



accenture  Google Cloud

Ransomware State of Mind: **How to Better Protect Your Business**

Authors:



John T. Forman
Accenture

Director; Master Technology Architect



Alim H. Ali
Accenture

Director; Data Technology
and Platform Architecture



Ravi Kollipara
Sysdig

Sr Director of WW Global
System Integrator Business



Michał Kułakowski
GitLab

Senior Solutions Architect,
Global System Integrators



Tomas Gonzalez Blasini
Snyk

Senior Solution Architect
| GSI & MSSP | Alliances

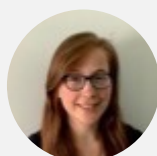


Vandana Verma Sehgal
Snyk

Security Leader



Editor:



Rachel Riedel
Accenture

Cloud Technical Architect



Table of Contents

- 04 **Executive Summary**
- 05 **Introduction**
- 06 Identify: What Exactly is Ransomware?
- 08 The Impact of Ransomware on Business
- 09 Recent Examples of Ransomware Attacks
- 10 **Mechanics of Ransomware Attacks**
- 10 Ransomware Attacks Occur in Phases
- 10 The Initial Attack Vectors
- 11 COVID-19 and the New Perimeter
- 11 Ransomware Trends Observed
- 12 **Defending Against Ransomware**
- 12 Rethink Perimeter Security
- 13 Practice Zero Trust Security
- 15 Implement Detection Mechanisms to Identify Ransomware
- 17 **Secure Your Applications**
- 17 Securing Outsourced Applications (COTS)
- 18 Securing In-House Applications
- 19 **Building Applications Immune to Ransomware Attacks Through Security In-Depth**
- 20 Declare and Configure Infrastructure as Code
- 21 Test and Validate Security
- 22 Shifting Security Testing and Remediation Left via Automation
- 23 Employ a Value Stream Delivery Platform for Auditability
- 24 **The I5R2D Principle**
- 25 **Conclusion**
- 26 **Bibliography**



Executive Summary

Today's fabric infrastructure in modern environments has unknown security gaps. Security continues to be an afterthought, as it is simply not considered a "first-class citizen." Numerous interviews with executives revealed that runtime security hardly ever appeared as part of their digital transformation endeavors.

From recent news, it is evident that basic best practices are not being applied. The attack on GitHub from April 2022, for example, involved stolen OAuth Tokens issued to third-party OAuth integrators¹. This gives cybercriminals many backdoors and opportunities to attack, which further enhances the trajectory to the current state of ransomware.

In this paper, we hope to build your awareness of ransomware attacks. We will share perspectives on how to use best-of-class tools from different domains within the cloud-native ecosystem to create patterns that will aid you in shaping your **ransomware state of mind**. With this state of mind, you can take action to protect yourself and your organization's most exposed assets — infrastructure, applications, and people — against ransomware attacks.

1. Hanley, Mike. "Security alert: Attack campaign involving stolen OAuth user tokens issued to two third-party integrators". GitHub Blog, April 15, 2022, <https://github.blog/2022-04-15-security-alert-stolen-oauth-user-tokens/>.

A photograph of two women in a busy market setting. The woman on the left is wearing a yellow floral top and is pointing at a blue smartphone held by the woman on the right. The woman on the right is wearing a yellow top, a dark blue apron, and a straw hat with a black band. They are both looking at the phone with interest. The background is filled with colorful market stalls and people, creating a vibrant atmosphere.

Introduction

Over the last couple of years, ransomware has proven to be a persistent security threat for organizations around the world. As companies have increased their digital presence, cybercriminals have sought to maximize their profits by exploiting the vulnerabilities that come with the unfamiliarity of a rapidly expanding ecosystem. Consequently, those cybercriminals have the potential to disable the technology infrastructure and thus the operations of any modern business.

Ransomware is not new in concept or execution. The first successful attack occurred in 1989. It was called the AIDS Trojan (aka the PC Cyborg).² It was distributed using floppy drives handed out to participants of a World Health Organization (WHO) conference on AIDS (hence the name). Since 2016, an average of 4,000 ransomware attacks have occurred each day. BlackFog estimates show that ransomware attacks target businesses every 11 seconds, on average.³ While not every attack succeeds, global ransomware damage losses are projected to reach \$20 billion this year.

2. Dossett, Julian. "A timeline of the biggest ransomware attacks". CNET, Nov 21, 2021, <https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/>.

3. "The State of Ransomware 2022". BlackFog, July 4, 2022, <https://www.blackfog.com/the-state-of-ransomware-in-2022/>.

In 2020, the FBI reported that total losses from ransomware in the U.S. alone increased by more than 225%.⁴

One of the contributing factors to this stark increase is the fact that, as research by Cybereason reveals, even organizations who paid ransom demands are not immune from subsequent ransomware attacks, often by the same attackers!⁵

As businesses embrace the cloud and transform themselves to become cloud-native, the need to educate on ransomware and its impacts has never been more relevant. To address these concerns, we present this paper to educate on how to leverage the cloud and cloud-native principles to shield against these ransomware attacks.

Identify: What Exactly is Ransomware?

Ransomware is a type of malicious software that puts your organization's important data at risk. Usually, but not exclusively, it is delivered through spear phishing emails. Once ransomware infects a computer system, it targets critical data and restricts users' access to said data until a ransom is paid to unlock it.

There are several attack vectors of ransomware through which a computer can be attacked. The most common ones are:

- Phishing spam
- Social engineering
- Remote desktop/terminal protocol (RDP)
- Software vulnerabilities

4. "Internet Crime Report 2020". Federal Bureau of Investigation: Internet Crime Complaint Center, 2021, https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

5. Curry, Sam. "Report: Ransomware Attacks and the True Cost of Business". Cybereason, June 16, 2021, <https://www.cybereason.com/blog/research/report-ransomware-attacks-and-the-true-cost-to-business>.

Phishing and Social Engineering

Using links, attachments, or even both, an email phishing attack entices users into taking some sort of action in an attempt to obtain their data. These emails may contain links that appear to have come from a known and trusted contact, but, in actuality, they are asking a user to enter credentials for a nefarious purpose. Other tactics include asking the user to click on a fake attachment, after which ransomware automatically begins downloading.

It is important to note that, in Q4 of 2020, phishing rose to #1 as the most-used ransomware attack vector.

Unsecured RDP

Though RDP is, narrowly, the second-most popular attack vector, it accounts for the most successful attacks since it is cheap, easy, and highly available. RDP ports are often poorly secured and easily compromised, either by brute force attacks or credential stuffing.

