Secureworks®

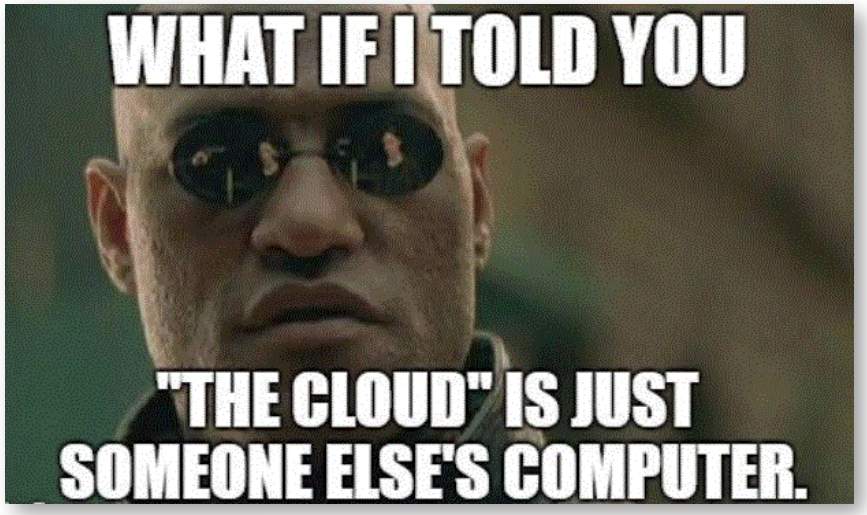
Cybersecurity at Secureworks

Ron Henry,
Director of Corporate Security Governance

Cybersecurity at Secureworks

Agenda

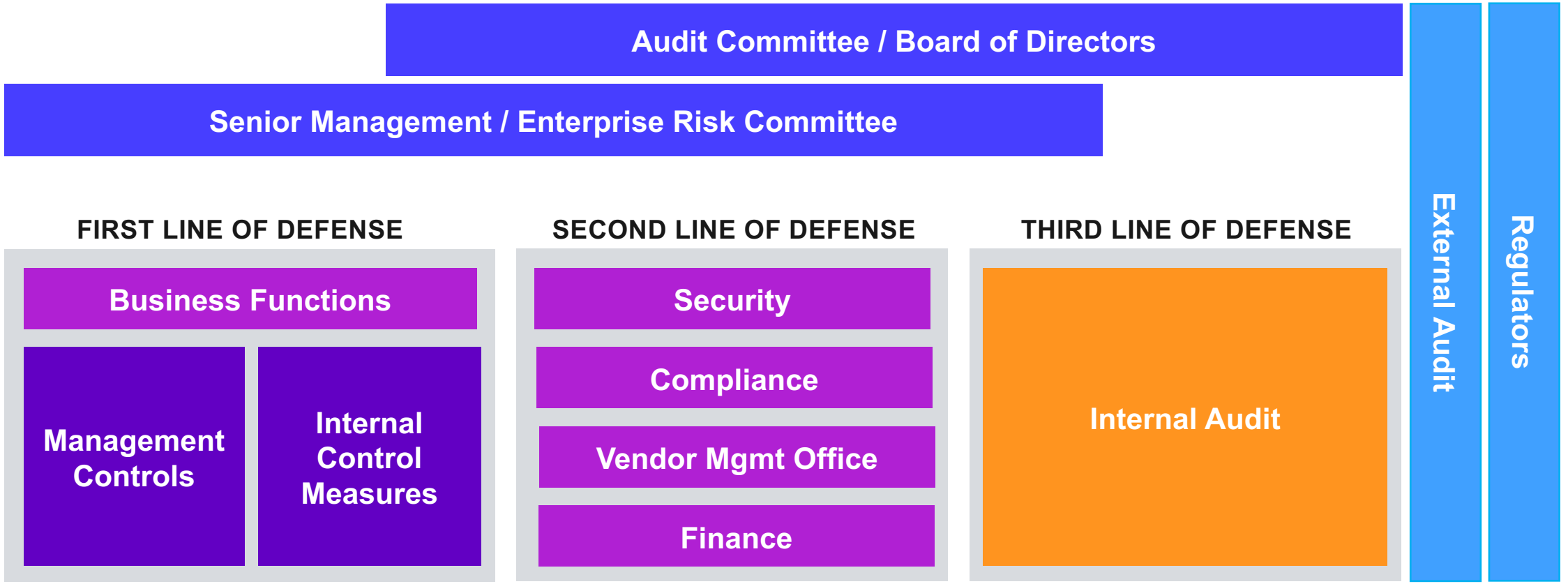
- Overall approach to cybersecurity
  - Enterprise Risk Management
  - Organization
  - Strategy & Goals
  - INFOSEC Risk Management
  - Security by Design
- Cybersecurity Maturity
- Where are we going?



