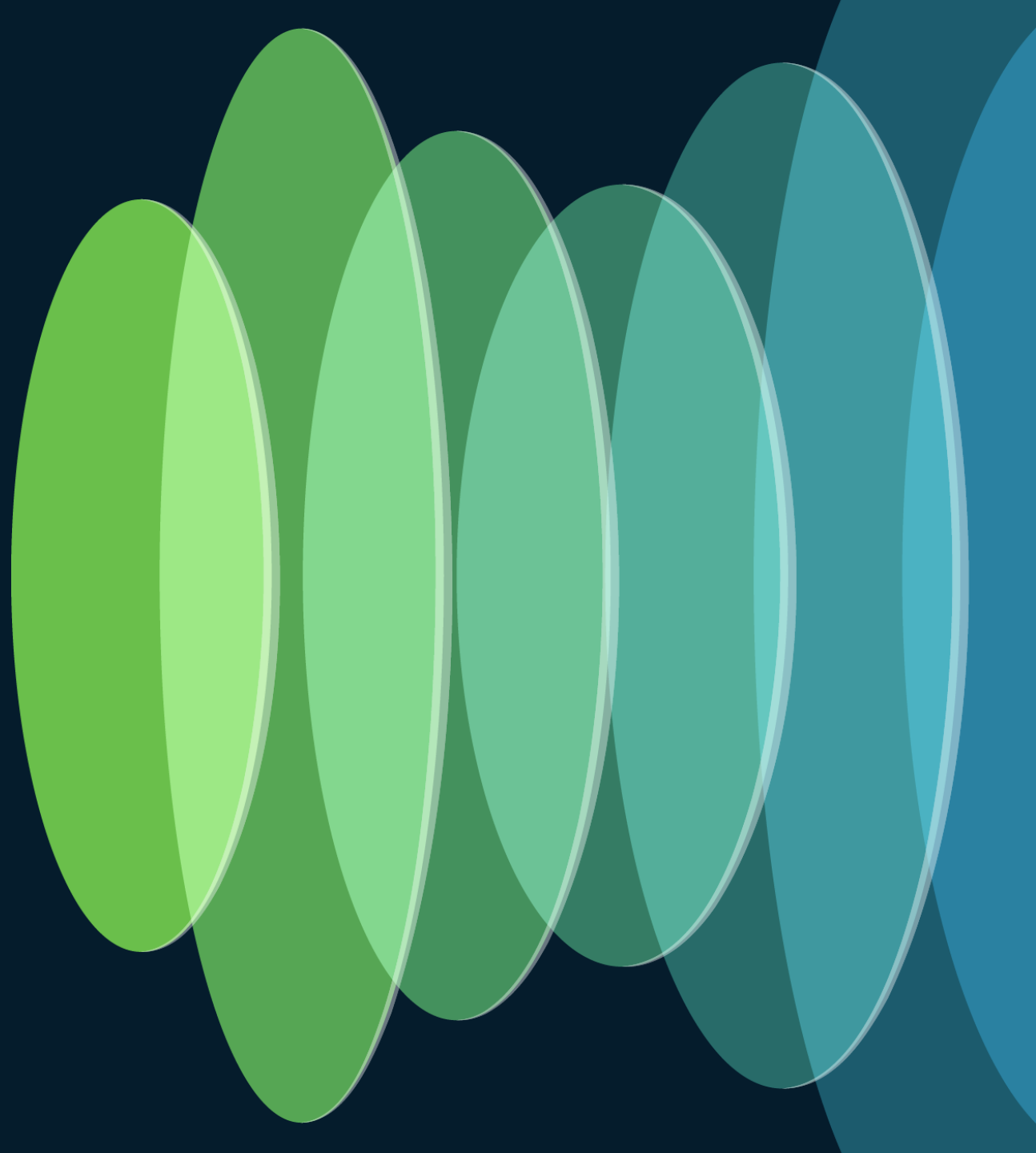


CISCO *Live!*
IT Leadership Program





Latest Cyber Challenges with Practical Advice for IT Leaders

Matt Carling, National Cybersecurity Advisor – ANZ
ITLGEN-1015

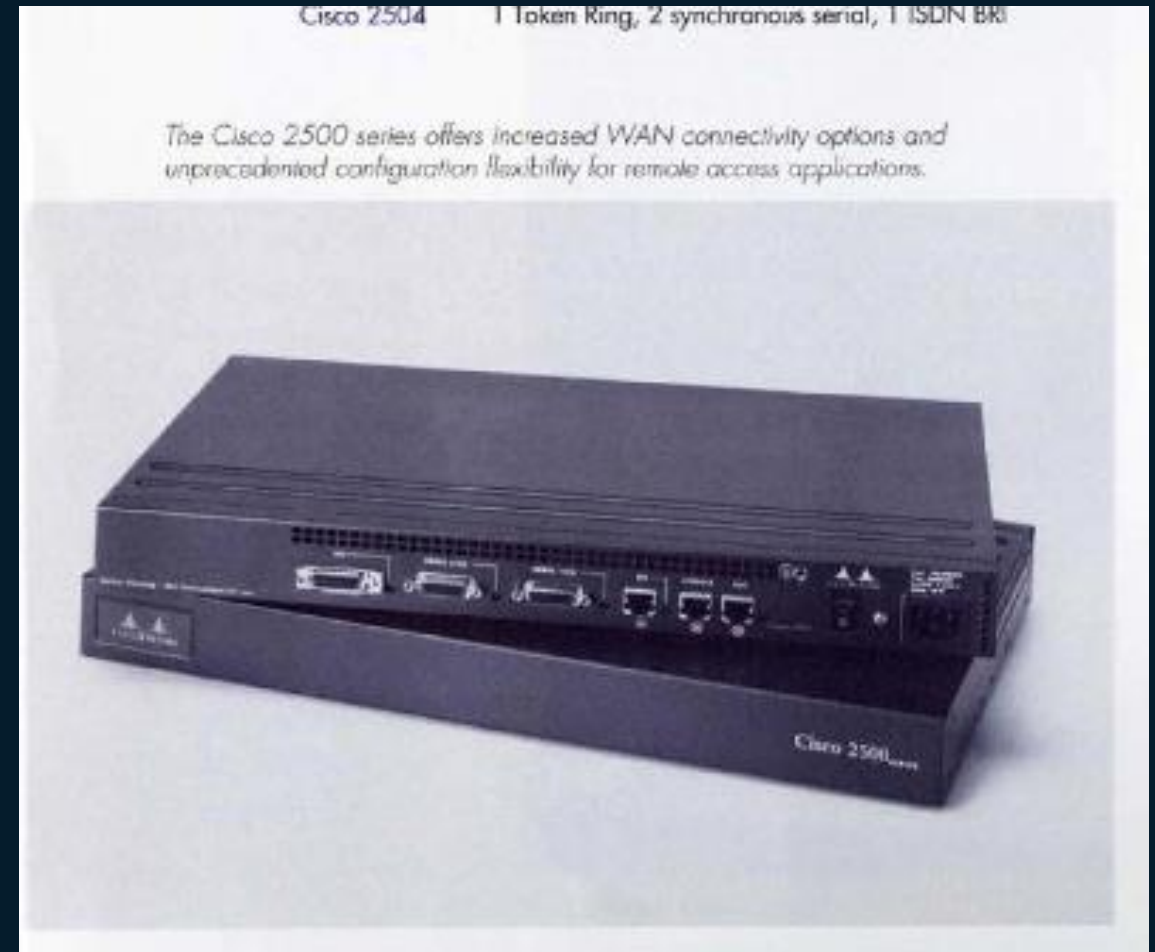
Agenda

- Technical debt
- Transforming workspaces
- Tightened regulations
- Technological advancements
- Tempo