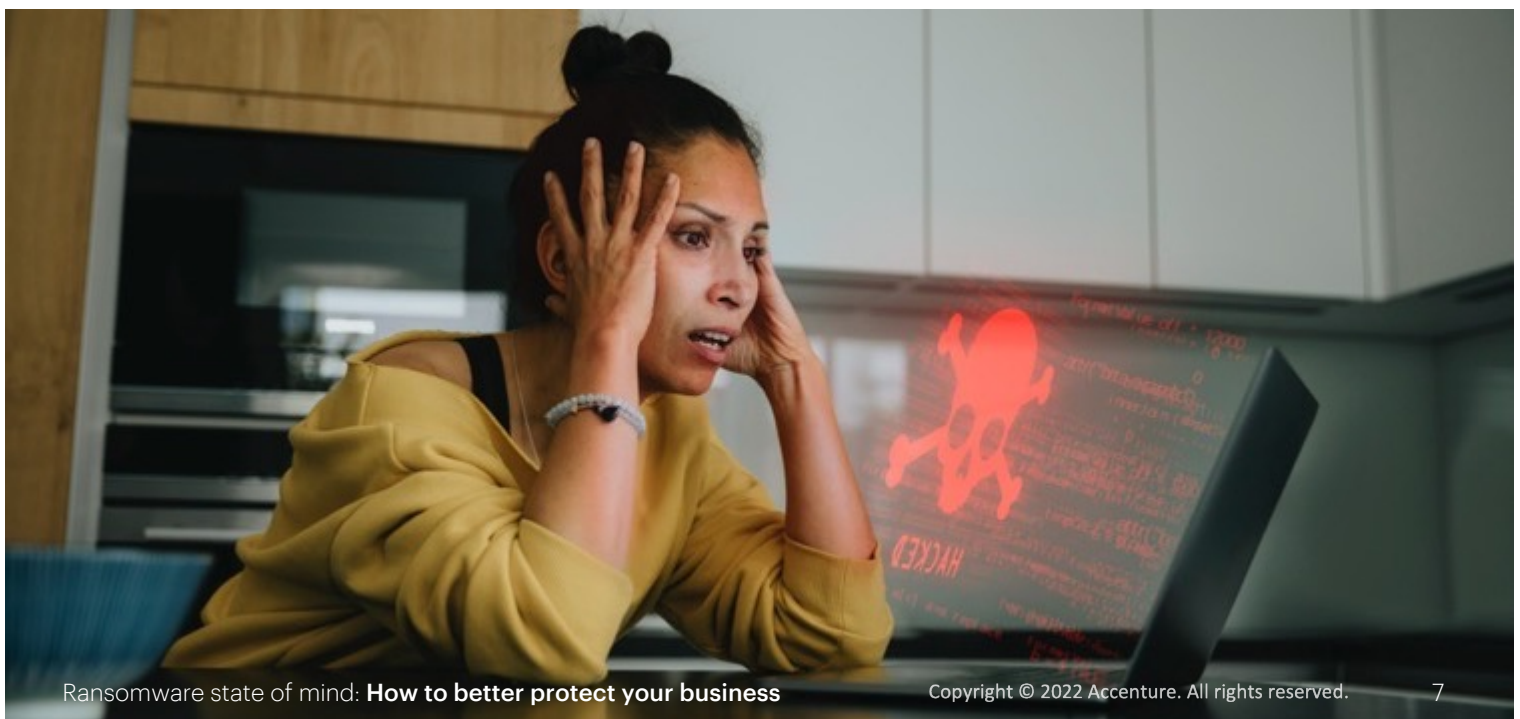
Once attackers acquire credentials and obtain access, **they can bypass endpoint protection and begin wreaking havoc on enterprise systems**, including wiping or encrypting data backups.

Software Vulnerabilities

The software vulnerabilities attack vector may use a phishing email as the initial vector, but it is not the ransomware payload's delivery vector. Instead, something such as an email serves to open the front door for the exploit kit, which functions as the delivery vector since it evaluates the visitor's web browser, operating system, and/or other software for vulnerabilities. If the exploit kit detects a supported vulnerability, it "wakes up" and activates its exploit code to install ransomware on the victim's machine.

This type of scenario is known as a **"drive-by download."** Attackers can set up their own websites to conduct drive-by downloads. To do so, however, they need to use redirect chains, typo-squatting, and other evasive tactics. Otherwise, email gateways will flag their embedded links outright. Alternatively, attackers can attempt to compromise a legitimate website, misusing its reputation to distribute malicious code.

Beyond these attack vectors, the hasty adjustments companies made to accommodate changing work conditions as a result of COVID-19 — such as extending the corporate network perimeter to employee homes — brought upon a new set of challenges.



The Impact of Ransomware on Business

Gartner estimates that, by 2025, at least 75% of IT organizations will have faced one ransomware attack or more. Researchers have documented an increase in ransomware attacks during 2020, pointing to sevenfold or higher growth rates. According to International Data Corporation's (IDC) 2021 Ransomware Study, "approximately 37% of global organizations said they were the victim of some form of ransomware attack in 2021."⁶ The FBI's Internet Crime Complaint

Center reported 2,084 ransomware complaints from January to July 31, 2021, representing a 62% increase year-over-year.⁷

What does this mean for the business of organizations? Ransomware attacks can negatively impact an organization in many ways, with combined losses potentially reaching into the tens or even hundreds of millions of dollars.

Short-term implications of ransomware attacks can include:

- Being unable to access data
- Costs associated with incident response, recovery, and mitigation efforts
- Interruption of business processes and lost productivity
- The ransom payment (if the organization chooses to acquiesce to the extortion demand)
- Reputation loss and litigation costs related to attackers releasing stolen data, including customer records

According to Cybereason's Sam Curry, the long-term consequences of ransomware attacks are the following.⁸

Loss of business revenue:

66% of organizations reported a significant loss of revenue following a ransomware attack.

Ransom demands increasing:

35% of businesses paid ransoms between \$350,000-\$1.4 million, while 7% paid ransoms exceeding \$1.4 million.

Brand and reputation damage:

53% of organizations indicated that their brand and reputation were damaged because of a successful attack.

C-Level talent loss:

32% of organizations reported losing C-Level talent as a direct result of a ransomware attack.

Employee layoffs:

29% reported being forced to lay off employees due to financial pressures following a ransomware attack.

Business closures:

A startling 26% of organizations reported that a ransomware attack forced the business to close operations for some period of time.

Business critical projects:

Put on hold because access to vital resources is suspended, with restoration of data taking weeks to be made available.

6. Dickson, Frank and Christopher Kissel. "IDC's 2021 Ransomware Study: Where You Are Matters!". IDC, July 2021, <https://www.idc.com/getdoc.jsp?containerId=US48093721>.

7. "Alert (AA21-243A): Ransomware Awareness for Holidays and Weekends". Cybersecurity & Infrastructure Security Agency, August 31, 2021, <https://us-cert.cisa.gov/ncas/alerts/aa21-243a>.

8. Curry, Sam. "Report: Ransomware Attacks and the True Cost of Business". Cybereason, June 16, 2021, <https://www.cybereason.com/blog/research/report-ransomware-attacks-and-the-true-cost-to-business>.