Secureworks

Secureworks Approach to Risk Management

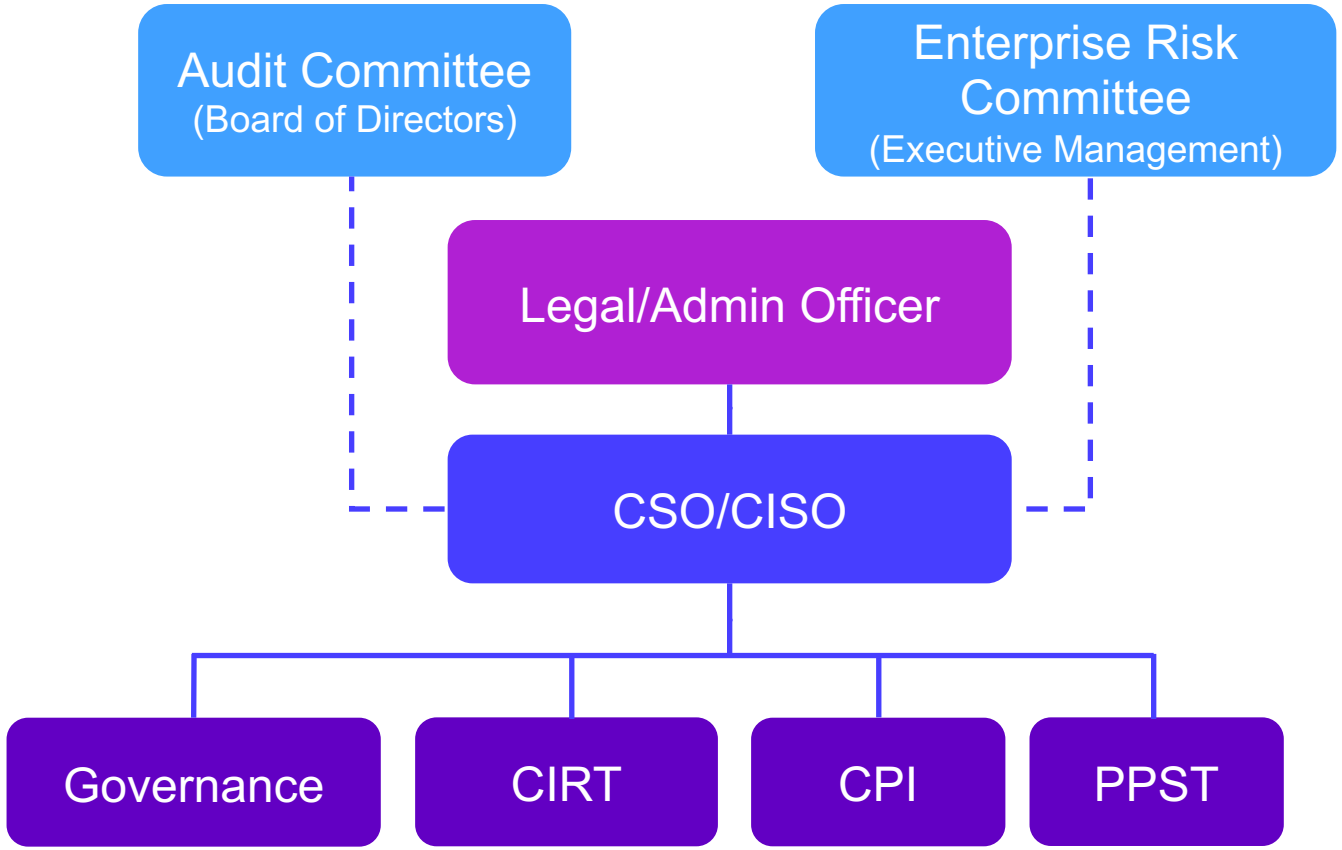
Enterprise Risk Management Framework



Secureworks

Secureworks Approach to Cybersecurity

Organizational & Reporting Structure



Security Governance Team:

- 3rd Party Risk Management
- Business Continuity Management
- Security Control Framework/Risk Management
- Architecture & Strategy

Corporate Incident Response Team (CIRT):

