Cloud Native Corporate IT Infrastructure

Modernizing IT with Cloud Native patterns

Reports of ransomware attacks punctuate the news cycle with increasing regularity. From city services in Atlanta to Baltimore's 911 system to a Boeing manufacturing facility, these attacks can disrupt operations and threaten the security of organizations everywhere. That's why Chris Borte, InsideTrack's director of information technology, made it a priority to develop an IT infrastructure that would be impervious to ransomware. His solution was to move InsideTrack to a cloud native architecture that not only secures InsideTrack's network, but also enhances flexibility and productivity. In the following white paper, Borte discusses the advantages of going cloud native and offers tips for organizations that are ready to modernize their IT system.

What is cloud native?

"Cloud native" is increasingly being used as a marketing term. But as Justin Garrison and Kris Nova point out, "It can still be meaningful for Engineering and Management."[1]

Broadly, it assumes and likely depends upon public cloud infrastructure that didn't exist a decade ago. Cloud native goes beyond simply copying legacy on-premise solutions in their current form into the cloud. Rather, it involves higher levels of abstractions with public cloud, scalability, and internet-hardened security as first-class priorities rather than afterthoughts. As the name implies, the solution is native to the cloud.

Cloud native vs "In the Cloud"

Unfortunately simply lifting legacy anti-patterns into the cloud results in services that are nominally in the cloud but still have most, if not all, the weaknesses, vulnerabilities and risks associated with legacy corporate IT infrastructure. How does an organization differentiate when evaluating SaaS? When researching providers, here are some common hallmarks to look for:

- Public API
- SSO as default
- Free tier, or "try before you buy" with self registration
- Open documentation that doesn't require login
- Not only monthly pricing but monthly billing allowing for cancellation anytime
- OS agnostic (including ChromeOS) or web-based client software
- Real-time collaboration
- Transparent history of incidents and outages

The following sections review the mutually reinforcing advantages brought by cloud native patterns that diverge from traditional corporate IT infrastructure. This white paper concludes with recommendations for getting started with a transformation to a cloud native architecture.

Zero Trust Network Architecture

Traditional network and security center around trusted local networks that are ostensibly protected by perimeter defense, limiting inbound ports and inspecting inbound and outbound traffic. There is no assurance that the reported IP address in an IPv4 packet in fact came from that address, but it often completely obscures the actual originating IP. In other words, "You have no idea where that packet's been." It is still common to attempt a secure architecture that primarily allows and disallows traffic based on the IP address primarily at the perimeter. This made sense when IT was less mature, and securing and inspecting every connection to file servers, sensitive databases and systems was uncommon and largely cost-prohibitive. The model was to build an intranet with all the resources needed locally and safety behind a firewall was assumed. Even with the addition of defense in depth, end users' laptops ultimately become possible vectors for a pivot behind the firewall if the machine was compromised by a malicious web page or email.

This perimeter defense in traditional network security is often referred to by security professionals as "hard on the outside, soft on the inside." Even today there are zero day exploits that remain open for months. This means that anyone with a little knowledge can compromise a workstation and thus pivot to attack other local resources using that compromised workstation.

A zero trust network architecture turns this concept on its head and assumes nothing. Access to resources is based upon mutual cryptographic authentication rather than the hope that an IP address that matches an internal office subnet is in fact the origin of the traffic. Rather than assuming trust and dangerously transmitting in cleartext far too often, communication is authenticated, authorized and encrypted by default.

This approach not only facilitates security and flexibility but recognizes the increasingly important role remote workers play across industries. In a zero-trust environment it doesn't matter whether an employee is in an office or travelling, whether at a coffee shop, or at home. When the infrastructure supporting internal business processes assumes nothing and requires all connections to be authenticated and encrypted, all traffic is treated the same, untrusted until proven otherwise.

Laptop Management Patterns

While it is neither possible to migrate physical laptops nor elegant today to move Windows or MacOS into the cloud, it is possible to transition to cloud native management for end user laptops.

Cloud native patterns and legacy anti-patterns

ANTI-PATTERNS	PATTERNS
Anti-Malware/Blacklisting	Whitelisting
Manual/Routine Backup/File Synchronization	Cloud native storage
Manual revisions emailed as attachments	Real time multi-user editing with automated revision history
Helpdesk for routine requests	Self Service/SaaS administration
Manual patching or patching that requires human intervention	Automated patching with prompts to reboot
Laptop authentication tied to local auth/AD	Cloud native authentication
Routinely vulnerable software platform middleware like Flash, Java, and Acrobat Reader	Web-based clients using HTML5, or browser extensions when necessary

On any given day, according to Lastline Labs' analysis, much of the newly detected malware goes undetected by as many as half of the antivirus vendors. Rather than attempt a real time evaluation of every possible piece of software, file addition or change against an ever-growing list of threat signatures, cloud native architecture denies by default. While whitelisting has come up as a possible suggestion, not until mobile phones and chromebooks was it successful.