Recent Examples of Ransomware Attacks

The media are plagued by kidnap and ransom stories these days. However, these stories are not about people. Instead, they are about data, the lifeblood of any organization, being held for ransom. These recent high-profile attacks demonstrate that ransomware is aimed at disrupting the operations of its target in order to create the incentive to pay the ransom. Some recent examples where public security was jeopardized, and victims paid the ransom include:

Colonial Pipeline

an American oil pipeline system, suffered a ransom attack that impacted computerized equipment managing their pipeline. The attack caused fuel shortages along the east coast, leading to massive queues in gas stations and surging gasoline prices.⁹

JBS Foods

a major food processing company, was forced to stall some of its production plants due to a ransomware attack.¹⁰

CD Projekt

a video game company behind games like The Witcher and Cyberpunk 2077, was attacked and threatened with having their intellectual property and employee information released to the public should they refuse to pay the ransom.¹¹

These are just some of the many high-profile names attacked in 2021/22. Others include Brenntag (chemical distribution company), Acer (computer manufacturer), Quanta (Apple supplier), NBA, AXA, 7-Eleven, and many more.

9. Shwartz, Michael, and Nicole Perlroth. "Darkside, Blamed for Gas Pipeline Attack, Says it Is Shutting Down". The New York Times, May 14, 2021, <https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html>.

10. "Meat giant JBS pays \$11m in ransom to resolve cyber-attack". BBC, June 10, 2021, <https://www.bbc.com/news/business-5742300>.

11. Humphries, Matthew. "Cyberpunk 2077 Developer Suffers Cyber Attack and Ransomware Demand". PCMag, February 9, 2021, <https://www.pcmag.com/news/cyberpunk-2077-developer-suffers-cyber-attack-and-ransomware-demand>.



Mechanics of Ransomware Attacks

The scope and nature of ransomware attacks are often misunderstood. Thus, inadequate precautions and responses, both active and passive, can result in successful attacks. To better prevent ransomware attacks, it helps to understand the mechanics of how an actual attack operates.

Ransomware Attacks Occur in Phases

A ransomware attack is a phased activity, meaning there is a time gap between the initial infection and the ransom event. For example, the AIDS Trojan bore its fangs after the computer booted up 90 times. During this time, attackers may remain hidden and attempt lateral

movement to build an inventory of resources at the compromised organization, identify those of value, and elevate their privileges accordingly by exploiting network-based trust relationships.

The Initial Attack Vectors

While the effectiveness of lateral movement attempts varies and depends on the environment, similarities between how attacks begin have been documented. Usually, attacks originate from a compromised endpoint, such as a personal computer or mobile device that has access to the target network. Personal endpoints

are a favorite among attackers because they are notoriously hard to patch, there are a great number of them, and their operators do not usually possess security expertise.

Coveware’s Ransomware Marketplace Report digs deeper into how endpoints become compromised, stating that 50% of attacks start with unsecured RDP ports, around 25% by phishing email, and 12% due to software vulnerabilities.¹²

None of this is new information. Unsecured RDP is a well-known issue, and phishing has existed for decades. Both have known safeguards that can be used to prevent them, including proper configuration and user awareness campaigns, respectively. Still, because of the significant attack surface, these two issues combined are responsible for over 75%+ of ransomware attacks. Just one user responding to a phishing probe or one open RDP endpoint existing is necessary for the attack to succeed.

COVID-19 and the New Perimeter

At the start of the pandemic, most organizations were forced to adopt a “work from home” paradigm, even though many were not ready for it. Many had to modernize from how they had traditionally approached security. Traditional security mechanisms are based on a castle and moat concept (aka perimeter security), which segregates privileges based on the network from which the attacker is connecting, rather than his or her personal identity.

This universally acknowledged but still widespread omission played a major role in making ransomware attacks possible when employees started working from home. Though the (fire)walls of the office had previously served as the edge of the security perimeter, many SOCs found themselves inadequately prepared to handle the increased attack surface area of the perimeter needed to support a remote workforce.

Ransomware Trends Observed

As ransomware became more mainstream, two interesting trends appeared. The first is double extortion. Since high-profile attacks are targeted, meaning there is a person behind them looking at the data and determining the best angle from which to extract the ransom, they often have multiple threats attached to them. For example, a cybercriminal can threaten both with encrypting data and deleting backups internally and leaking sensitive data to the public.

The second is Ransomware as a Service (RaaS). Cybercriminals are splitting the “value chain” of an attack. One group becomes a ransomware software provider, e.g., such as the now-defunct DarkSide or REvil, while the other is the actual group committing the crime, often referred to as “the affiliate.” This scheme not only helps attackers avoid some criminal charges, but also significantly lowers the entry bar for someone willing to earn money this way, making it popular among both existing and new cybercriminals.

12. “Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020”. Coveware, April 29, 2020, <https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>.



Defending Against Ransomware

Now that we've provided an initial context to help you become more familiar with ransomware, its attack vectors, and the mechanics of a ransomware attack, let's dive into how you can defend against malicious actors looking to cripple your operations.

Rethink Perimeter Security

As mentioned above, traditionally, IT security was based on the concept of a secure perimeter, like a moat around a castle. The moat is effective if attackers stay out, but once crossed, it becomes useless. In IT, the moat represents the boundaries between network segments. This approach to security was born due to the realities of how applications were traditionally built- hard to understand and very slow to change. Filtering network traffic based on policies became the security approach of choice, especially since policies could be adapted quickly in response to an attack.

In the cloud era, this reactive approach comes with significant shortcomings:

- Filtering network traffic is an afterthought that assumes the application is vulnerable and needs to be protected. There is nothing wrong with doing this, as there is nothing wrong with managing endpoints well. However, this should not be a core defense line.
- Once an attacker is already inside, network policies around the perimeter become useless.

For example, if there is an infected terminal connecting over a VPN, we would need to move defense back to where it is due — next to the data. Traditionally, the answer would've been to build more moats. However, cloud-native applications are not built like castles.

In a Kubernetes setting, thousands of pods exist concurrently. Pods are deployed and decommissioned on multiple nodes many times per day as applications scale out and back in, making it extremely difficult to add additional policies. Imagine building moats where all the buildings are moving!

Practice Zero Trust Security

Beyond a reactive defense, zero trust security is another component of a robust ransomware defense strategy. Zero trust boils down to never assuming any of the implied trust relationships between application services, applications, and users; it's a deviation from the traditional "trust but verify" model. If privileges are ever granted, they are given based on an authenticated identity. In a zero-trust model, there is no need for a perimeter or moats. Each component is responsible for verifying the requestor and which privileges they should have.

Traditionally, such a principle has been difficult to implement in applications released quarterly or bi-yearly.