- Vulnerability Discovery & Management
- Threat Management & Incident Response
- Countermeasures & Security Operations

Counterintelligence, Physical Security, & Investigations (CPI) Team:

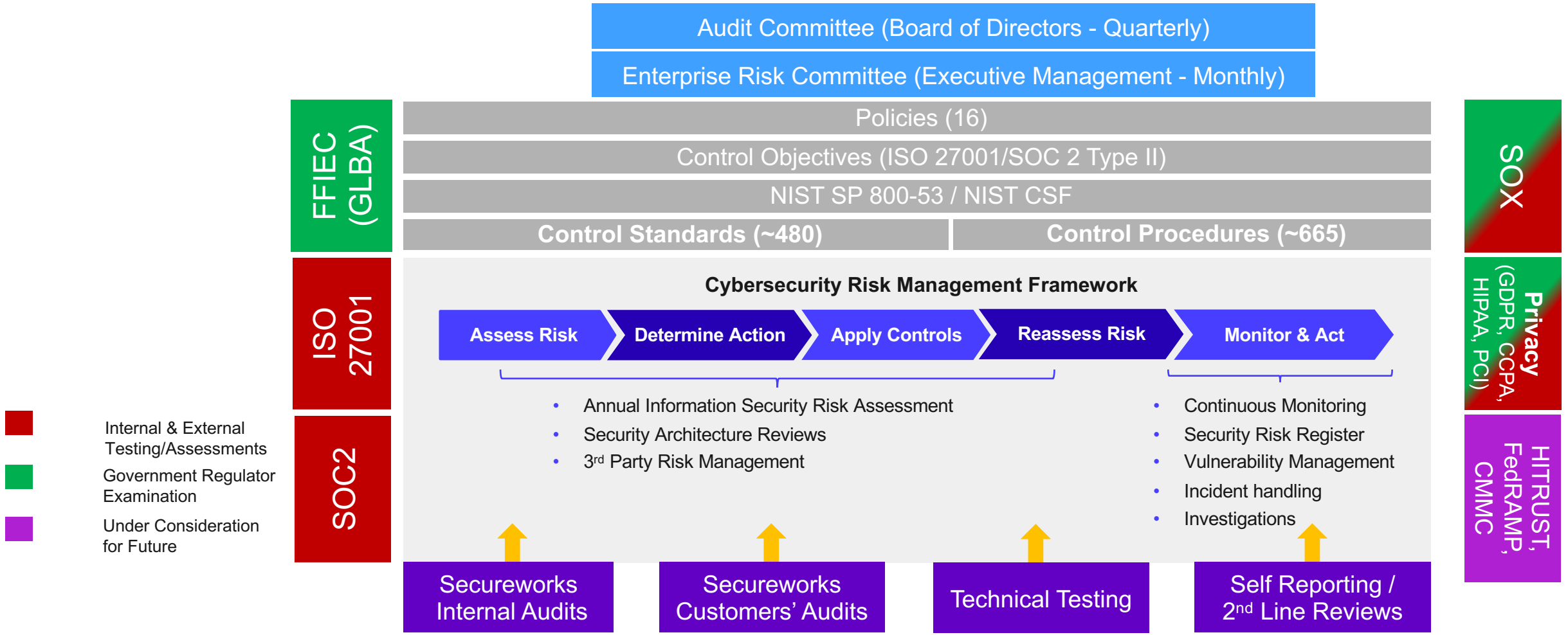
- Regional Security Officers
- Insider Risk Management & Investigations (Security/Ethics/Insider/Etc.)
- eDiscovery
- Physical/Personnel Risk & Threat Assessments

