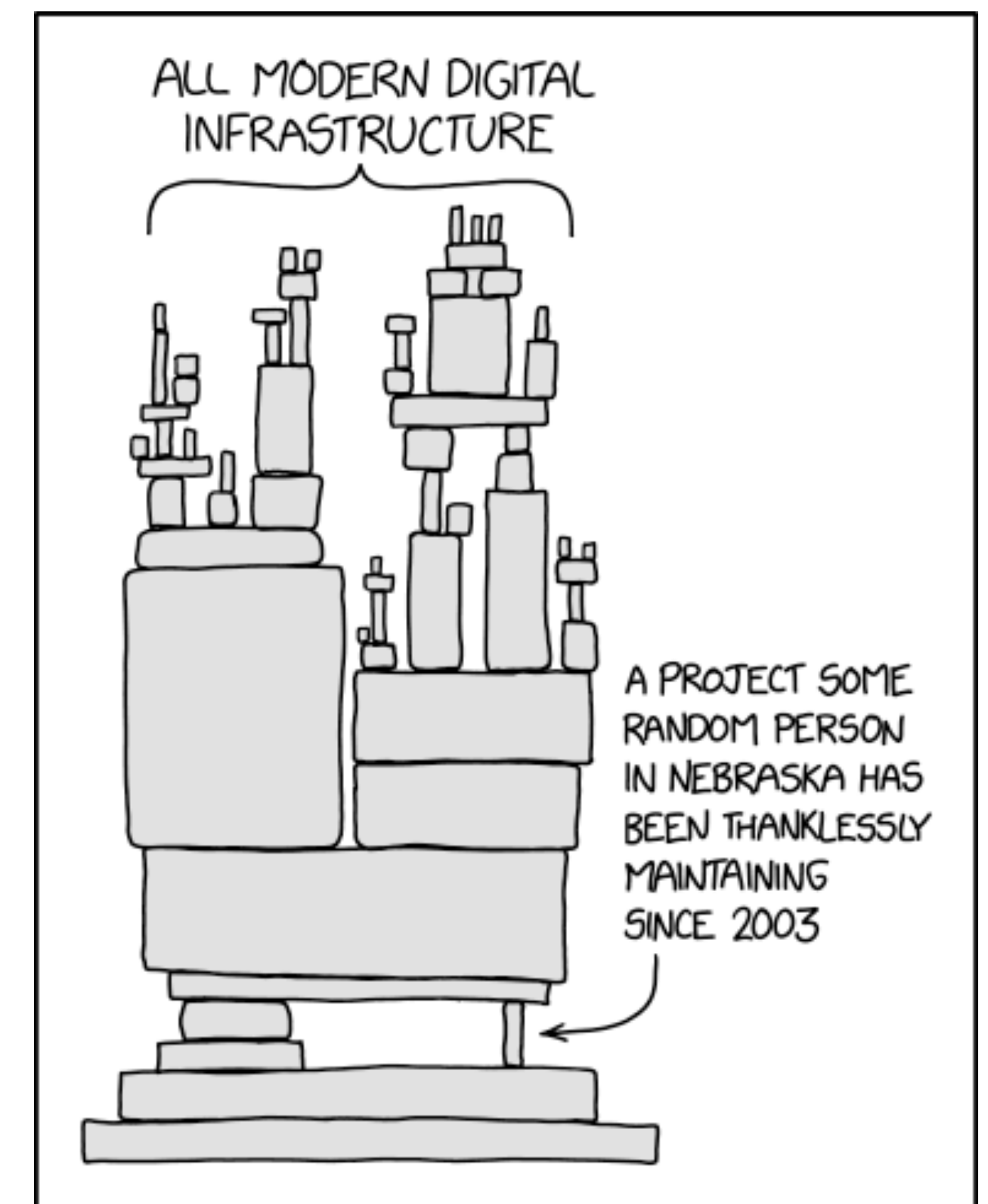


Figure 1: xkcd’s comic “Enterprise Dependencies”

Authenticate

Patch and update

Ransomware groups have weaponized Log4j – Cobalt Strike and Kerberoasting – in hopes of hitting paydirt through malicious .NET files, infecting files, obtaining remote access, taking over servers and accessing passwords; generally wreaking havoc on systems throughout the world.