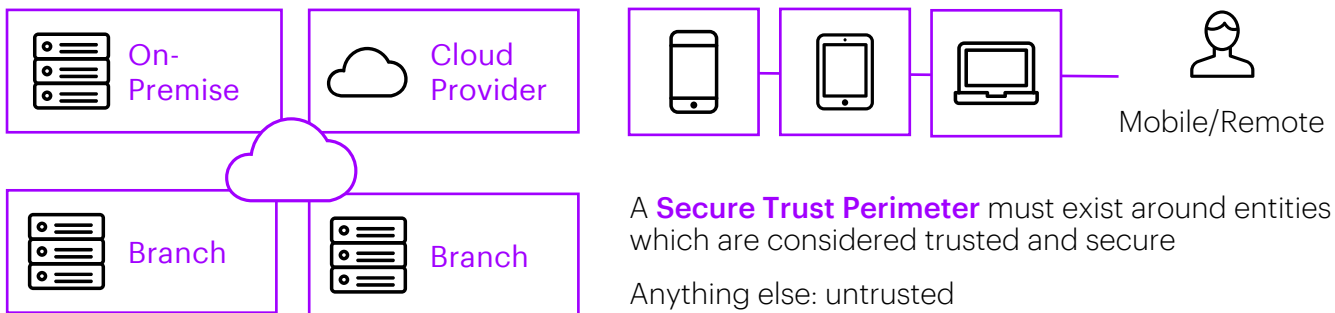
Fortunately, the growing pace of change comes to the rescue. Modern cloud-native applications are built on small services, which are easy to change. Consider a case where a vulnerability is detected in an application service, allowing for exploitation by an unauthenticated agent or escalation of privileges. A traditional security response would be to build a perimeter in front of this service or tinker with an existing one. Instead, a cloud-native application only needs to update the service or services. This change is not only much simpler to implement but also the change more durable, carrying a low probability that someone will accidentally undo it in the future.



Zero Trust at Work: Implementing Secure, Trusted Perimeters

One example of a zero-trust architecture pattern is a Secure Trusted Perimeter (STP). STPs are boundaries established around entities from an organizational perspective, considered trusted and secure. With work-from-home initiatives and employee mobility, the STPs must also extend to worker's end devices.

Secure Trust Perimeter (STP)



STPs are built according to the following principles:

- Address gaps and patterns with SLAs, policies and procedures, functionality, operations, and partnerships with trusted vendors.
- Consider everything else as “untrustworthy.”

But this is only part of the big picture — it is more important to determine what traffic is supposed to enter these STP perimeters.

Leverage Multi-Factor Authentication

Zero trust security is often accompanied by multi-factor authentication (MFA). This plays an enormous role in blocking infected terminals and stopping attackers from elevating their privileges.

MFA requires users to consciously submit additional authentication information — typically either biometric data or proof they own a token — for high-risk operations. This way, even if a

terminal has been hacked and the user password has been eavesdropped, the attacker cannot take action on behalf of the user.

An application is free to determine which actions carry a high-enough risk needed to justify MFA. For example, it is legally required for any European bank to require an MFA for online card transactions since such transactions pose such a high risk.



Implement Detection Mechanisms to Identify Ransomware

Conceptual solutions need to have a run-time threat detection mechanism based on open-source projects like Falco.¹³ The solution needs to define a baseline of known “good behavior” to then use Artificial Intelligence (AI) and Machine Learning (ML) models to ingest data from real-time events and detect suspicious behavior. Events can be used to define signatures that

trigger data-driven alerts, including evidence from system call data and running processes. The alerts can then be exposed via IDS/IPS or SIEM/SOAR systems for SOC analysts to conduct further investigation in real-time.

Zero Trust at Work: Protect Against Anomalous Behaviors Using Quarantine Zones



What Is Happening?

- The quarantine zone (QZ) within the STP proactively scans traffic ingressing or egressing across the STP perimeter. It is used to analyze and detect any anomalies among patterns, derived with the aid of trusted vendor software designed to analyze the data.
- Within the QZ, mal-traffic is isolated and not allowed to propagate further within. Traffic should be intensely analyzed to derive its “intention.”
- Traffic is dropped, researched, logged, or subjected to scrutiny by SOC and security vendors.
- For remote/mobile devices, QZ Endpoint Mobile Device Agents (qzEMDA) should be deployed to remain consistent.
 - Smart NICs with AI/ML provisioning


13. Falco, <https://falco.org/>.

Re-Evaluate Endpoint Security Tools

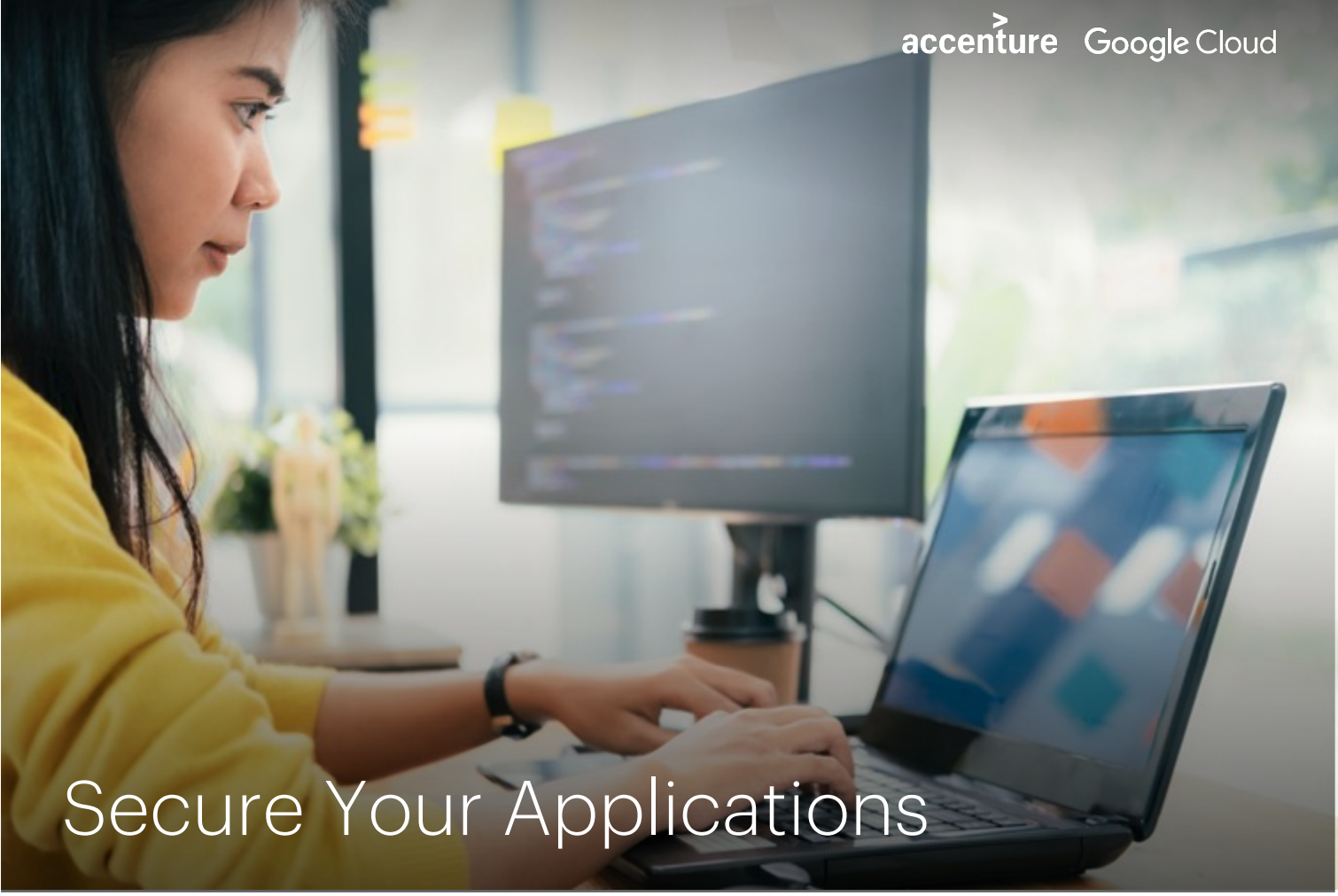
The changing application landscape has shown that legacy endpoint security tools aren't as effective at preventing advanced attacks, as SOC teams are constantly adjusting to increasingly complex environments. Failing to re-evaluate outdated policies can create unnecessary noise, leaving your SOC with performance issues and policy drifts.