Product & Platform Security Team (PPST):

- DevSecOps
- Technical Testing
- Security Development

Secureworks Approach to Cybersecurity

Cybersecurity Risk Management



Secureworks

Secureworks Approach to Cybersecurity

Objectives & Strategy

Vision

Provide world-class security for all our stakeholders.

Security Objectives

- Every customer loves the security of our products and services.
- Teammates can safely access the tools, resources, and data they need when and where they need.
- Be the trusted choice in security by executing on our security vision.
- Be a great long-term investment by appropriately managing risk.
- Outmaneuver the Adversary and out-innovate the competition by enabling rapid capability development in a secure manner.

The Risks We Face

- Loss of Intellectual Property
- Regulation/Compliance
- Resilience of Critical Systems
- Keeping Pace with Business Transformation
- Third-Party
- Reputation
- Emerging Technology
- Insiders

How We Address them

Secureworks

Secureworks Approach to Cybersecurity

Achieving Our Goals

In order to achieve these objectives, we have adopted the NIST Cybersecurity Framework (CSF)
NIST CSF has become the de Facto standard for Cybersecurity Program Management

Security Objectives

- Every customer loves the security of our products and services.
- Teammates can safely access the tools, resources, and data they need when and where they need.
- Be the trusted choice in security by supporting customer audits with a model program.
- Be a great long-term investment by appropriately managing risk.

Identify

Protect

Detect

Respond

Recover

Secureworks

Secureworks Approach to Cybersecurity

Security by Design

Operational execution requires multiple capabilities…
Information Security Function Operating Model

…but is enabled by the architectural design.

Design facet	Example key choices
Participants	Screen vendors Ensure employee skills
Foundational requirements	Encryption Data classification Data retention
Control type	Appropriate mix of proactive and reactive controls

Source: "Introducing the Gartner Information Security Function Operating Model," (G00370282)

Secureworks

Secureworks Approach to Cybersecurity

Example: Vulnerability Management – Requirements

Vulnerability Classification

- **Emergency/Blocker:** Vulnerabilities that may cause exceptionally great harm to SCWX if exploited and must be addressed with all due haste (e.g., remote code execution vulnerabilities with active exploitation seen in the wild). Have a CVSSv3 score of 10.
- **Critical**: Vulnerabilities that may cause great harm to SCWX if exploited, however a mitigating factor such as difficulty to exploit or compensating controls keep them from being emergencies. Have a CVSSv3 score of 7 or greater (e.g. denial of service for sensitive systems or remote code execution vulnerabilities).
- **Non-Critical/Major**: Vulnerabilities that could harm SCWX. Have a CVSSv3 score of less than 7 (e.g. information disclosure or denial of service for non-sensitive systems).
- **Low-Risk/Minor**: Vulnerabilities that do not pose a meaningful risk to SCWX. Have CVSSv3 score of less than <5

Remediation Targets

- Emergency/Blocker: 96 hours
- Critical: 30 days
- Non-critical/Major: 90 days
- Low-risk/Minor: N/A

