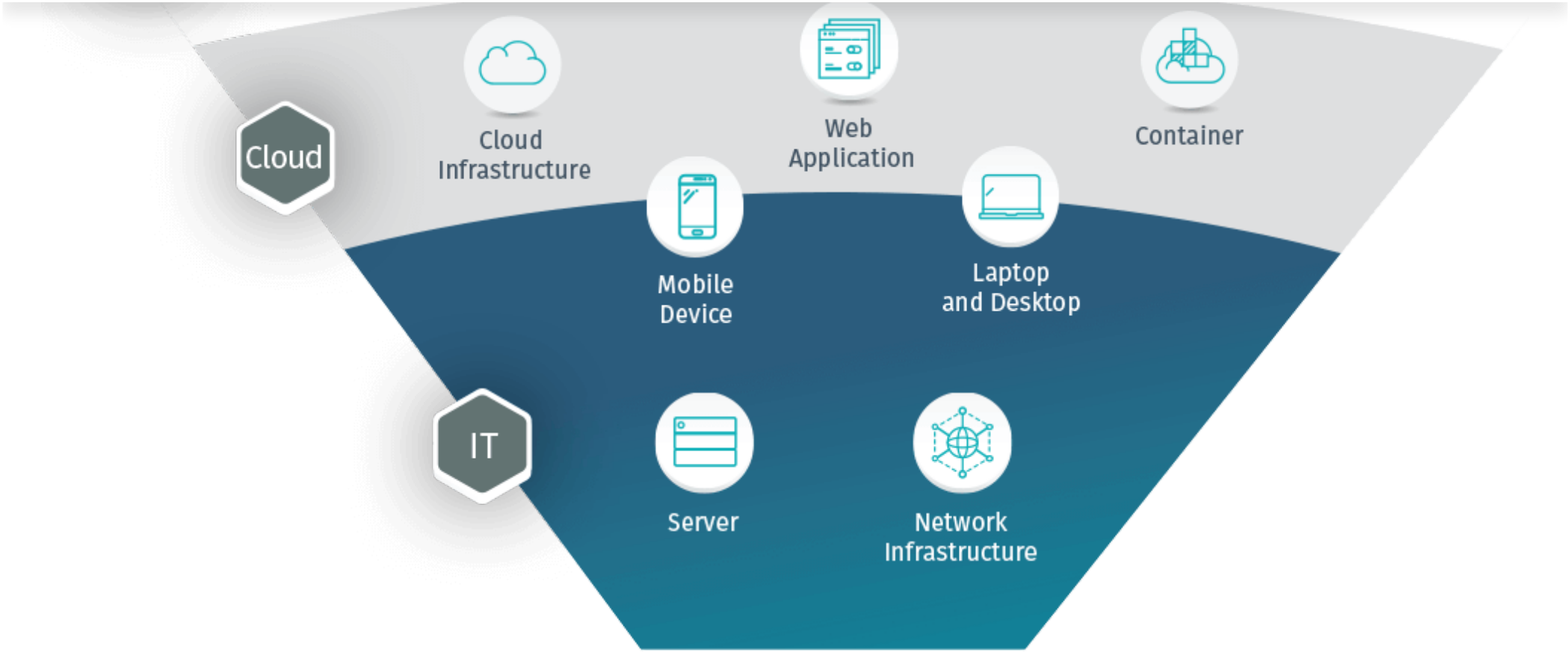
THE MODERN ATTACK SURFACE

Organizations of all sizes have embraced digital transformation to create new business models and ecosystems, deliver new products and services and operate more efficiently in the digital economy. New digital compute platforms and development shifts such as cloud, mobile, SaaS and DevOps have made it possible to move from concept to capability on a daily basis. Physical devices and systems of all types - from corporate conference systems to power grids - are now network connected and programmable, creating even more opportunities for digital transformation.

Some say these digital technologies are the future. But the truth is, the future is here and now. By 2019, there will be over 9 billion IoT devices deployed in the enterprise and over 90% of organizations have applications running in the cloud today.



This elastic attack surface has created a massive gap in an organization's ability to truly understand its Cyber Exposure at any given time. We call this the Cyber Exposure gap.

of opportunities, this is your new cyber attack surface to defend.

And it's exploding.

THE CYBER EXPOSURE GAP

The tools and approaches organizations are using to understand cyber risk don't even work in the old world of client/server, on-premises data centers and a linear software development lifecycle where there is less complexity and more control over security. An asset is no longer just a laptop or server. It's now a complex mix of digital compute platforms and assets which represent your modern attack surface, where the assets themselves and their associated vulnerabilities are constantly expanding, contracting and evolving - like a living organism.

tenable

WAYS

Throw 100s of security tools at the problem to protect from the 'threat of the week', creating siloed visibility, management overhead and reactive firefighting.

Rely on a CMDB to get visibility into asset configuration, but 85 percent of these projects fail in part due to stale data and they weren't built to discover and map today's modern assets.

Take a 'scan the network' approach to identify vulnerabilities. While this is foundational to understanding your cyber exposure gap, the old "one size fits all" techniques and tools haven't adapted for the modern attack surface.

No one has been able to provide the visibility and focus

WELCOME TO THE MODERN ERA OF CYBER EXPOSURE

Cyber Exposure is an emerging discipline for managing and measuring cybersecurity risk in the digital era. Cyber Exposure transforms security from static and siloed visibility into cyber risk to dynamic and holistic visibility across the modern attack surface. Cyber Exposure translates raw vulnerability data into business insights to help security teams prioritize and focus remediation based on business risk. Cyber Exposure provides executives and boards of directors with a way to objectively measure cyber risk to help guide strategic decision making. Just as other functions have a system of record - including ITSM for IT and CRM for Sales - Cyber Exposure solutions will provide Security with a system of record to help them effectively manage and measure cyber risk.