Technical debt

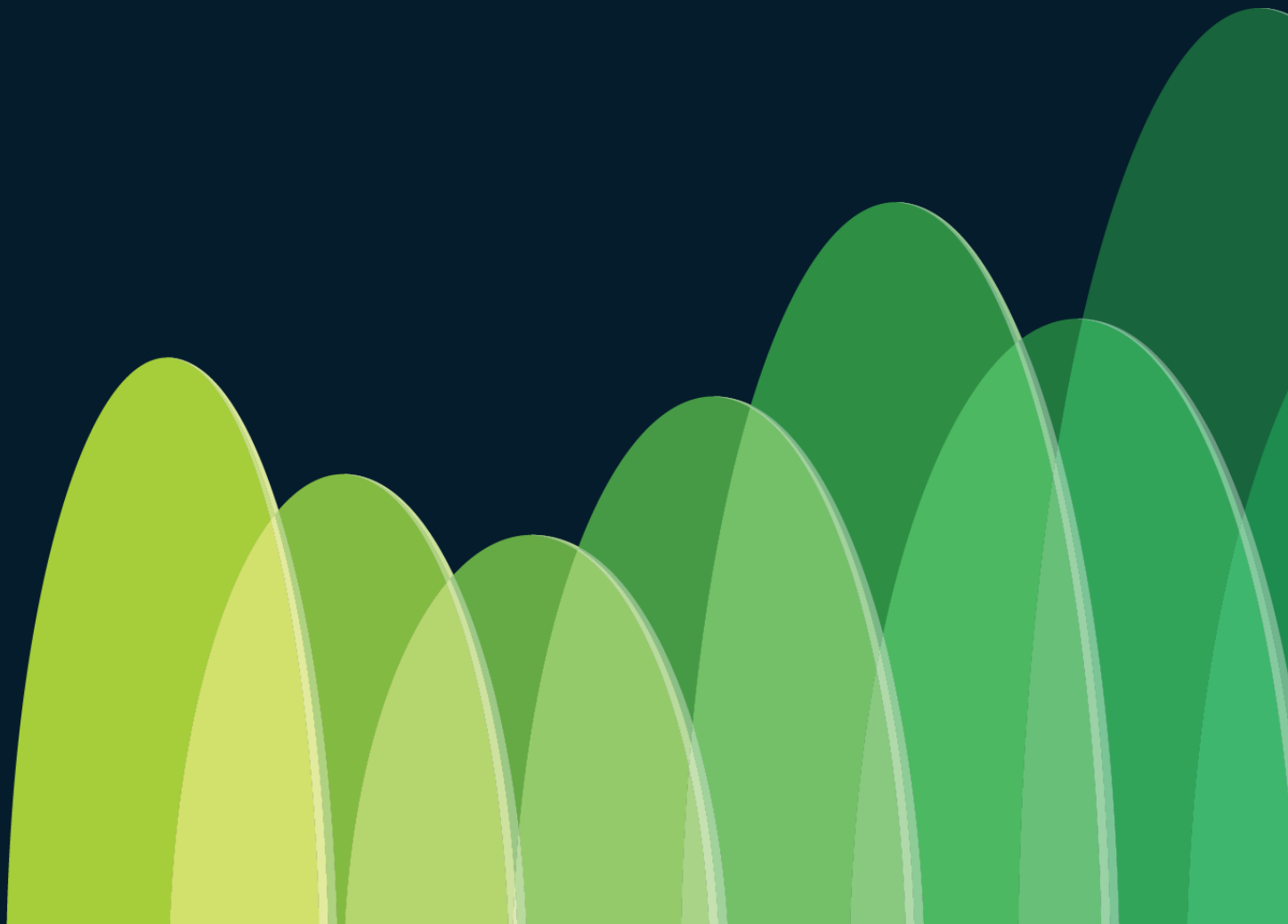
Technical debt and legacy systems

- From software development...accumulated debt from deliberate and unintentional choices
- Past End of Life, debt also includes lack of security fixes
- Opportunities...
 - Reduction – SDN / controller architecture, visibility platforms
 - Acceptance – segmentation, hardening, MFA, monitoring, attack surface reduction



Source : Computer History Museum Centre for Cisco Heritage

Transforming workspaces



Transforming workspaces

- For many organisations, hybrid work is here to stay
 - only the ratio is up discussion
- Who is connecting? To what? How? What is the perimeter?
 - Verify users AND devices
 - Secure access (to resources)
 - Defend hybrid workers anytime from anywhere