Jen Easterly, director of the U.S. Cybersecurity and Infrastructure Security Agency, called Log4Shell “the most serious” vulnerability she’s seen in her career.¹⁹

Log4j illustrates the worst of the worst-case scenarios. But it’s also led software developers to new best practices. Developers now strive to understand their entire software supply chain and the software bill of materials (SBOM) that documents production software. It’s important to learn from experience; knowing about software and firmware vulnerabilities helps facilitate patching or mitigation efforts.

Prioritize the patch. Make a date to update.

21,957

Vulnerability disclosures in 2021 were the highest ever.⁷

**24
minutes**

On average, a new vulnerability was registered every 24 minutes in 2021.⁷

Protect data

Globally, there are about 2.5 quintillion bytes of data created each day. In 2020, we collectively sent and received roughly 306.4 billion emails each day.²⁰ That's a lot of data. And given the sheer volume and scale, it should come as no surprise that it's easy to take data and our access to it for granted, despite its position as one of the most valuable assets in the organization.

Data's organizational value made it a prime target for ransomware during the global pandemic. Adversaries quickly learned that organizations were willing to pay big if access to their own data was taken away. Amid the chaos, threat actors attacked vulnerable healthcare organizations. In 2020, ransomware attacks cost the healthcare industry over \$20 billion in lost or impacted revenue, lawsuits and ransom paid. In 2021, more than 2,302 hospitals, clinics and other healthcare organizations were victims of 108 ransomware attacks.²¹

Fortunately, there are several tools in the cybersecurity arsenal to help protect organizational data, many of which rely on authorization.

Protecting data starts with understanding where sensitive data is in the enterprise. Data classification is a critical part of this. Within government and the military, data is often classified according to the information it contains, for example, top secret, secret or controlled unclassified information. Labeling data allows you to control access to the document, asset or data. Security professionals can control and protect information by not allowing it to be sent out of the organization if it falls into a certain category. Data labeling can be extremely specific; enabling fine-grain authorization controls will prevent sensitive data from being shared.

True data protection means organizations need to identify sensitive data and know where it's stored and transmitted. Knowledge is power, and coupled with the appropriate authorization protocols, both the data and the systems holding sensitive data can be protected from the rogue programs ransomware attackers use. Data protection must include appropriate levels of authorization to ensure only those with permission can access data. Multiple authorization methods exist, from the role/group-based access control (RBAC) standard on most computer systems to more sophisticated capabilities.

Attribute-based access control (ABAC) manages access based on the attributes of subjects (person, organization or device) and objects (information or capability) and a known set of environmental conditions and policies.²² ABAC is implemented as a service for other applications to consume. When a subject uses an application to access an object, a request is sent to an ABAC server with the attributes of the subject and the object as well as any environmental conditions. The subject is approved or denied access depending on their attributes.

Conditional access control is a middle ground that uses role identities from RBAC combined with selective attributes on the subject or the object to grant or deny access. Combining these controls can make lateral movement by ransomware difficult or impossible, limiting the blast radius of an attack.

Limit privilege

The concept of least privilege centers on limiting administrative privileges to everything within your enterprise. The fewer people who have a key to your house the fewer who can enter uninvited.

Unless there's a clear, documented or mission-related reason for elevated privileges vetted by the CISO, CIO or IT department, access isn't granted. Disabling permission protocols at the admin, root or super-user level reduces the likelihood of nefarious actors gaining entry. Elevated privileges allow a user to execute certain actions on a computer system or enterprise; if those privileges are compromised, bad actors can take the same actions as a super user or administrator.