Service Level Agreements (SLA)

- **Workstations (laptops, Flex or VDI)** > 96% of devices remediated withing target and nothing is more than 30 days past the target.
- **Emergency/Blocker** = 100% of vulnerabilities are remediated within target and nothing is more than 0 days past the target.
- **Critical** > 96% of vulnerabilities are remediated within target and nothing is more than 30 days past the target.
- **Non-Critical/Major** > 90% of vulnerabilities are remediated within target and nothing is more than 90 days past the target.
- **Low-Risk/Minor** = N/A

Secureworks Approach to Cybersecurity

Example: Vulnerability Management – Operational Design & Reporting

1 ***Example Vulnerability Performance Report***

	SLA	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Now	YTD
Workstations	96	99	99	92	95	97	97	98	98	98	98	98
3 Critical	96	97	88	87	92	96	2 75	81	68	66	74	82
Non-Critical	90	97	98	92	92	92	90	86	91	97	97	93

Open vulnerabilities – 1,505 Critical, and 44,581 Non-Critical 4

1. **Goal setting** - goals must be attainable
2. **Performance** – requires continuous effort and leadership;
   - **Accountability** at the first line leader level
   - Regular **live meeting** cadence (weekly) – Security + IT
   - **Exception process** – remediation dependent on vendors
   - **Tool** – individual access VMS toolset to verify actions
3. **Criticality** – tier so teams can prioritize
4. **Workload / Motivation** – patching it is not a career goal

Prerequisites processes need to be mature

- Asset management across the enterprise
- Infrastructure redundancy / disaster recovery
- Availability monitoring

