
TREND MICRO | research
MISCONFIGURED
THE FUTURE IS
Cloud and DevOps migrations present risks as well as rewards to adopters, underscoring the need for security throughout the deployment pipeline.

The Future is Misconfigured

The future of organizations' infrastructures is in the cloud, utilizing a DevOps culture to take advantage of its full potential. Offering a world of new possibilities, the cloud provides organizations with greater flexibility, scalability, and cost savings that ultimately provide a competitive edge for their business. But cloud and DevOps migrations present some serious risks that, if not properly managed, can leave the organization vulnerable. Trend Micro Research has produced predictions for 2020, based on our experts' opinions and insights on current and emerging threats and technologies. And it is no surprise that cloud misconfigurations are front and center.

Vulnerabilities in container components will be top security concerns for DevOps teams

The container[1] space is fast paced. Releases are quick, architectures are continually integrated, and software versions are regularly pushed. Traditional security practices will not be able to keep up.

This highlights the importance of DevSecOps principles for DevOps teams, as containers overturn more conventions and assume more roles that are critical to organizations. Rapid development cycles may leave little room for security and vulnerability testing and an application may now require an organization to secure hundreds of containers, spread across multiple virtual machines in different cloud service platforms.

Needless to say, organizations will have their hands full with issues in different components of the container architecture, including vulnerabilities in runtimes (e.g. Docker®, CRI-O, Containerd, and runC[2]), orchestrators (e.g. Kubernetes®), and build environments (e.g. Jenkins®). Attackers will find ways to take advantage of any weak link to compromise the DevOps pipeline.

Vulnerabilities in widely used container images have a detrimental effect on the enterprise pipeline, if they are subsequently downloaded. Patching containers will be particularly tricky if organizations rely on a third party for the image fix, trusting that it is secure. Vulnerabilities in containerized applications will not only affect the container code or engine, but also the many other elements across the stack, which malicious actors can move in on for access and control.

Serverless platforms will introduce an attack surface for misconfiguration and vulnerable codes

More enterprises are embracing serverless platforms to integrate cloud applications and reduce costs. Gartner projects that more than 20% of global enterprises will have serverless computing technologies deployed by 2020.[3] Serverless platforms offer "function as a service," allowing developers to execute codes without the organization having to pay for all of the servers or containers.[4] However, going serverless does not mean immunity from security problems.

We expect outdated libraries, misconfigurations, and known and unknown vulnerabilities to be threat entry points to serverless applications. Attackers can take advantage of these to gather sensitive information or penetrate enterprise networks.[5]

Serverless platforms also include containers, serverless functions, and other dependencies, further underscoring the complexity of where a threat may originate from. Since serverless computing renders functions—especially those that are open source—as stateless, monitoring permissions and storing sensitive data will also be top concerns in 2020. Besides increasing network visibility, improving processes and documenting workflows will be essential to running serverless applications.

As it is in container-based applications, DevSecOps should also be at the forefront of the serverless deployment. Serverless environments will also benefit from the continuous integration and ease of use that DevSecOps aspires to.[6] Security tools that tackle serverless infrastructures, including open-source application dependencies and vulnerabilities, will be important in serverless adoption and deploying specific functions.

User misconfigurations and unsecure third-party involvement will compound risks in cloud platforms

Despite regularly updating systems and putting up appropriate measures, an organization can still be at risk if there are misconfigured applications and authentication issues in the deployment. Basic security controls that are not implemented properly will be a huge security threat to organizations' data.

We foresee more incidents of compromised networks due to cloud services' weak points. Misconfigurations in cloud storages that cause data leakage will still be a common security issue for organizations in 2020. Insufficient access restrictions, mismanaged permission controls, negligence in logging activities, and publicly exposed assets are only a few of the missteps companies will make as they set up their cloud networks. Mistakes and failures involving cloud services will expose a significant number of company records and even lead to incursion of fines and penalties. These risks can be curbed by improving the overall cloud security posture, this means properly configuring and deploying infrastructures and ensuring that best practices and industry standards are upheld.

As more companies and productions (e.g. manufacturing facilities)[7] move to the cloud, third-party service providers will be increasingly involved. However, there also lies the risk that these vendors may not be experienced with the cloud and equipped to protect the infrastructure. Attackers will be motivated to perform DDoS attacks against service providers via botnets to disrupt cloud services.