Cyber Exposure builds on the roots of Vulnerability Management, designed for traditional assets such as IT endpoints and on-premises infrastructure, moving from identifying bugs and misconfigurations and expanding to the following:

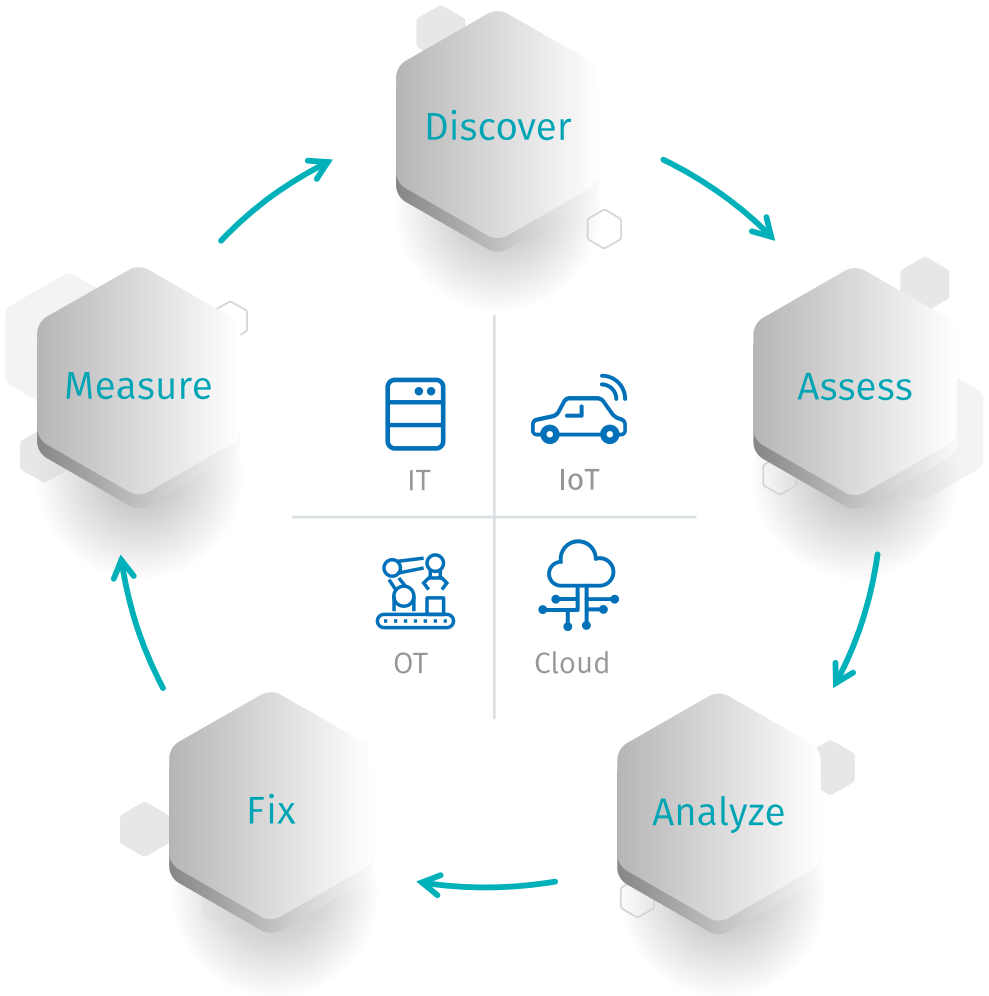
Live discovery of any digital asset across any computing environment

Continuous visibility into where an asset is secure, or exposed, and to what extent

Prioritization of remediation based on business risk

Benchmarking of cyber exposure compared to industry peers and best in class organizations

Measurement of Cyber Exposure as a key risk metric for strategic decision support



Understand the cyber exposure of all assets, including vulnerabilities, misconfigurations and other security health indicators

Analyze

Understand exposures in context, to prioritize remediation based on asset criticality, threat context and vulnerability severity

Fix

Prioritize which exposures to fix first, if at all, and apply the appropriate remediation technique

Measure

Measure and benchmark cyber exposure to make better business and technology decisions

Every organization, no matter how large or small,

tenable

2 *prioritize based on risk?*

3 *Are we reducing our exposure over time?*

4 *How do we compare to our peers?*

Learn more about Tenable.io Lumin, the new Tenable solution that for the first time empowers CISOs to confidently visualize, analyze and measure cyber risk. With the industry's first Cyber Exposure command center, Tenable is arming CISOs to quantify and benchmark their Cyber Exposure.

Learn More

tenable

... well, that's just untenable.

Join the Movement.

Tenable is built on innovation. We started with Nessus, creating the world's most widely deployed vulnerability assessment solution. Powerful yet flexible to adapt to the unique requirements of today's modern assets. Now with Tenable.io, we've delivered the world's first Cyber Exposure platform to provide visibility into any asset on any computing platform. And we're just getting started...

Explore our Products | Read the Blog Post

tenable

Overview

TENABLE.SC

Overview

LUMIN

Overview

PCI ASV

INDUSTRIAL SECURITY

Overview

Finance
Healthcare
Retail
State / Local / Education
IT / OT
US Federal

CUSTOMER RESOURCES

Support Portal
Education
Professional Services
Tenable Community
Customer Ambassador Program
Documentation
System Status
Security Advisories
GDPR Alignment

INVESTOR RELATIONS

Corporate Profile
Stock Quote/Chart
News Releases
Investor Events
Presentations
SEC Filings
Annual Reports

CONNECTIONS

Blog
Contact Us
Newsletter Signup
Resource Library
Webinars
Research

tenable

繁體中文
日本語