IT Landscape – Hybrid Work Evolution

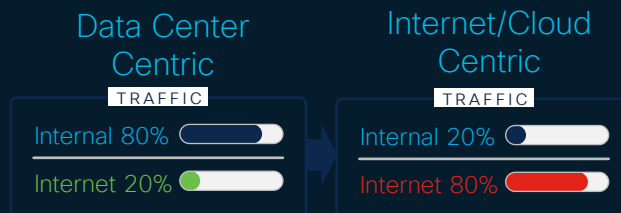
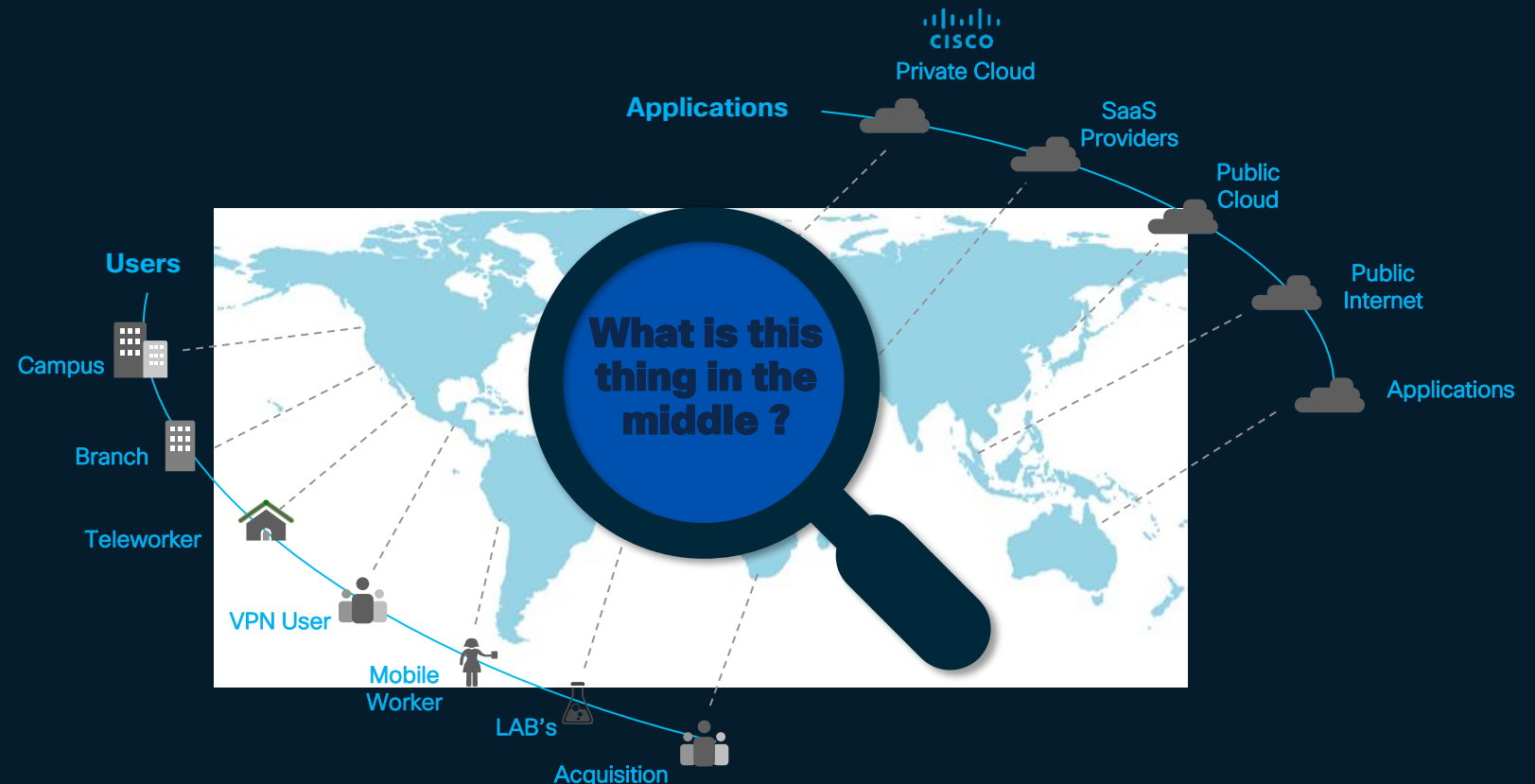
Challenge

Enabling users ANYWHERE to talk to applications EVERYWHERE!

WE ARE LIVING IN A HYBRID WORLD

75% work from home
over 50% of the time

Business applications
move to **Cloud & SaaS**



What is Cisco Secure Access (SSE)

Connecting users & things anywhere to applications everywhere

Better for users
Consistent user experience
wherever you are



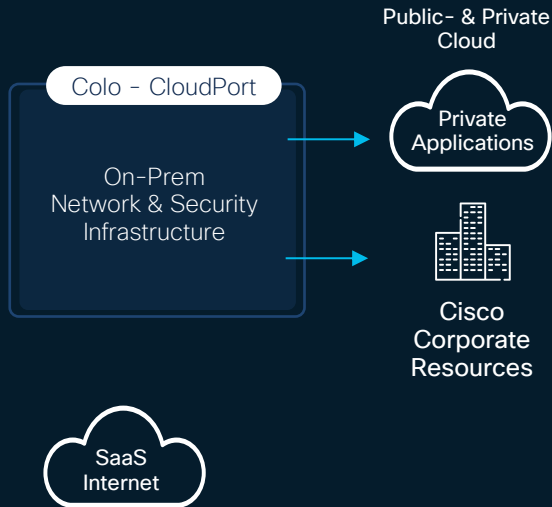
Traffic Acquisition
Consistent everywhere