Privilege is an integral part of a zero trust security framework. This cybersecurity defense paradigm focuses on users, assets and resources. A good rule of thumb is "never trust, always verify." Endorsed by the National Institute of Standards and Technology (NIST), a zero trust architecture doesn't grant implicit trust to assets or user accounts based solely on their physical or network location (that is, local area networks versus the internet) or based on asset ownership (either enterprise or personal). Authentication and authorization (both subject and device) are discrete

functions performed before establishing a session to an enterprise resource.²³

CISOs who employ zero trust think in terms of authentication, authorization and monitoring: Can I trust you? Should I not trust you? If I do trust you, what can I trust you with? And, once I trust you, I will monitor what you're doing on my enterprise network.

Many government employees (including the authors of this ebook) were victims of the Office of Personnel Management (OPM) data breach of 2015. This hack exposed millions of SF-86 forms, which contain the personal information gathered during background checks of people seeking government security clearances, as well as compromised millions of people's fingerprints.²⁴

Myriad errors caused the OPM breach. And this wasn't the first time the agency's technical leadership tangled with hackers, who had previously gained broad access to the OPM network using stolen credentials from a vendor with administrative privileges. Unfortunately, OPM didn't deploy MFA for users who had elevated privileges. Without MFA, when an attacker steals a valid username and password (as the X2 hackers did, using a login pilfered from KeyPoint)

they gain free access to the system and all the privileges associated with that user, including administrative rights.

Tight controls that limit elevated privilege would have helped protect the data of millions.



Authenticate

Patch and update

Protect data

Limit privilege

Enable anti-malware

Enable anti-malware

Malicious, malevolent, malign, malady – anything with the Latin root “mal,” meaning bad or evil, is never a good thing. This includes malware, the hypernym used to describe malicious software and viruses. The best defense to combat malware is a good offense. IT professionals should deploy anti-malware software to help protect networks. But deploying anti-malware isn’t enough; security teams must be sure that antivirus and anti-malware software are updated as well as run regular scans to protect networks.

Unfortunately, human error accounts for the largest number of breaches. Unscrupulous individuals gain access to an enterprise by gaining your trust. An innocent mouse click by an unsuspecting user may be all it takes for an attack to begin. Phishing is the most common form of cyberattack. It’s meant to trick you into clicking, forwarding or providing sensitive information. Phishing comes in many forms.

In 2021 there was a 240% growth in ransomware. The most common attack was email containing malicious links or attachments.

– NTT “2022 Global Threat Intelligence Report”⁷

Similar to its famed historical namesake, a Trojan Horse (or Trojan) is a type of malicious code or software that looks legitimate but can take control of your computer.²⁵ Trojans accounted for 65% of malware in 2021, up from 35% in 2020. Overall, NTT cyber forensics observed a 50% increase in detected malware led by Trojans and botnets during 2021.⁷ An increased use of banking Trojans indicates a rise in cybercriminal activity, while the increased use of other Trojans suggests a rise in espionage and theft of trade secrets.

A botnet is a network of computers or internet-connected devices infected with malicious software or controlled by hackers, while a bot (short for robot) is a computer application programed to perform a certain task. In the case of a cyberattack, a bot crawls through a network to spread a virus or create chaos.²⁶

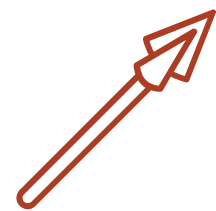
Think before you click. If it looks suspicious, it’s probably not something you should share or forward. Enable anti-malware to identify most types of ransomware and malicious applications before they’re installed on your system. Anti-malware provides a rampart, blocking attacks and preventing ransomware from breaching your organization.



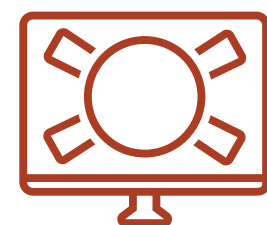
Phishing comes in many forms.



Email phishing is when scammers create an email to look like it originated from a real company to steal your information.