Chromebooks

Chromebooks are unfortunately the only cloud native personal computer in widespread use today. Fortunately, they adopt all of the cloud native patterns and result in a secure, low cost laptop with long battery life. The further along in a cloud native journey the easier it will be to adopt Chromebooks for end users. The more widespread the use of cloud native personal computers is in the organization, the more resilient the organization will be to ransomware and other malicious attacks.

Loosely Coupled

Whether or not a service has a Public API, it's important to strive for a loose coupling of services. While in the short term a service may seem easy or efficient, in the face of the speed of change we're seeing today, all organizations are best served by planning for eventual service transitions.

Loose coupling is an understood advantage of microservice architecture. Likewise, there is an analogous advantage to having a loosely coupled stack of cloud native software. Loose coupling includes weighing the cost benefits of making year vs monthly commitments. Monthly commitments are recommended when possible as they allow for greater flexibility. But if the savings is significant and it's clear you won't have a superior alternative or bandwidth for another migration within the year, making a year commitment could be justified.

With the rate of innovation, displacement and disruption there is no way to confidently choose a technology that is not at risk of becoming outdated by better, cheaper, faster, or paradigm-shifting capabilities within twelve months. Given this reality, making two- or three-year commitments even with the promise of a significant discount should generally be off the table. While it may be somewhat challenging to know ahead of time, it's worth attempting to size the effort required to onboard/offboard a given service.

As always, use caution when reviewing contracts for hidden exit clauses that require additional and/or written notice of cancellation. The advantages of loose coupling not only allow for a rapidly evolving internal stack but also facilitate faster and simpler acquisitions and mergers.

Public API

There is no more powerful architectural enablement of loose coupling than a public API. Why is something as technically specific as having a Public API such a useful differentiator when evaluating solutions? First, it's a likely indicator of cloud nativity as the vast majority of cloud native SaaS options have a Public API. It's also an indicator (though not a guarantee) of attention and rigor of security, because having a publicly accessible API requires good security practice and monitoring to avoid exploit and compromise. With a stack of services with increasing API functionality it becomes more possible to automate internal processes, quickly wire up integrations between other providers or even potentially facilitate a rapid pivot to a more robust or competitive service when it's warranted.

Single Sign-On as Default

SSO integration has matured enough to bring into question the use of a separate dedicated tool for SSO. Organizations that are currently locked into on-premise Active Directory as the primary authentication mechanism or other similar legacy and on-premise technology may need a thirdparty SSO integration to bridge or fill gaps during a transition phase. Both OAuth and SAML are increasingly standard components of SaaS solutions and also a good indicator of a cloud native solution.

Self-Service

While security or the particulars of a given process often require a ticketing system with a one-for-one ticket-to-human interaction ratio, a growing pattern within cloud native systems is a decidedly self-service orientation. This orientation flows naturally from relatively small teams who have built tools that otherwise scale well until a process requires human interaction.

Even today in large enterprise organizations who've outsourced their helpdesk, you can find a 24-hour turnaround for tasks as simple as adding a distribution group or a shared folder. Moving to a self-service orientation requires those familiar with a traditional IT process to learn to trust both end users and cloud native solutions that increasingly remove insecure configuration options. While high security or otherwise highly sensitive tasks may not lend themselves to self-service orientation, often the efficiency gains are matched by end user satisfaction because end users are empowered to move as fast as they can. While self-service won't eliminate the need for a helpdesk or SaaS administration, employees will be happier with the increased velocity and empowerment self-service brings.

Collaboration

Legacy systems had to assume not everyone could be connected to the internet. Even where online editing was possible, it required checking out and locking access to a single user to avoid the eventual merge conflicts.

Cloud native systems assume everyone is online. Real-time collaboration allows for an order of magnitude improvement in speed and efficiency in collaboration. Instead of taking hours, days or weeks to collect feedback from multiple users, with cloud native it is as simple as publishing a deadline and sharing access. Making comments, suggestions or edits in real time optimally gathers the best thinking from multiple contributors in a fraction of the time and effort.

How to Get Started

Avoid hybrid cloud options

A common anti-pattern for organizations considering a move to the cloud is to adopt half measures and plan for long-term retention of some resources on the local network or data center. But this is most likely a mistake given the threat and the cost to support and defend those local resources.

Consider that defending local resources to the same level as cloud native services requires a Security Operations Center complete with a SIEM and staff for that SOC with security professionals providing 24/7 coverage. For most companies that's cost prohibitive to do themselves. Economies of scale allow SaaS providers to ensure that the cloud native equivalent of that file server, phone system and videoconferencing server is protected.