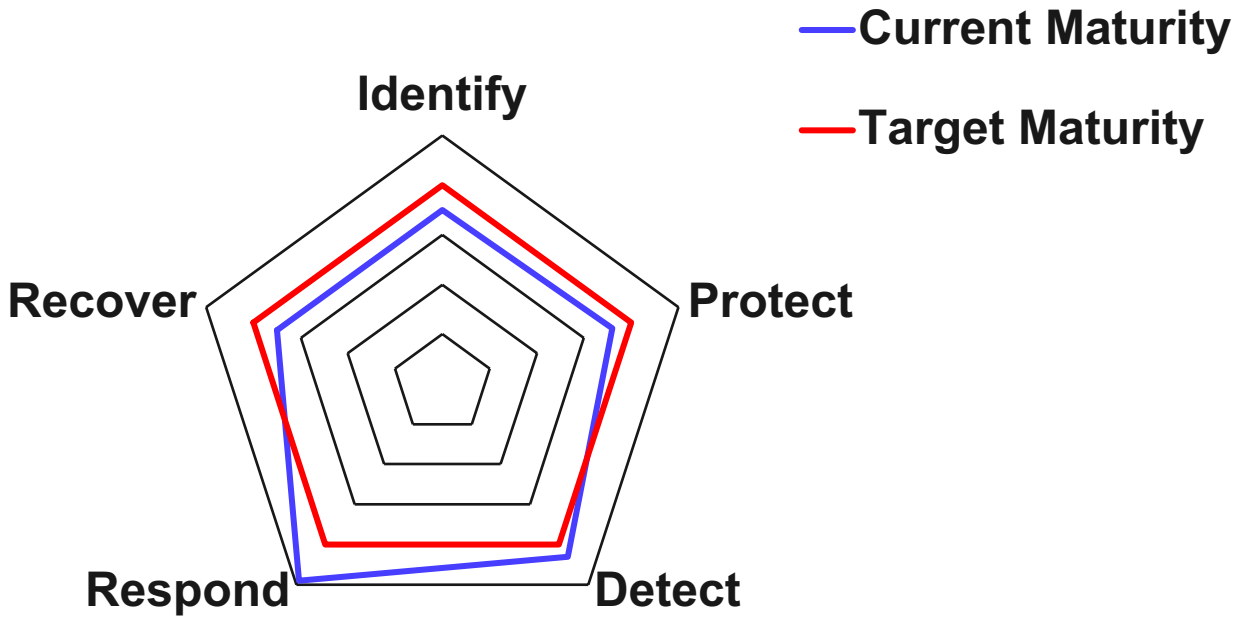
Lessons Learned

- **Goals must be attainable**, previously a single vulnerability was a “failure” so effort waned, use industry benchmarks
- **Automation is critical** to allow security to scale
- Burden of securing immature workloads / infrastructure will **motivate change** (e.g., use of public cloud, SaaS products)

Overall Cybersecurity Maturity

NIST CSF Maturity

Function	**Maturity** (out of 5) **Maturity Target** (4 or above)	
	FY20	**FY21**
Identify	3.3	3.5
Protect	3.5	3.6
Detect	3.8	4.3
Respond	4.1	4.9
Recover	3.0	3.5



Maturity	Definition
1	Processes are *ad hoc* and disorganized.
2	Processes follow a regular pattern.
3	Processes are documented & communicated.
4	Processes are monitored & measured
5	Processes are monitored, measured, and automated

Overall Cybersecurity Maturity

NIST CSF Maturity Drilldown

Function	Maturity (out of 5)	
Identify	3.3	3.5
Protect	3.5	3.6
Detect	3.8	4.3
Respond	4.1	4.9
Recover	3.0	3.5

Category	Maturity
Asset Management	2.8
Business Environment	3.2
Governance	3.8
Risk Assessment	3.8
Risk Management Strategy	4.0
Supply Chain Risk Management	3.0
Identity Management, Authentication & Access Control	3.7
Awareness & Training	2.6
Data Security	3.4
Information Protection Processes & Procedures	3.8
Maintenance	4.0
Protective Technology	4.0
Anomalies & Events	4.4
Security Continuous Monitoring	4.1
Detection Processes	4.6
Response Planning	5.0
Communications	5.0
Analysis	4.6
Mitigation	5.0
Improvements	5.0
Recovery Planning	3.0
Improvements	3.0
Communications	4.0

Our Security Strategy

Why we needed a new Security Strategy?

Our ‘perimeter’ security model had never changed and was beginning to impact company growth

Challenges

- Company security posture needed to be modernized
- Rapid innovation and service delivery were constrained
- Inability to respond quickly to business demand to host services in new geographic regions
- Support ensuring that we remain an innovative leader in the security market
- Attract and retain top talent by providing a modern working environment

Technology Security Strategy Summit - 2017

Vision Core Team

Roadmap Core Team

Vision Breakouts

What changes will I see as we implement Zero Trust?

I can be productive, innovative and work in a collaborative fashion

Our company can innovate and expand at the rate desired by the business

I can login once, with one set of credentials, and access my applications

I have direct access to my applications in an easier and faster manner than today