More Secure for everyone
Unified security controls & telemetry



Simpler for IT
From Do-it-yourself to as-a-service

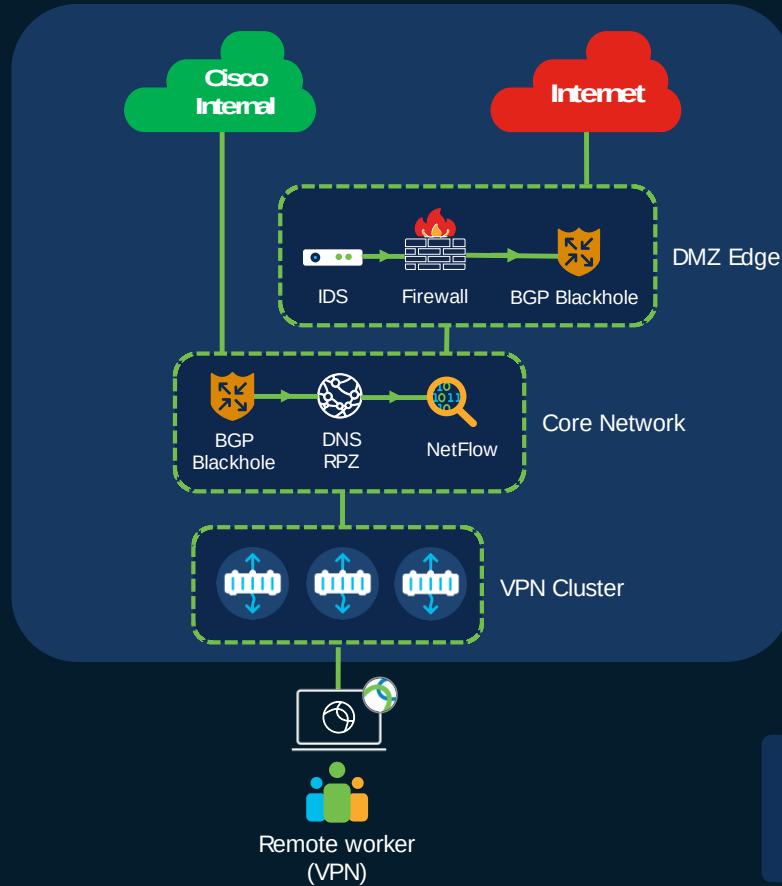
ROUTER IN THE SKY
Consistent traffic flows
and security



