The major impact of runtime security controls on risk and efficiency

CRISTIAN IORDACHE PRODUCT MARKETING MANAGER, CISSP

Bitdefender

WWW.BITDEFENDER.COM

Agenda

- What runtime risks are you missing?
- Preserving agility and efficiency
- Bitdefender and analyst insights, and best practices

Cloud-native application and workload security

Misconception: Pre-runtime processes such as image validation and vulnerability scanning, immutable infrastructures, are enough to protect against modern cyberthreats

“Organizations that adopt Gartner’s continuous and adaptive risk and trust assessment (CARTA) strategic framework and a zero trust security architecture acknowledge that CWPP strategies cannot rely solely on preventive controls. Thus, ***server workload behavioral monitoring (endpoint detection and response [EDR] for servers) is becoming a critical requirement of CWPPs.”***

Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, Tom Croll, July 12, 2021

Bitdefender®

Runtime threats and vulnerabilities

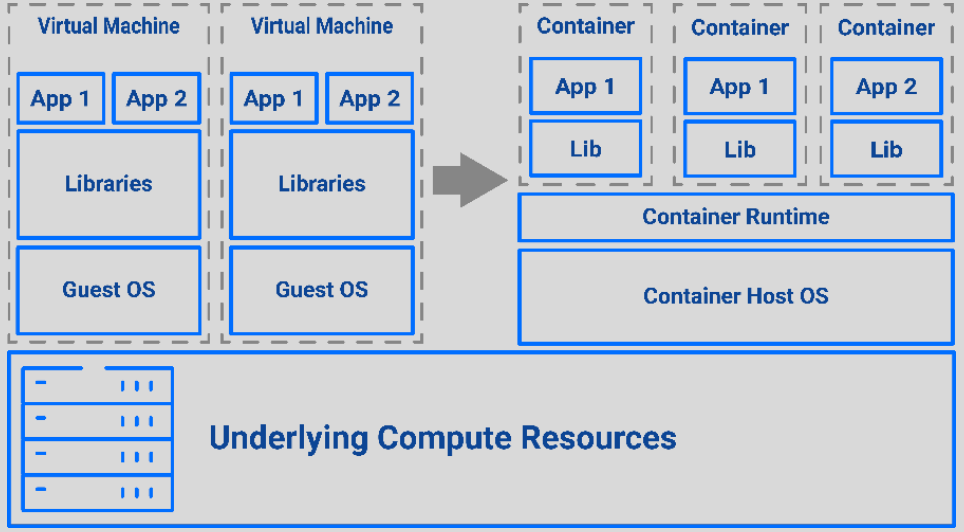
0-day Linux Kernel and application Exploits

e.g: Docker Escape: CVE-2019-5736
https://www.cvedetails.com/cve/CVE-2017-18641/

2020 - 126 kernel vulnerabilities
- 4 Code Execution CVEs
- 3 Privilege Escalation CVEs

2021 - 101 kernel vulnerabilities
- 10 Code Execution CVEs
- 1 Privilege Escalation CVE

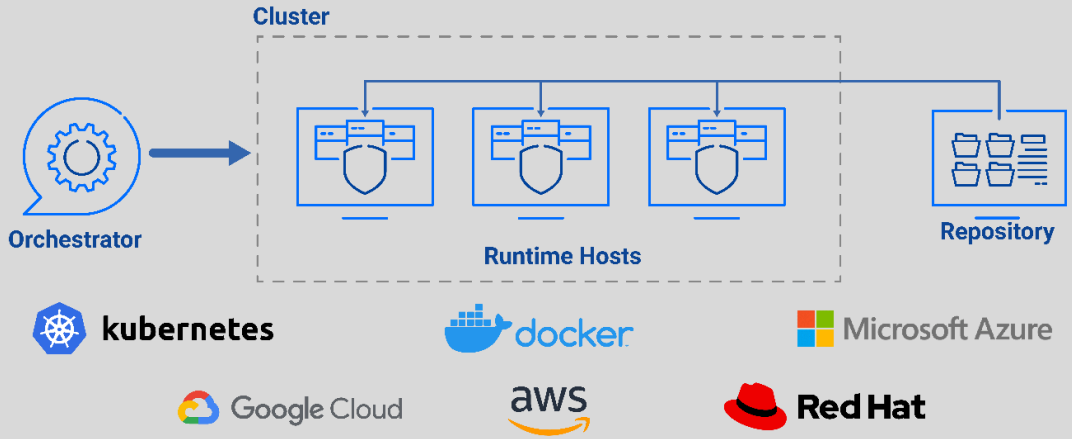
Source: https://www.cvedetails.com/product/47/Linux-Linux-Kernel.html?vendor_id=33



Bitdefender

Runtime threats and vulnerabilities

- Insider threat
- Compromised credentials
- Misconfigurations
- Overreliance on container image repositories (such as Docker Hub)
- Insecure coding practices: sharing snippets