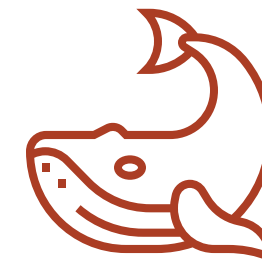
Spear phishing also uses email, but it's more personal. It might look like it comes from your boss or a trusted entity. New York Oncology Hematology (NYOHA) employees and patients were lured by a clever phishing scheme that sent an email directing them to the NYOHA login page where the data they entered was used to breach accounts.²⁷



Pop-up phishing is another common tactic used to entice an innocent user to click on a malicious link, which in turn installs malware. Often, malware is imbedded in an advertisement that may be dangerous to the user. Unsuspecting users hoping to win prizes or investigate a product or service may unwittingly install spyware on their computer.



Clone phishing is very sneaky. As the name implies, scammers clone an email you receive and then add a malicious link or attachment.



Whaling is when scammers go on a big hunt — targeting a high-ranking executive to gain access to sensitive data or money. In 2016, John Podesta, Hilary Clinton's campaign manager, received an email from the Russian hacking gang Fancy Bear with the subject line "Someone has your password." Mr. Podesta did the right thing and forwarded the email to the technical team. Next, things went very wrong, and IT told him to change his password.²⁸ The rest is history.



SMS phishing, or smishing, is like phishing but it uses text messaging. Cybercriminals reach out via text to an unsuspecting user of one of the world's 3.5 billion smartphones with an urgent, compelling text message.²⁹ The text often looks very real, mimicking companies or mentioning friends with whom the recipient regularly interacts. The "gotcha" comes when the response requests a text back with private data or provides a link that downloads malicious software.³⁰

Conclusion

Cyber risk is real. It goes beyond demands for ransom, bitcoin or otherwise, and releasing data. In the public sector, the combination of critical infrastructure, cyber terrorism and a host of other challenges create the perfect storm of conditions for increased risk (as almost everything has some type of technology controls).

While writing this ebook, for example, CISA, the National Security Agency/Central Security Service and the Multi-State Information Sharing and Analysis Center issued a joint alert warning agencies about the malicious use of remote management software, in this case ConnectWise Control and AnyDesk. Officials said that while the specific activity “appears to be financially motivated and targets individuals, the access could lead to additional malicious activity against the recipient’s organization — from both other cybercriminals and [advanced persistent threat] actors.”³¹ Although specific agencies weren’t named, cybercriminals tricked federal employees into downloading remote monitoring software to gain access to victims’ bank accounts.³²

Cities and municipalities are another prime target for increasingly sophisticated thieves. Atlanta and New Orleans, as well as Pensacola, Florida, and Greenville, North Carolina, have joined a growing list of the attacked. Threat vectors hit cities from all sides because they’re ill-equipped to



Figure 2: Implement A.P.P.L.E for up to 98% protection

synchronize systems, track third-party vendors and provide training. They’re also habitually underfunded. A cyberattack on Baltimore, for example, demanded an escalating bitcoin payout. The city didn’t yield to the demands even as the Robbinhood virus spread, crippling city services. Instead, IT professionals shut down systems and began recovery efforts, the cost of which city officials estimate at more than \$18 million.³³

But there’s hope. Recent research from Microsoft indicates that security professionals can implement the basic security protocols of A.P.P.L.E. and combat 98% of cyberattacks (see Figure 2).³⁴

Remember: Authenticate, patch, protect data, limit privilege and enable anti-malware. This A.P.P.L.E. a day will keep will keep ransomware at bay — and protect your enterprise.

Let NTT DATA cybersecurity experts help you get started.