I can access critical workload directly without Citrix or jump servers

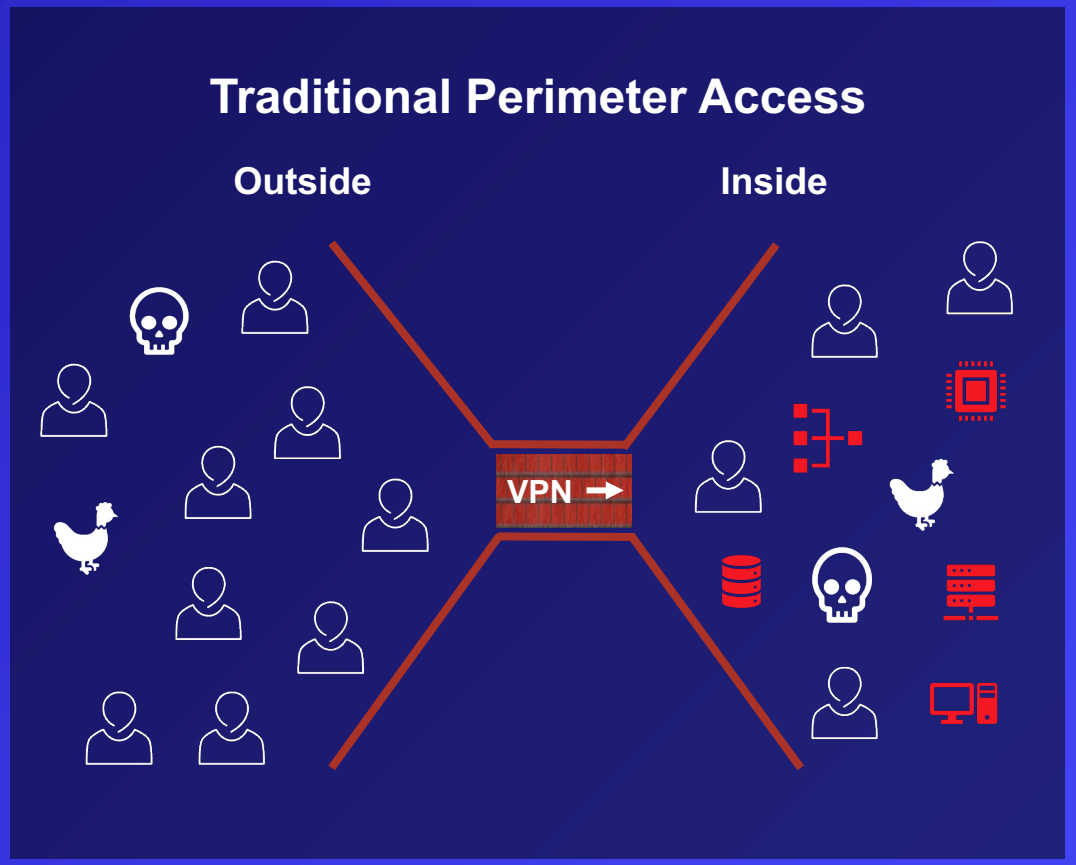
I can access less critical applications with unmanaged devices

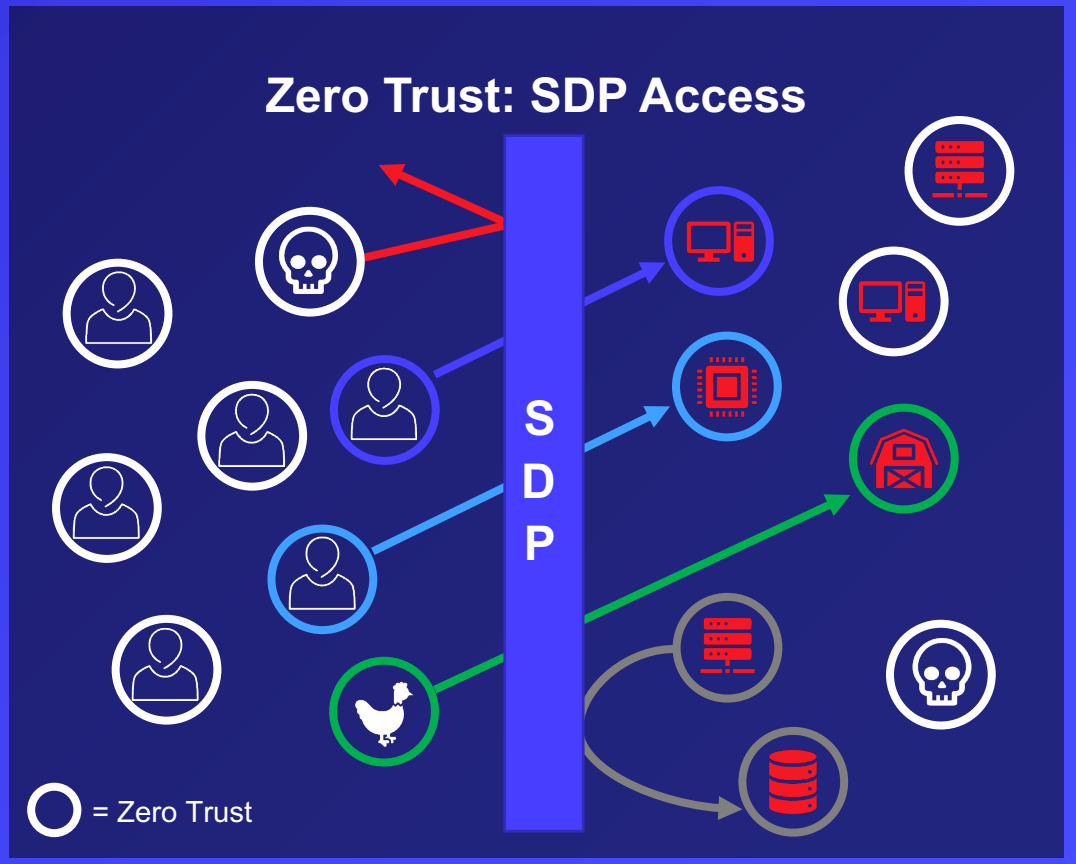
My laptop is no longer overwhelmed by overlapping security tools

