Cyber Exposure: Essential Visibility into the Modern Attack Surface

Liz Leon
Security Engineer - Tenable
Verizon’s 2018 Data Breach Investigations Report

53,308 security incidents, 2,216 data breaches, 65 countries, 67 contributors.

Source: 2018 Verizon DBIR
Threat Actors and Their Motives
Economic Impact

Global ransomware damage costs are predicted to exceed $8 billion in 2018, according to Cybersecurity Ventures.

Source: 2018 Outlook report Goldman Sachs investment division
What is attacked?

76% of external attacks are carried out by exploiting software and web application vulnerabilities, according to Forrester.

42% say it is difficult to prioritize which vulnerabilities are most important, according to Forrester.

99.9% exploited software vulnerabilities that had been compromised more than a year after the associated CVE was published, according to the Verizon 2015 Data Breach Investigations Report.
There is no such thing as being secure, everyone is just operating at an acceptable level of risk.
It’s Not All About Technology
Clicking Willy-nilly ...
The attack surface is **expanding**

- Industrial IoT
- ICS/SCADA
- Enterprise IoT
- Cloud
- Container
- Web app
- Virtual machine
- Mobile
- Laptop
- Server
- Desktop
- Network infrastructure
Application containers are exploding in adoption...

Docker Adoption

500,000+
Dockerized apps in Docker Hub

24 Billion+
Docker Container Downloads

DOCKER ADOPTION IS UP 40% IN ONE YEAR

Percent of Datadog Users

Month (segmentation based on end-of-month snapshot)
...and are creating a major Cyber Exposure gap

Organizations with containers in production

- 18% Perform Image Scanning

Risk Assessment Index
Organization’s ability to assess cybersecurity risks

- Containerization Platforms: Score: 52% Grade: F
- DevOps Environments: Score: 57% Grade: F

Average number of vulnerabilities in Docker Hub

- Official Images: 15.9
- Community Images: 40.5

Sources:
1) Anchore, “Snapshot of the Container Ecosystem,” 2017
3) Tenable, “Sourcing Container Images from Docker Hosts,” 2017
Cyber Exposure Lifecycle: Integrations are key to success

Discover
- CMDB, Public Cloud Platform, Network Access Control, Network Monitoring

Assess
- Credential and Privileged Access Management, Mobile Device Management (MDM), IP Address Management

Measure
- Governance, Risk and Compliance (GRC)
- Service Desk / Ticketing / Workflow, Patch Management, Network Access Control

Fix
- SIEM, Security Analytics, Endpoint Security

Analyze
- IT, IoT

OT, Cloud
From vulnerability management to strategic guidance

Live discovery of every asset
Continuous exposure visibility
Risk-based scoring & prioritization
Communication of cybersecurity risk
Strategic decision support
Four Key Questions

Where are we exposed?
Where should we prioritize based on risk?
How are we reducing exposure over time?
How do we compare to our peers?
Fundamentals

✓ Vulnerability Management working group
✓ Prioritize (threat data, attack path)
✓ Active scanning alone is no longer adequate for the modern attack surface
✓ A written, measurable patch policy
Fundamentals

✓ Measure and report on non-compliance
✓ Engage system/business owner
✓ Apply compensating controls
✓ Automate as much as possible
Tenable at a Glance

- Founded in 2002
- Exploded with the widespread adoption of Nessus and later, SecurityCenter
- Released Tenable.io in 2017 to introduce the first cyber exposure platform and evolve vulnerability management
- Relentless innovator: “Tenable has [massive] brand equity with Nessus, yet [is] one of the most forward-thinking companies in VM.” – Forrester, 2017

![Tenable Partnerships]

- 23,000+ Customers
- 1.6M Global Users
- 1200+ Employees
- 50% Fortune 500
- 100% Top 10 US Tech Companies
- 80% Top 10 US Financial Institutions