Consider if your endpoint security tooling allows you to:

- Endpoint security management is easier with a centralized infrastructure. It is also more accurate and saves time for you and your IT staff. Provide a single lightweight agent that doesn't negatively impact terminal performance.
- Leverage analytics to capture real-time activity data from all endpoints, analyze it for anomalous behavior, and create a global threat monitoring system. Using sophisticated machine learning and analytics processes that study behaviors, file reputations, threat feeds, and other data sources, the cloud proactively identifies anomalies as they occur.
- Analyze unfiltered data, whether related to a threat or not, to accelerate your ability to zero in on new attacks and take immediate action. In addition, this data can be used as input for next-gen AI modeling of cyberthreats.



Endpoint security is still part of a robust ransomware defense strategy. In addition to the considerations mentioned above, ensure your endpoint security provider uses a data-driven approach to endpoint security.



Secure Your Applications

Zero trust can reduce the chances that attackers gain access through your perimeter, but it doesn't replace the need to ensure the application landscape is secure in case attackers manage to break in. Zero trust can be augmented by hardening the application landscape.

Securing Outsourced Applications (COTS)

For outsourced, Common Off The Shelf (COTS) applications, typically delivered in the SaaS model, choose reputable vendors and apply MFA when possible. Independent certifications exist to assess the security processes of an Independent Software Vendor like SOC2 or ISO 27001. Once you select a vendor, application security becomes their contractual responsibility.

Securing In-House Applications

1. Securing in-house applications is critical for two main reasons: In-house applications are often one-of-a-kind, competitive differentiators situated at the center of critical business processes and thus have access to all sorts of data.
2. In-house applications introduce a massive number of attack vectors, many stemming from the development and operations team’s implementation decisions. For example,
 - a. Infrastructure misconfigurations, including credential leaks, unencrypted and publicly accessible storage buckets, and open-to-the-world load balancers.
 - b. DevSecOps toolchain vulnerabilities, such as unauthorized access to hosts and storage, pipeline plugins (integrations), and misconfigured settings and scripts.
 - c. Open-source supply chain issues via application dependencies (libraries, base images), resulting in dependency confusion, artifact injection, and unmanaged binaries.
 - d. Human/developer error or lack of experience, often around insecure coding practices.
 - e. Lack of build integrity, including unauthorized tampering with the build and/or with the deployment rules.

Unfortunately, the monitoring for and addressing of these highlighted points becomes more difficult as development teams adopt Agile and DevOps methodologies and as applications are modernized and refactored. For example:

1. The complexity of the tooling used to develop applications grows over time as the cloud provider delivers more services in the PaaS model.
2. The number of services composing modern cloud-native applications grows as teams introduce tooling, languages, frameworks, and practices.

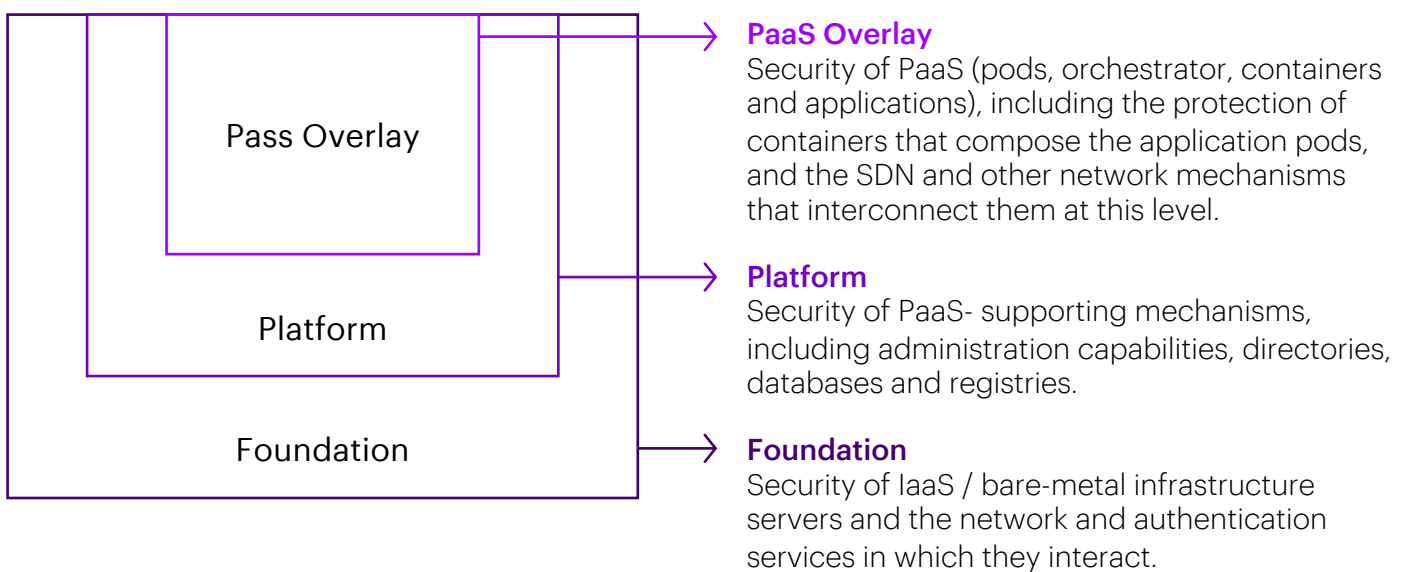
The combination of the above leads to an explosion of complexity, resulting in limited visibility, security management issues, and increased risk. In the remainder of this paper, we will focus on best practices related to secure app development with an emphasis on building immunity to ransomware.



Building Applications Immune to Ransomware Attacks Through Security In-Depth

Review of each of the protection designed security layers to ensure general security principles have been applied to the environment to minimize threats and vulnerability exposure.