Security Evolution

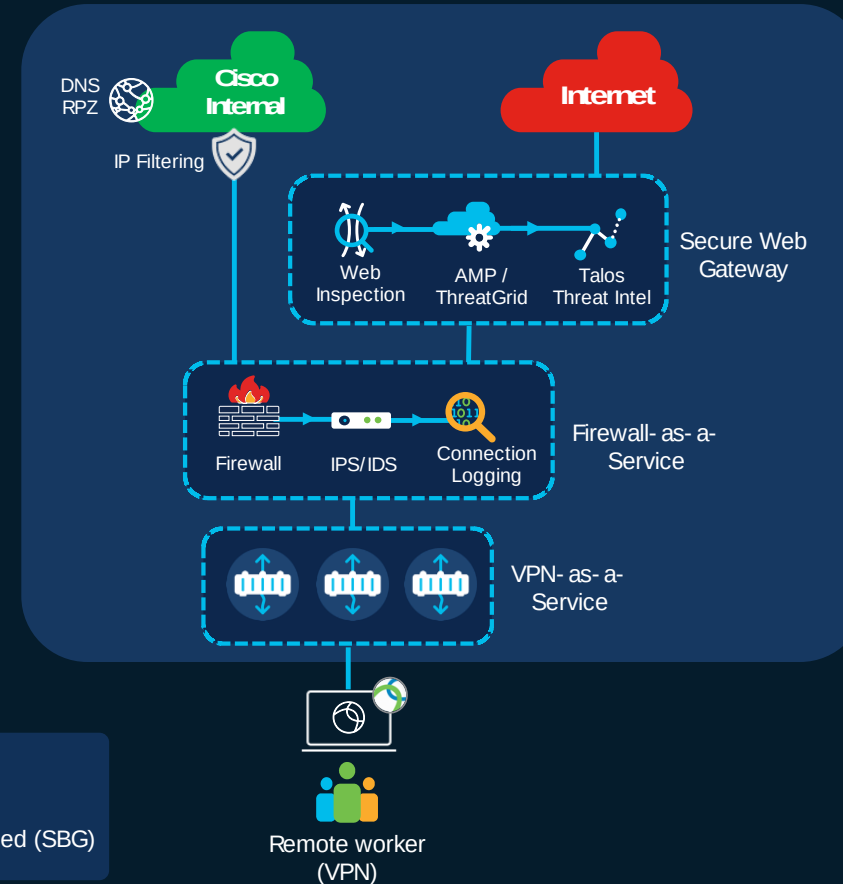
Cisco IT - CloudPort

Today

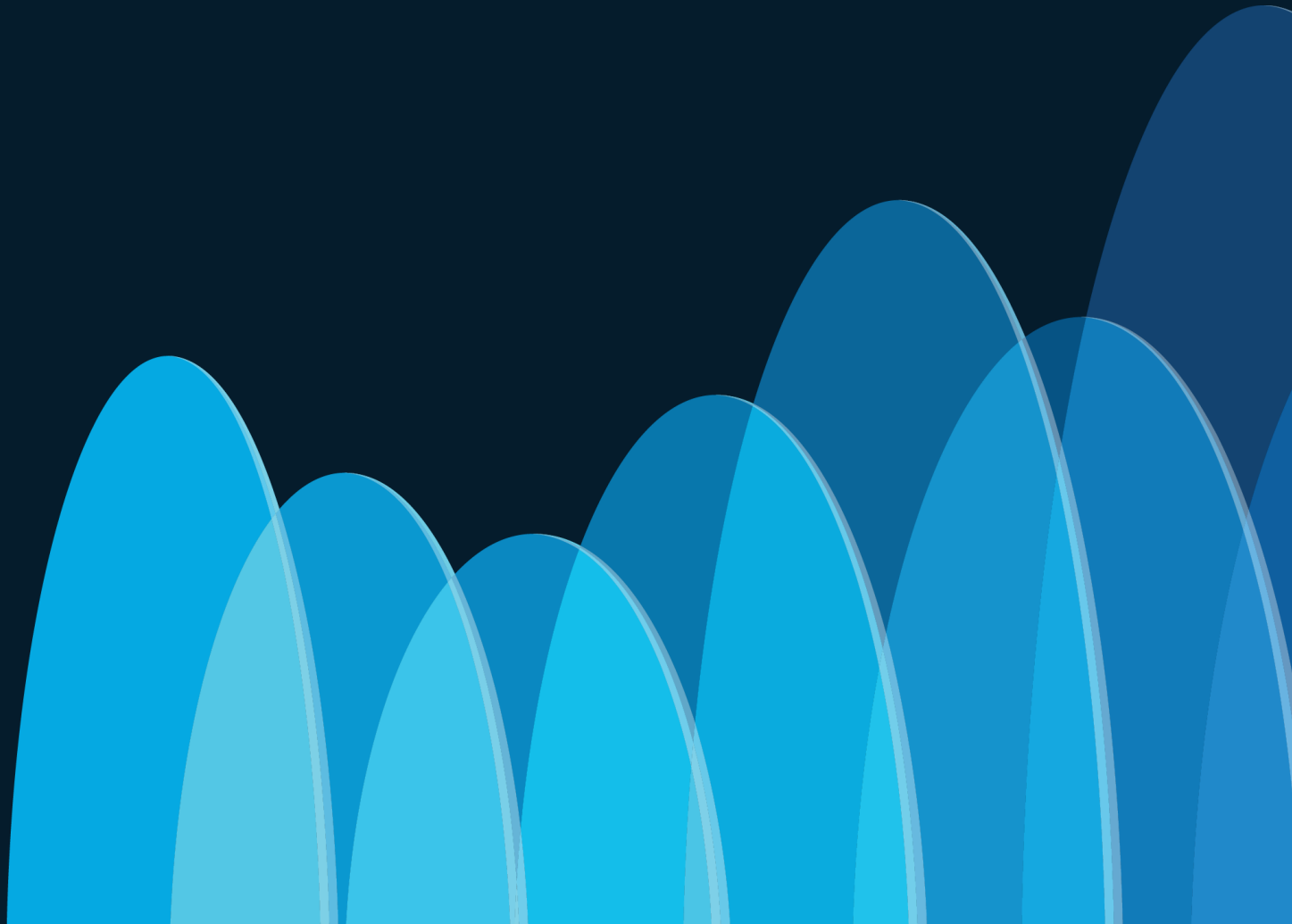


Cisco Secure Access

North Star

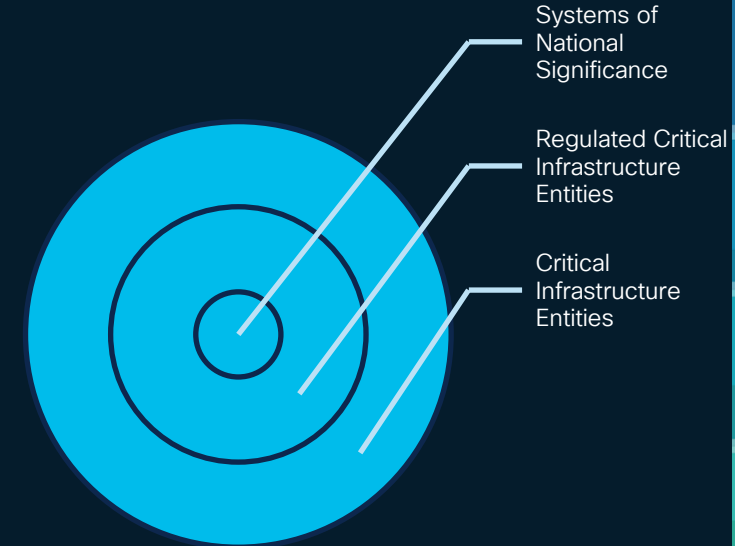


Tightened regulations



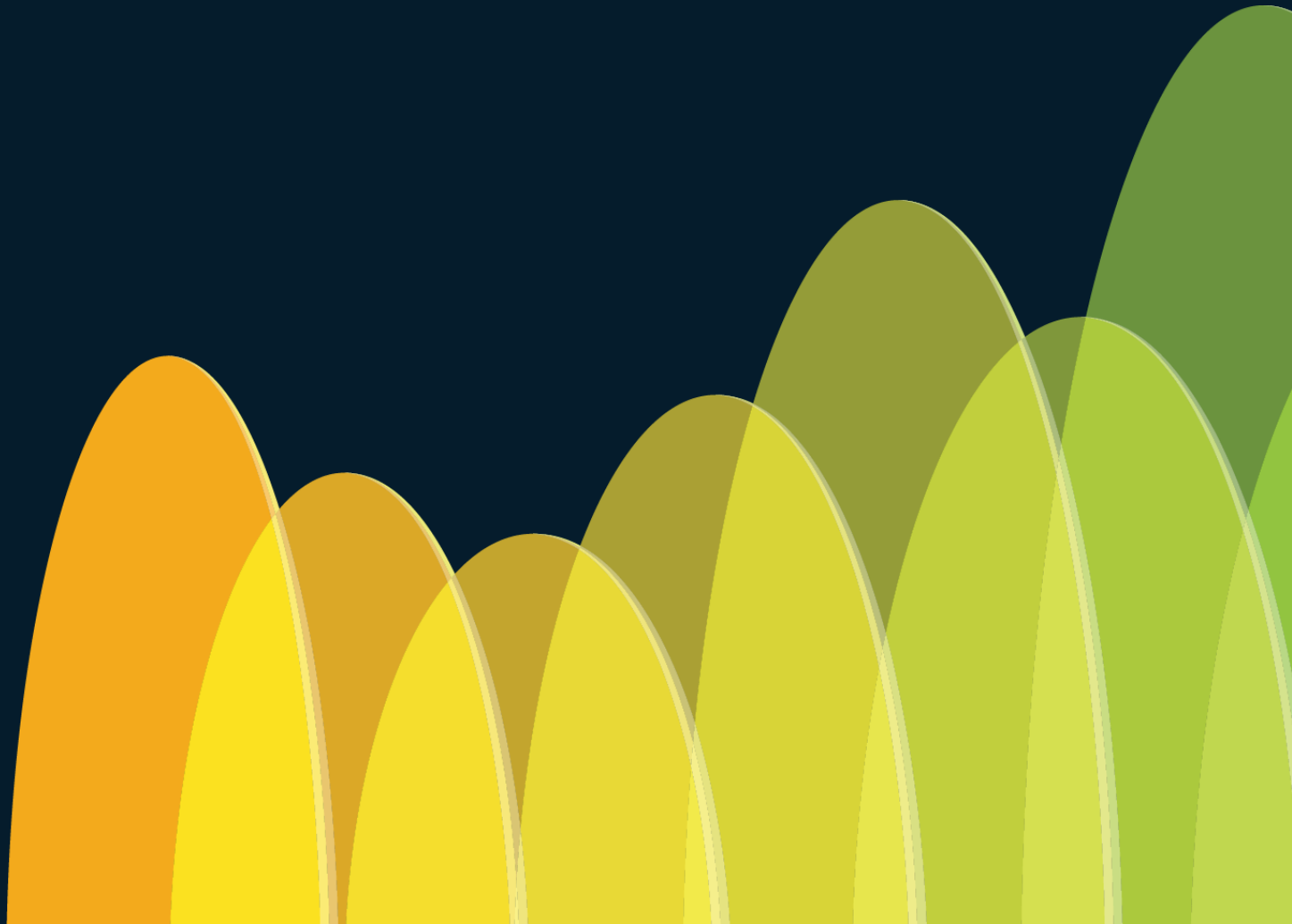
Tightened regulations

- SOCI
 - 11 sectors, Risk Management Plan – 4 hazards
- Australian Privacy Act
 - Increased penalties
 - Tranche 1 – Part 5 – Security, retention and destruction of personal information
 - Tranche 2 – Parts 8-11 – Civil penalties and enforcement powers (for less serious)
- Mandatory guardrails for High Risk AI



<https://trustportal.cisco.com>

Technological advancements



Technological advancements

- AI for Security and
- Security *for* AI
- Guardrails and voluntary standards (in development)
 - ISO/IEC 42001 for AI governance
 - ISO/IEC 23894 for risk management
 - ISO/IEC TR29119-11 and 24027 for testing



The Cisco Responsible AI Framework

Trustworthy AI by Design

At Cisco, we appreciate that Artificial Intelligence (AI) can be leveraged to power an inclusive future for all. We also recognize that by applying this technology, we have a responsibility to mitigate potential harm. That is why we have developed the [six Principles for Responsible Artificial Intelligence](#) of Transparency, Fairness, Accountability, Privacy, Security and Reliability – all necessary for promoting and enabling safe and trustworthy AI.