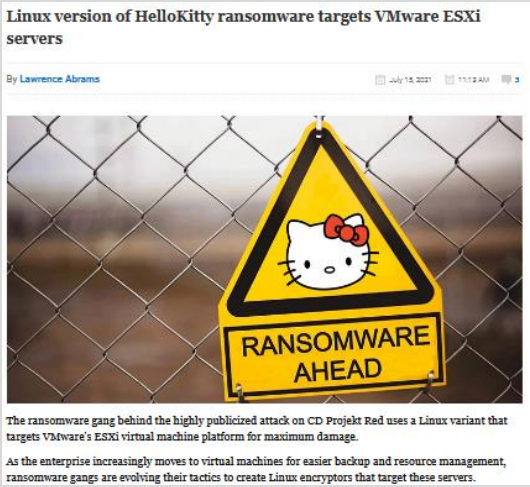
Linux increasingly targeted by APT groups and ransomware

We’re seeing more ransomware families that target Linux binaries and that include code aimed at encrypting virtual ESXi hard drives.

Examples of attackers that have migrated towards linux as well- multiplatform attacks

- **Trickbot** migrated to linux in 2020 - APT Wizard Spider
- **IPStorm** a migrated to Linux in 2020 (APT)
- **Lazarus** – began developing malware on linux (APT)
- **Revil**

- **Revil**
- **Babuk**
- **HelloKitty**
- **Defray**
- **DarkSide**



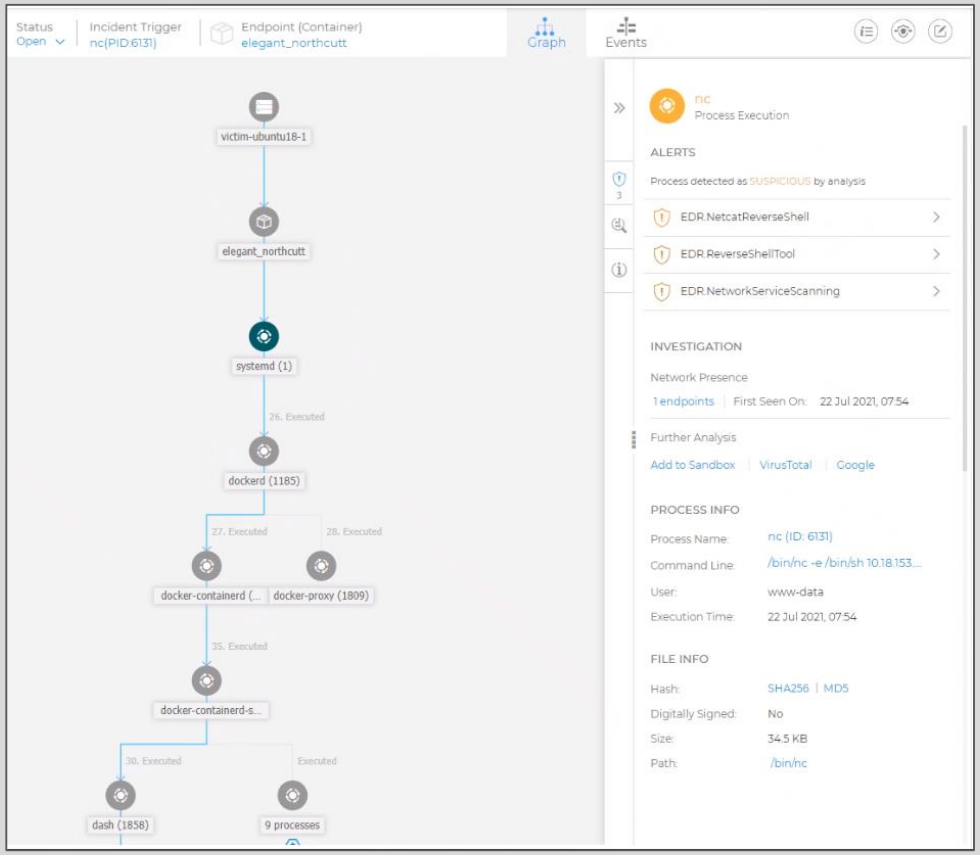
Bitdefender®

Container and Linux runtime security and visibility is key to reduce risks

Cloud Workload Protection Platforms offer security designed for dynamic workloads, servers, Linux

Some key capabilities:

- Stop 0-day Linux kernel and application exploits
- Prevent ransomware / malware
- Gain visibility into runtime security events, attack chains, understand attack impact
- Detect anomalous behavior at runtime
- Investigate potential threats
- Respond quickly and efficiently, become resilient



Bitdefender®

Major impact of container runtime & workload security on efficiency and agility

The choice of Container runtime and cloud workload security can massively impact risk but also operations, agility, and cloud ROIs

Key pitfalls we're seeing:

- **Lack of container context** and controls built for Linux, use of EPP/Next-gen AV
- **Lack of security controls built for container and Linux** server threats
- Difficult to support multiple or new Linux distributions
- **Point solutions** add complexity, lack of consistent threat visibility and control
- High security agent **resource consumption** impacting cloud ROIs
- **Lack of automation** or support for virtualization/cloud platforms, Docker, Kubernetes

Analyst cloud workload security insights and best practices

CWPP, not EPP

"Enterprises using endpoint protection platform (EPP) offerings designed to protect end-user devices for server workload protection are putting their data and applications at risk.."