Security controls and measures are organized and established in three different layers:



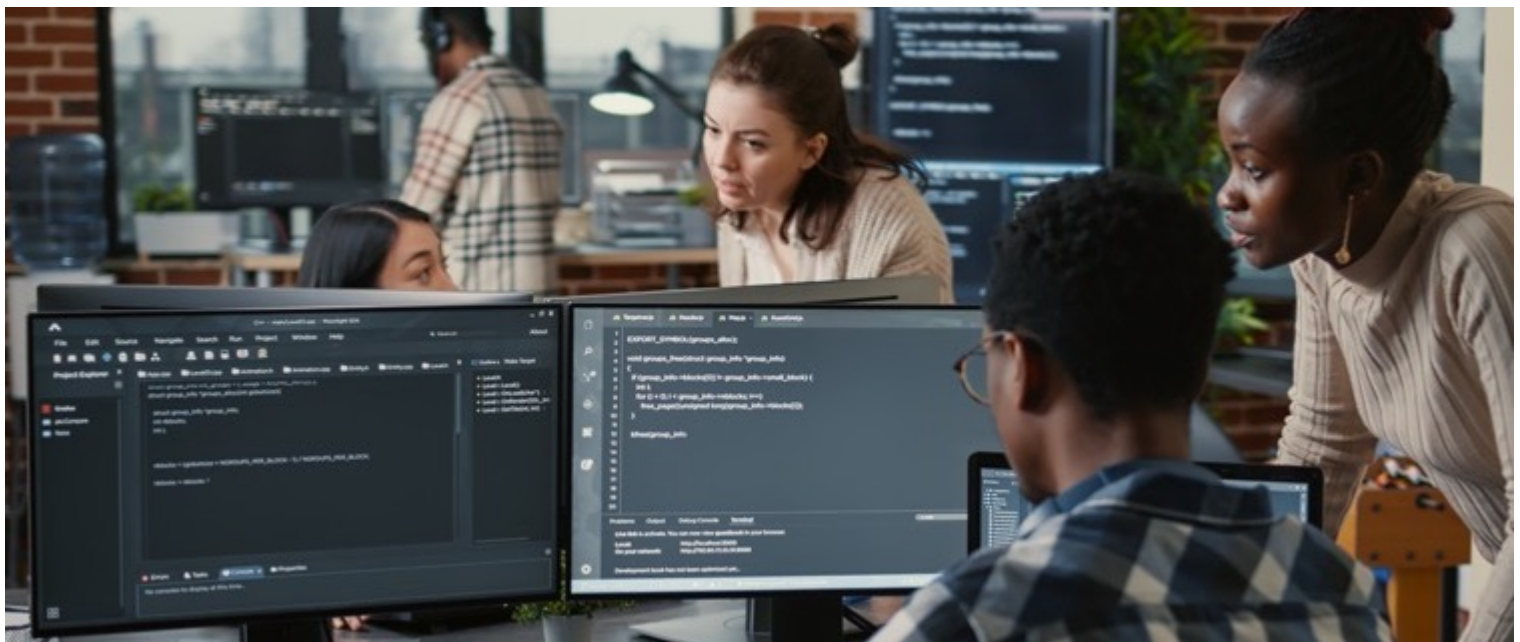
Declare and Configure Infrastructure as Code

An application is not just code — it is code deployed onto infrastructure configured to run as code. Infrastructure security is paramount. Most cloud-native applications are packaged into containers and deployed into a container platform orchestrated by some flavor of Kubernetes (AKS, EKS, GKE, etc.).

An increasingly popular best practice for secure infrastructure change management is GitOps, an operational framework that takes DevOps recommendations used for application development such as version control, collaboration, compliance, and CI/CD and applies them to infrastructure automation¹⁴, encourages:

1. Expressing all the infrastructure definitions as code (e.g., YAML files).
2. Maintaining and managing a single source of truth by versioning infrastructure configuration in a Source Code Management system
3. Automating a two-way enforcement process to retain consistency and prevent drift by:
 - a. Ensuring every change in the repository is applied to the actual cluster.
 - b. Ensuring every out-of-band change gets rolled back.
4. Expressing every Change Request as a branch in the source-code management (SCM) repository and every “change” as a merge to master branch, subject to approval.

By practicing GitOps, any attempts to modify infrastructure are completely visible and subject to the usual approval processes, where they can be either accepted and merged or rejected and rolled back.



14. “What is GitOps?”. GitLab, <https://about.gitlab.com/topics/gitops/>.

Test and Validate Security

There is a wide array of risks to screen for when building an application's container images.

Insecure Source Code

Due to many possible reasons, including developer inexperience, human error, or malicious intent, source code may contain security vulnerabilities that compromise the application or quality defects that negatively impact its performance. Employing a Static Application Security Test (SAST)¹⁵ scanner to “spell check” the code is an easy way to help developers avoid these kinds of issues.

Open-Source Vulnerabilities

According to the 2021 Snyk State of Cloud Native Application Security Report, 45% of the responding organizations building cloud-native applications suffered from an incident resulting from a known vulnerability.¹⁶ To avoid this, open-source libraries should be screened for potential vulnerabilities that may be introduced indirectly as libraries, dependencies, or container base images.

Attestations as Checkpoints

Checks for each of these risks should be reflected with attestation, and a record of provenance that the image complies with the risk policy at release time should be maintained. If an image changes infrequently, it may require periodic re-scans to detect newly disclosed vulnerabilities. Attestations should be verifiable by anyone in the organization and tested and validated by the deployment process. In cases where break-glass is required, those should be logged for tracking purposes.

Ensuring the Immutability of Artifacts

The next link in the security chain is ensuring the integrity of the deployed artifacts. You may run every type of test as container images are developed and built, but none of them are useful if they can be modified on their way to deployment. The foundation of a secure architecture is ensuring provenance and immutability; that is, each deployable artifact must come from a known source and cannot be changed. Like infrastructure and configuration, if new functionality is required, a new version of an artifact is built and certified before deployment.

Promoting Artifacts Securely (as Code)

Typical enterprise software release processes depend on a range of increasingly complex environments. For example, testing a particular service interface may only require that service to be deployed. However, testing complex workflows can require its own complete environment or simulation of one. Testing performance can also require a scaled copy of an application.

Since complex environments are more expensive to build, teams logically carry out simple tests first to catch bugs as quickly and efficiently as possible. The mechanism for promoting an image from one environment to another and asserting it for further promotion is commonly referred to as Continuous Deployment (CD). This piece of automation carries its own logic and is subject to change. Therefore, it should be expressed as code too, and managed in the SCM. CD logic modification is particularly dangerous as it can circumvent all the container image assertions (by introducing a rogue image into the process). Managing CD logic as code makes unauthorized change impossible at best and visible at worst.

15. SAST is a testing methodology that analyzes source code to find security vulnerabilities that make your organization's applications susceptible to attack.

16. “The 2021 State of Cloud Native Application Security”. Snyk, 2021, <https://go.snyk.io/2021-state-of-cnas-report>.

Shifting Security Testing and Remediation Left via Automation

Continuous Deployment contains a dangerous hidden circular dependence responsible for many DevSecOps failures.

The process depends on a quick Mean Time to Resolve (MTTR), yet additional checks, verifications, and attestations slow it down. It is easy to overload the whole release process and end up stalling it, which goes against all DevOps values.