To implement these principles, we have a Responsible AI Framework that can be applied to the development, deployment and/or use of AI by Cisco, whether in developing a product or model for our customers and partners to use, integrating and building upon a third-party model for unique offerings, or providing AI tools or services for our own, internal operations. In practice, we strive to bring these principles to life by combining Security by Design, Privacy by Design, and Human Rights by Design to surface and mitigate risks to provide AI that is responsible and trustworthy.

Cisco Public



Cisco Principles for Responsible Artificial Intelligence

Our Artificial Intelligence Mission

Artificial intelligence (AI) and subdisciplines such as machine learning offer enormous positive potential for humanity, businesses, and public services that span industry sectors, economies, and societies. These technologies also create new challenges for customers, users, and other stakeholders that deploy, use, or are impacted by them. As part of our ongoing work to maximize the benefits of emerging technologies while addressing challenges and mitigating risks, Cisco has grounded our approach to AI development, deployment, and use in a set of principles and a clear governance framework.

Cisco Public

Tempo



What Kind of Volume?



47 TB
Internet traffic inspected
(NGIPS & Stealthwatch)



1.2 Trillion
Security log events



28 Billion
Netflows **analyzed**
(**Stealthwatch**)



7.6 Billion
DNS requests (**Umbrella**)



13.4 Million
Intrusion alerts (**NGIPS**)



6.25 Million
DNS requests **blocked** (**Umbrella**)

Security Staff & Devices



400 InfoSec & IT
security staff



1,232 Devices deployed
for prevention & detection

Data Analytics
(4TB/day)



2.0 Million
Web transactions blocked (**WSA**)



2.5 Million
Email transactions **blocked** (**ESA**)



17K
Files analyzed (**Threat Grid/AMP**)



2000
Phish emails sent to employees

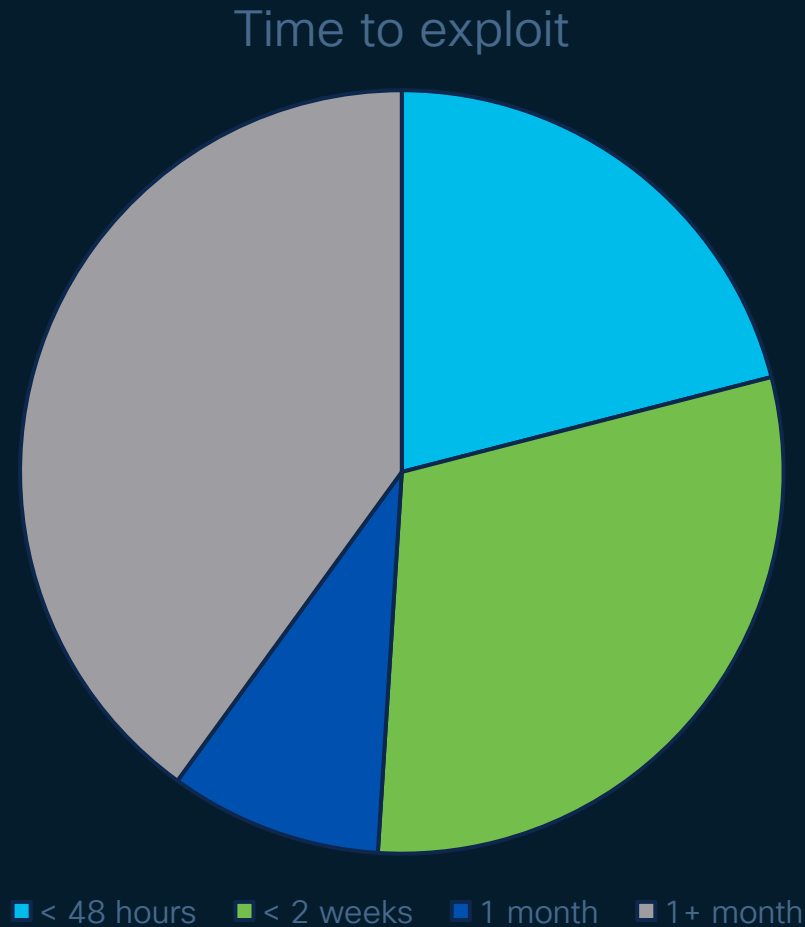


8%
New phish click rate, down from 30%



22 Incidents
...that need analyst intervention

Tempo



Patching

SWIM Upgrades in the Last Year:

- 17.6.4 x 3625 upgrades
- 17.9.3 x 3625 upgrades
- 17.12.2 x 3625 upgrades

Source : Cisco IT



Thank you