Sources

- 1 [The Content Authority. "What Does 'An Apple A Day Keeps The Doctor Away' Mean?"](#)
- 2 [Federal Bureau of Investigation. Ransomware resources.](#)
- 3 [Statista. "Percentage of organizations victimized by ransomware attacks worldwide from 2018 to 2022."](#)
- 4 [Check Point Software. "Check Point Research: Weekly Cyber Attacks Increased by 32% Year-Over-Year; 1 out of 40 Organizations Impacted by Ransomware." July 26, 2022.](#)
- 5 [Abigail Nig. "A major U.S. pipeline is still mostly shut due to a cyberattack. Here's what you need to know." CNBC. May 10, 2021.](#)
- 6 [Julie Pattison-Gordon. "Most Governments Were Hacked in the Past Year, Reports Reveal." Government Technology. April 18, 2022.](#)
- 7 [NTT. "2022 Global Threat Intelligence Report."](#)
- 8 [Rebecca Klapper. "Most Businesses That Pay Off After Ransomware Hack Hit with Second Attack: Study." Newsweek. June 16, 2021.](#)
- 9 [Touro College Illinois. "The 10 Biggest Ransomware Attacks of 2021". November 12, 2021.](#)
- 10 [Brian Fung and Geneva Sands. "Ransomware attackers used compromised password to access Colonial Pipeline network." Cable News Network. June 4, 2021.](#)
- 11 [Danny Palmer. "These are the most commonly hacked passwords – is one of them yours?" ZDNET. April 20, 2019.](#)
- 12 [Zerofox Team. "How Hackers Use Social Engineering to Get Passwords on Facebook" ZeroFox. January 27, 2021.](#)
- 13 [NTT. "2021 Global Threat Intelligence Report."](#)
- 14 [Cybersecurity & Infrastructure Security Agency. Definition of multi-factor authentication.](#)
- 15 [Cybersecurity & Infrastructure Security Agency. "Statement From CISA Director Easterly on 'Log4j' Vulnerability." December 11, 2021.](#)
- 16 [Michael Novison. "10 Technology Vendors Affected by the Log4j Vulnerability." The Channel Co. \(CRN\). December 13, 2021.](#)
- 17 [James Wetter and Nicky Ringland. "Understanding the Impact of Apache Log4j Vulnerability." Google Security Blog. December 17, 2021.](#)
- 18 [XKCD. "Dependency."](#)
- 19 [CNBC. "CISA director says the LOG4J security flaw is the 'most serious' she's seen in her career." December 16, 2021.](#)
- 20 [Branka Vuleta. "How Much Data Is Created Every Day? +27 Staggering Stats." Seed Scientific. October 28, 2021.](#)
- 21 [Paul Bischoff. "Ransomware attacks on US healthcare organizations cost \\$20.8bn in 2021." Comparitech. Updated October 5, 2022.](#)

Sources, continued

- 22 [Nat Bongiovanni. "A Solution to Fix Authorization." NTT DATA Blog. July 22, 2019.](#)
- 23 [National Institute of Standards and Technology. "SP 800-207 – Zero Trust Architecture." Information Technology Laboratory Computer Security Resource Center. August 2020.](#)
- 24 [Josh Fruhlinger. "The OPM hack explained: Bad security practices meet China's Captain America." CSO Online. February 12, 2020.](#)
- 25 [Kristina Jaruseviciute. "What is a Trojan Virus? How to Avoid it?" Cybernews. Updated January 18, 2023.](#)
- 26 [Dan Rafter. "What is a botnet?" Norton. May 17, 2022.](#)
- 27 [Greg Belding. "5 phishing emails that led to real-world data breaches." Infosec. June 12, 2019.](#)
- 28 [CBS News. "The phishing email that hacked the account of John Podesta." October 28, 2016.](#)
- 29 [Proofpoint. "What is Smishing?" Glossary entry.](#)
- 30 [Fortinet. "What is Smishing?" Definition.](#)
- 31 [Cybersecurity & Infrastructure Security Agency. "Alert \(AS23-025A\) – Protecting Against Malicious Use of Remote Monitoring and Management Software." January 25, 2023.](#)
- 32 [Christian Vasquez. "Cybercriminals scam two federal agencies via remote desktop tool, CISA warns." FedScoop. January 26, 2023.](#)
- 33 [Ian Duncan. "Baltimore estimates cost of ransomware attack at \\$18.2 million as government begins to restore email accounts" Baltimore Sun. May 29, 2019](#)
- 34 [Microsoft. "Cyber Signals."](#)



Visit [nttdata.com](https://www.nttdata.com) to learn more.

NTT DATA is a \$30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group.

© 2023 NTT DATA Americas, Inc. All rights reserved. 0000022023 | 1092718-NTT-DATA-Cybersecurity-A.P.P.L.E.-eBook.indd | Rev. 1.0