The act of scanning itself doesn't slow the process down as much as human wait times. Consider that developers are the change authors who remediate any vulnerabilities identified. Running scans out of the developer context or delivering results days or weeks after a code push can take a long time to take action due to competing priorities. The solution is to shift security left, which executes automated tests early and presents results to developers in the context of their workflows.

Test on Branch Merge

One point in the process that is particularly suited for automated testing is the feature branch merge. Agile methodologies insist that the feature branch (a branch representing actual change owned by the individual coding it) is short-lived and merged early. Long-lived feature branches introduce the risk of merge conflicts, i.e., what a developer is working on does not correspond to the rest of the application code anymore, and their work is wasted.

That said, merging a code that is not completely tested introduces a risk, too, since the code may be difficult or impossible to pull back later, when others rely on its existence for their changes. The only way to mitigate this risk is by building a dedicated environment for complete security testing dynamically for every feature branch, executing the tests in question there, and presenting the results to the code review team.

This leaves them with full flexibility to select one of the following:

- Fix the vulnerabilities
- Accept the risk by ignoring the vulnerability
- Postpone the work until a solution is found

Inform Developers Prior to Code Commit

Once the team reaches a decision, they present developers with the information needed to help them remediate the issue. Rather than simply sending developers a report with all the issues to fix, shifting remediation left is most effective when you present them the information in the context of the dev flow in their workstation, with background information about how to fix the issue and where in the code the issue lies.

As a result of this approach, the risk of a vulnerability slipping to production is reduced, as is the risk of release delay because of vulnerabilities surfacing late. Finally, the psychological comfort of developers improves. They know when their work is accepted as complete and do not fear being hunted down by security teams with an urgent fix.

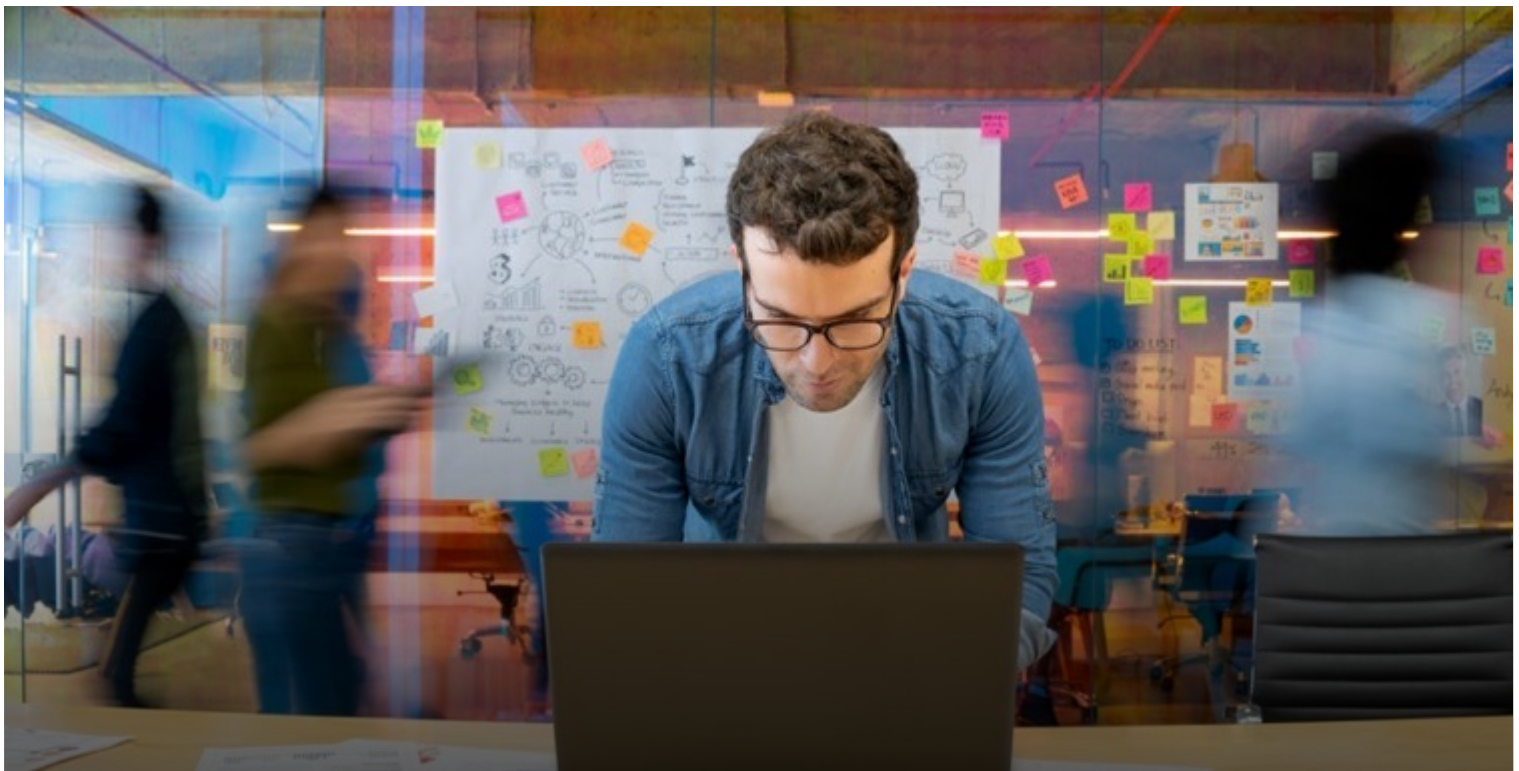
Employ a Value Stream Delivery Platform for Auditability

All of the processes discussed above can be automated in software that Gartner refers to as a “Value Stream Delivery Platform.”¹⁷ It encompasses all the facilities needed to turn an idea into code and into a production application, including issue management, source code management, continuous integration, continuous delivery, environment management, vulnerability management, and monitoring. This platform is a cornerstone of a secure, ransomware-proof application, as anyone capable of hacking this platform would have to take over the whole process.

Leveraging a Value Stream Delivery Platform allows you to audit the whole process:

- Who carried out what change, and when?
- Was this change successful?
- Who approved it?
- What was the motivation?

Once everything is managed as code, these questions are addressed by a series of code commits. Here, again, having a single platform to rely on helps greatly, as every activity can be easily mapped to specific users, and there is a single audit trail representing said activities.



17. Bhat, Manjunath, Thomas Murphy, Daniel Betts, Chris Saunderson, Hassan Ennaciri, and Joachim Herschmann, “2021 Gartner Market Guide for Value Stream Delivery Platforms”. Gitlab, October 18, 2021, <https://about.gitlab.com/analysts/gartner-vsdp21/>.

The I5R2D Principle[®]

Ransomware can have a high level of visibility. As your company matures, so must its resiliency. The I5R2D Principle[®], developed by Accenture's Alim H. Ali, provides an approach that should be in place to lead an organization's best defense against ransomware.

The I5R2D Principle[®] consists of the following actions:

Impact

Quantify the consequences of ransomware and the lasting effect it has on an organization's business and continued viability, reputation, and vertical value.

Identify (informally)

Consider how the threat is being perpetrated currently and how it could potentially happen in the future.