Start with a single cloud service

A growing number of companies are already using one or many cloud native services. To join them, start with a single service. Most cloud native providers offer a free tier or 30-day trial often with minutes or hours for initial configuration rather than the days or weeks required for traditional infrastructure.

Build a map of dependencies

For example, to move off of Active Directory dependent on an Exchange mail server either on-premise or in a colo facility, migration of the email service comes first. To break site-to-site VPN links between offices, the system may not function without that flat and open network infrastructure.

Identify Your Biggest Obstacle

When planning a migration to cloud native infrastructure, identify the system that presents the largest challenge. Consider legacy applications, Active Directory, colocation facilities, custom or internally developed tools. Which have systems that have deficient or completely absent documentation?

Then identify the largest application or challenge, estimate how long it will take to overcome that challenge and create a roadmap centered around that bottleneck. Verify the capacity to migrate or replace the remaining services/applications either simultaneously or consecutively and adjust the roadmap. Remember that replacing or backing up old data is often simpler and faster than migrating old information into a new SaaS provider.

Conclusion

For those who have never considered a shift of infrastructure this significant, it may seem impossible. It's not. In fact from a technical standpoint, it's easier than it has ever been. While it's not surprising that vast majority of Silicon Valley startups follow cloud native patterns for their corporate IT infrastructure, that option is not reserved for startups. Don't try to fight the growing trend of shadow IT as individual employees or departments learn how simple it is to add a cloud native service and do so without the knowledge, approval or assistance from IT or the organization as a whole. Rather, engage the innovators and embrace a company-wide cloud native infrastructure which will bring increased security, stability and agility and reduce redundant and conflicting solutions. Your employees will thank you as they feel their potential become unlocked by the most modern and rapidly evolving software available.

Author's note:

Throughout my 20-year career in IT, including years securing and auditing critical infrastructure, I have been concerned about the state of security. My concern has grown during this time as I've witnessed the increasingly technical focus of the security industry trend toward pen testing and other forms of real world validation over paper evidence reveal the fundamental insecurity that is far more prevalent than most people know.

It became clear that any remedy for increasingly sophisticated and increasingly widespread attacks would be found through the kind of automation and infrastructure as code being demonstrated within the nascent DevOps movement.

My general concern about the state of security sharpened into focus when the company that employs a member of my family (who also works in IT) was compromised by a ransomware attack. When I learned that both consultants and law enforcement recommended paying the ransom, I began to think about how I could architect a corporate infrastructure resilient to a ransomware attack.

When I joined InsideTrack I was able to materialize the results of that exploration into a cohesive whole combining my experience in DevOps, specifically new cloud native patterns, and rearchitect the corporate IT infrastructure. Since then, multiple high profile targets from hospitals to banks and governments have endured ransomware attacks; even as I write this, the county next to mine is still recovering from a ransomware attack that hit late last year. If you take nothing else from this whitepaper I hope it prompts you to ask yourself, "How am I prepared for ransomware or similarly crippling attacks?"

Chris Borte, Director, Information Technology and DevOps, InsideTrack, Inc.

Chris Borte joined InsideTrack in 2015. His 20-year IT career spans a breadth of environments, from small startups and nonprofits to large civilian federal agencies and international enterprises. Chris started in traditional IT environments and then moved on to 10 years in high security focused work where he learned to differentiate between compliance and technically tested and validated security. He was amazed at the paradigm shift brought on by DevOps as an early adopter of DevOps patterns years before it was popular. Chris is grateful to be working with InsideTrack's talented engineering team, which has built an impressive microservice-based application that he hopes to migrate to Kubernetes in the near future. Chris is a Portland native who recently moved to Nashville, Tennessee with his wife and two young children.

About InsideTrack

Improving one student's experience in school and chance of success can have a lifelong impact on not just that individual, but on greater society. That ripple is why we do what we do. InsideTrack is passionate about student success. Since 2001, we have been dedicated to partnering with colleges and universities to provide adaptive coaching solutions that generate measurable results. These solutions combine professional coaching, technology and data analytics to increase student enrollment, completion rates, and career readiness.

Our adaptive student coaching methodology is based on the latest behavioral science research and knowledge gained from working with more than 1.5 million students and 1,600 programs. In combination with our uCoach® Platform, our approach generates valuable insights on the student experience and uses predictive modeling, behavioral analysis and multichannel communication to optimize student engagement. InsideTrack became a member of the nonprofit Strada Education Network in 2017, increasing our capacity to enhance student and institutional success. Join us and the leading institutions, foundations and others working to bring the transformative power of education to all individuals.

REFERENCES:

1. *Cloud Native Infrastructure: Patterns for Scalable Infrastructure and Applications in a Dynamic Environment*, by Justin Garrison and Kris Nova, O'Reilly, 2017, pp. 6.