Cloud platforms will fall prey to code injection attacks via third-party libraries

More compromises in cloud platforms will happen in 2020 by way of code injection attacks, either directly to the code or through a third-party library. Malware injection can be done in an attempt to eavesdrop or take control of a user's files and information on the cloud. Common forms of such attacks in cloud services' web applications are cross-site scripting attacks and SQL injection attacks. Successful attacks allow hackers to remotely retrieve sensitive data and manipulate database content. On the other hand, attackers can go in a different route with third-party libraries that, when downloaded by users, execute injected malicious code.[8]

Meanwhile, we foresee more attackers following data to the cloud. Cloud breaches will be expected as software-, infrastructure-, and platform-as-a-service cloud computing models are being widely adopted. The more corporate data resides in the cloud, the more malicious actors get interested. Preventing cloud compromises will require due diligence from developers, careful consideration of providers and the platforms offered, and improvements in cloud security posture management.

Conclusion

Gone are the days of networks isolated behind a company firewall and a limited stack of enterprise applications. The bottom line is, as the world continues to shift to become more agile and flexible, the same needs to ring true for cybersecurity. Cloud computing requires greater visibility and control of all the moving parts in order to see and remediate vulnerabilities and misconfigurations hiding in the complexity that is the cloud. Otherwise, it can leave DevOps and cloud security teams with a trail of unmanaged risk across multi-cloud environments, creating devasting losses in revenue, reputation, and time. To avoid this, you will have to view security through many lenses to keep up with and anticipate cybercrime mainstays, game changers, and new players. While it sounds overwhelming, if done with the right tools, best practices, and informed decision making, you can achieve security with the speed and simplicity needed to keep up with the cloud.

1. Trend Micro. (n.d.). Trend Micro. "Container." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/definition/container.
2. Trend Micro. (28 February 2019). Trend Micro Security News. "CVE-2019-5736: RunC Container Escape Vulnerability Provides Root Access to the Target Machine." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/cve-2019-5736-runc-container-escape-vulnerability-provides-root-access-to-the-target-machine.
3. Gartner, Inc. (4 December 2018). Gartner. "Gartner Identifies the Top 10 Trends Impacting Infrastructure and Operations for 2019." Last accessed on 24 October 2019 at https://www.gartner.com/en/newsroom/press-releases/2018-12-04-gartner-identifies-the-top-10-trends-impacting-infras.
4. Scott Fulton III. (9 April 2019). ZDNet. "What serverless computing really means, and everything else you need to know." Last accessed on 24 October 2019 at https://www.zdnet.com/article/what-serverless-computing-really-means-and-everything-else-you-need-to-know/.
5. Guy Podjarny. (15 May 2018). The Register. "Hey cool, you went serverless. Now you just have to worry about all those stale functions." Last accessed on 10 October 2019 at https://www.theregister.co.uk/2018/05/15/stale_serverless_functions/.
6. Trend Micro. (13 April 2018). Trend Micro Security News. "Serverless Applications: What They Mean in DevOps." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/virtualization-and-cloud/serverless-applications-what-they-mean-in-devops.
7. Willem Sundblad. (18 July 2019). Forbes. "Smart Manufacturing: Creating a Hybrid Cloud-Edge Strategy." Last accessed on 10 October 2019 at https://www.forbes.com/sites/willemsundbladeurope/2019/07/18/smart-manufacturing-creating-a-hybrid-cloud-edge-strategy/#77fc5816af5a.
8. Trend Micro. (29 November 2018). Trend Micro Security News. "Hacker Infects Node.js Package to Steal from Bitcoin Wallets." Last accessed on 10 October 2019 at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hacker-infects-node-js-package-to-stealfrom-bitcoin-wallets.

For Raimund Genes (1963-2017)

TREND MICRO™ | research

Trend Micro Security Predictions for 2020

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information. Our innovative solutions provide our customers with layered security for data centers, cloud workloads, networks, and endpoints.

At the heart of our leadership, Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights with the public, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on targeted attacks, artificial intelligence, Internet of Things (IoT), cybercriminals, and more. We continually work to anticipate the next wave of threats and deliver thought-provoking research that can shape strategic industry direction.

www.trendmicro.com

For details about what personal information we collect and why, please see our Privacy Notice on our website at:
https://www.trendmicro.com/privacy
[Asset01_The_Future_Is_Misconfigured_200304US]