Identify (operationally)

Utilize detection mechanisms to proactively scan for ransomware patterns.

Implement

Implement the architecture, tooling, and models needed to support the detection and identification of current ransomware patterns while simultaneously learning and building new models for potential future versions of ransomware patterns.

Isolate and Remediate

Utilize quarantining, Secure Trust Perimeters (STPs), and Quarantine Zones (QZs) to help mitigate the effects of a ransomware pattern.

Report and Depose

Document the events of what occurred during a ransomware attack, how it was identified, what measures were taken, and how the event was handled, in addition to reporting to the required authorities, including CISO, SOC, government agencies, and local authorities.

Including this principle in your organization's security framework can greatly reduce exposure and help mitigate threats caused by ransomware.



Conclusion

Security is now more important than ever, especially with the increasing popularity of ransomware attacks. **Security must be implemented correctly and effectively across an organization.** A secure trust perimeter and quarantine zones are just some of the aspects needed for an effective security setup. In addition, the “shift-left” DevOps approach, securing an organization’s DevSecOps pipeline, can greatly reduce numerous vulnerabilities and aid in the overall safety of an organization’s applications and intellectual property.

Criminal cyberattacks will be around for the foreseeable future. However, we can help reduce the blast radius of ransomware attacks by following the principles and concepts from this paper.

By keeping a ransomware state of mind, your organization can be better prepared to secure its IT landscape today and in the future.

Bibliography

"Alert (AA21-243A): Ransomware Awareness for Holidays and Weekends". Cybersecurity & Infrastructure Security Agency, August 31, 2021, <https://us-cert.cisa.gov/ncas/alerts/aa21-243a>.

"Berkley Information Security Office FAQ". UC Berkely, <https://security.berkeley.edu/faq/ransomware/>.

Bhat, Manjunath, Thomas Murphy, Daniel Betts, Chris Saunderson, Hassan Ennaciri, and Joachim Herschmann, "2021 Gartner Market Guide for Value Stream Delivery Platforms". GitLab, October 18, 2021, <https://about.gitlab.com/analysts/gartner-vsd21/>.

"Container Threat Detection". Sysdig, 2022, <https://sysdig.com/learn-cloud-native/container-security/threat-detection/>.

Curry, Sam. "Report: Ransomware Attacks and the True Cost of Business". Cybereason, June 16, 2021, <https://www.cybereason.com/blog/research/report-ransomware-attacks-and-the-true-cost-to-business>.

Dickson, Frank and Christopher Kissel. "IDC's 2021 Ransomware Study: Where You Are Matters!". IDC, July 2021, <https://www.idc.com/getdoc.jsp?containerId=US48093721>.

Dossett, Julian. "A timeline of the biggest ransomware attacks". CNET, Nov 21, 2021, <https://www.cnet.com/personal-finance/crypto/a-timeline-of-the-biggest-ransomware-attacks/>.

Ensor, Mike, and Drew Stevens. "Shifting left on security". Google Cloud, February 25, 2021, <https://cloud.google.com/files/shifting-left-on-security.pdf>.

Falco, <https://falco.org/>.

Freed, Anthony M. "What are the Most Common Attack Vectors for Ransomware?". Cybereason, November 2, 2021, <https://www.cybereason.com/blog/what-are-the-most-common-attack-vectors-for-ransomware>.

Fruhlinger, Josh. "Ransomware explained: How it works and how to remove it". CSO, June 19, 2020, <https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remove-it.html>.

Hanley, Mike. "Security alert: Attack campaign involving stolen OAuth user tokens issued to two third-party integrators". April 15, 2022. GitHub Blog, <https://github.blog/2022-04-15-security-alert-stolen-oauth-user-tokens/>.

Harrison, Margret. "Top 3 Attack Vectors Ransomware Loves to Exploit". Digital defense by HelpSystems, <https://www.digitaldefense.com/blog/top-3-attack-vectors-ransomware-loves-to-exploit/>.

"How to Protect Your Networks from Ransomware". Computer Crime and Intellectual Property Section, <https://www.justice.gov/criminal-ccips/file/872771/download>.

Humphries, Matthew. "Cyberpunk 2077 Developer Suffers Cyber Attack and Ransomware Demand". PCMag, February 9, 2021, <https://www.pcmag.com/news/cyberpunk-2077-developer-suffers-cyber-attack-and-ransomware-demand>.

"Internet Crime Report 2020". Federal Bureau of Investigation: Internet Crime Complaint Center, 2021, <https://www.ic3.gov/Media/PDF/AnnualReport/2020/IC3Report.pdf>.

Kelley, Diane. "Top 3 ransomware attack vectors and how to avoid them". TechTarget, September 2021, <https://searchsecurity.techtarget.com/tip/Top-3-ransomware-attack-vectors-and-how-to-avoid-them>.

"Meat giant JBS pays \$11m in ransom to resolve cyber-attack". BBC, June 10, 2021, <https://www.bbc.com/news/business-57423008>.

"Ransomware Payments Up 33% As Maze and Sodinokibi Proliferate in Q1 2020". Coveware, April 29, 2020, <https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report>.

"Ransomware: The True Cost to Business". Cybereason, 2021, https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf.

Scroxtion, Alex. "Phishing back in vogue as ransomware vector". ComputerWeekly.com, Jun 29, 2020, https://www.computerweekly.com/news/252485340/Phishing-back-in-vogue-as-ransomware-vector?_gl=1*13mbczq*_ga*MTM0MDAwMDYzOS4xNjM3MTcwODI0*_ga_TQKE4GS5P9*MTYzNzE3MDgyMy4xLjAuMTYzNzE3MDgyMy4w&_ga=2.231963039.1438816154.1637170824-1340000639.1637170824.

Shwartz, Michael, and Nicole Perloth. "Darkside, Blamed for Gas Pipeline Attack, Says it Is Shutting Down". The New York Times, May 14, 2021, <https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html>.

"The 2021 State of Cloud Native Application Security". Snyk, 2021, <https://go.snyk.io/2021-state-of-cnas-report>.

"The State of Ransomware 2022". BlackFog, July 4, 2022, <https://www.blackfog.com/the-state-of-ransomware-in-2022/>.

"The True Impact of Ransomware Attacks". Threat Post, July 26, 2021, <https://threatpost.com/true-impact-of-ransomware-attacks/168029/>.

"What is GitOps?". GitLab, <https://about.gitlab.com/topics/gitops/>.

"What is Container Security?" Sysdig, 2022, <https://sysdig.com/learn-cloud-native/container-security/what-is-container-security/>.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Technology and Operations services and Accenture Song — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 710,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities.

Visit us at [accenture.com](https://www.accenture.com)

Accenture Google Business Group

When you put the biggest and most innovative companies in the world together, amazing things happen.

The Accenture Google Business Group combines Accenture intelligence with Google innovation to bring the promise of technology and human ingenuity to our enterprise clients.

Intelligent Innovation starts here
www.accenture.com/google



Accenture was awarded 2021
Google Cloud Global Services
Partner of the Year

accenture > **Google Cloud**