New Container capabilities

The shift to cloud-native application development using container-based application architectures, microservices-based applications and adoption of serverless PaaS **requires new CWPP capabilities both for development and at runtime.**

IaaS and PaaS

"There is no guarantee that an enterprise will be able to place agents in the Linux host […]This is increasingly the case with locked-down minimal kernels [...]. **The answer is to provide an architectural option to run the CWPP offering as a privileged container[…]"**

EDR critical req.

- ***"…server workload behavioral monitoring (endpoint detection and response [EDR] for servers) is becoming a critical requirement of CWPPs."***

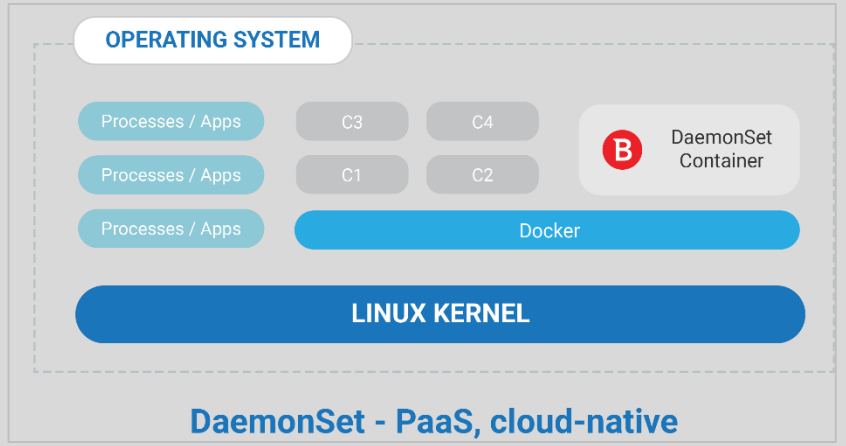
Bitdefender

Source: Gartner, Market Guide for Cloud Workload Protection Platforms, Neil MacDonald, Tom Croll, July 12, 2021

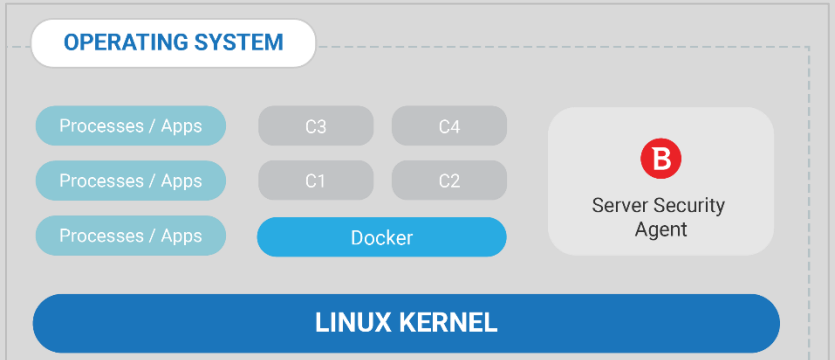
Bitdefender container and Linux security

Address container and cloud risks and efficiency challenges

- **Anti-Exploit and EDR built for containers** and Linux TTPs, plus tunable ML prevention, risk analytics
  100% detection of attack techniques for Linux in 2021 MITRE evaluations
- **Linux Kernel-Independent,** avoid security compatibility issues
- **Consolidated threat visibility and protection,** across cloud infrastructures and platforms (hybrid and multi-cloud workloads, containers in IaaS and PaaS, Linux, Win, physical endpoints)
  Bitdefender GravityZone – leader in Forrester Wave for CWS, 2019
- **High-performance cloud security agent**
  Best Performance in independent LoginVSI benchmarking
- **Automate** security agent deployment and scaling
- **Supports:** Amazon ECS, Amazon EKS, Google GKE, Docker, Podman, Kubernetes, Azure AKS



DaemonSet - PaaS, cloud-native



Server Agent - IaaS

Bitdefender

Takeaways and more information

- **Container runtime** and cloud workload visibility, protection, EDR are critical
- **Threats/vulnerabilities:** 0-day exploits, misconfigurations, insecure coding, etc
- **EPP solutions are not fit** for cloud security, point solutions add complexity
- **Main impact on risk and efficiency**: lack of Linux, and container-specific controls, Linux compatibility issues, fragmented visibility
- Bitdefender extended GravityZone CWPP with container and Linux security

Develop your cloud security strategy:

- **Talk to our cloud security specialists** @ the Bitdefender booth
- **Download the Gartner Market Guide** for Cloud Workload Protection Platforms complimentary copy from Bitdefender website
- **Download A Practical Guide to Container Security** and **Datasheet** from the Bitdefender Booth

Bitdefender®


Bitdefender
WWW.BITDEFENDER.COM

The major impact of runtime security controls on risk and efficiency