What is Zero Trust

Secureworks®

The evolution of the network to Zero Trust enables greater security & flexibility while enhancing the user experience





SDP = Software Defined Perimeter

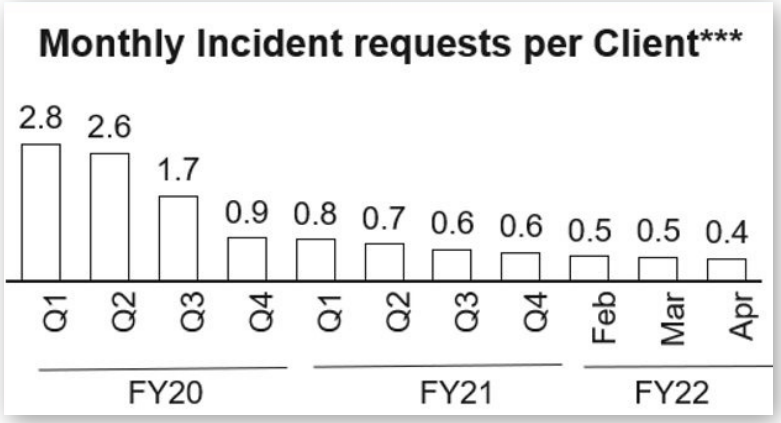
The VPNless Employee Experience

Before VPNless Employee

- OTP Tokens: Continual unlocks & issues
- Many passwords: Continual resets & expirations
- VPN: Instability in modern workplace

With VPNless Employee

- Authentication app: No unexpected token resets or issues. Enforced number match
- MFA with one strong passphrase, expiration only upon demand. Piloting true passwordless!
- Seamless SSO across 75+ SaaS services & cloud environments
- Cloud proxy & Zero Trust “just work”



Secureworks

Our 2021 Digital Transformation Success Measurements

83%

Overall Satisfaction with IT*

⬆ 24% (YoY)

Source: IT Pulse Survey, May 2021

45%

Response Rate

⬆ 80% (YoY)

Source: IT Pulse Survey, May 2021

6%

Reduction in IT Gross Spend**

5.7%

Reduction in Security Gross Spend**

Collaboration (engagement) Increased Entering Pandemic

"Things today with all of the improvements are significantly better than when I started 8 years ago. Great work and know that it is appreciated."

–Secureworks seller

Source: IT Pulse Survey, May 2021

*4 or 5 on a 5-point scale

**Fiscal year before Digital Transformation start –> today

Secureworks

Questions

Secureworks®