Trustwave Penetration Testing

DELIVERING RAPID THREAT DETECTION AND ERADICATION TO ENABLE DIGITAL RESILIENCE

Trustwave®

Contents

About Trustwave and Digital Resilience

About Trustwave

Trustwave is a cybersecurity company with deep expertise in detection and eradication of threats.

Trustwave

Delivering rapid threat detection and eradication to enable Digital Resilience.

- One of the largest and fastest growing, global cybersecurity and managed security services pure-play firms

- By assuming a state-of-compromise, we enable digital resilience by focusing on detection and response

- Our Trustwave Fusion platform provides a unique combination of
  - Consulting and Professional Services
  - Products
  - Managed Security Services

Consulting and Professional Services

Global expertise and best practices to architect and design, to assess and implement and manage and respond. Regional and industry capabilities and expertise

Products

Security technologies from Trustwave and leading partners that control and provide multi-layered protection of critical assets

Managed Security Services

24/7, vendor agnostic global capabilities to monitor and manage critical assets. Threat detection and response using security expertise, AI and analytics. Proactive threat hunting and intruder eradication. Delivered from a technology platform and based upon global and local threat intelligence

200,000+
Business and government customers

5,000+
Enterprise MSS clients

96 countries
Global Trustwave customer footprint

2,000+
Security professionals worldwide

9
Global Security Operations Centers
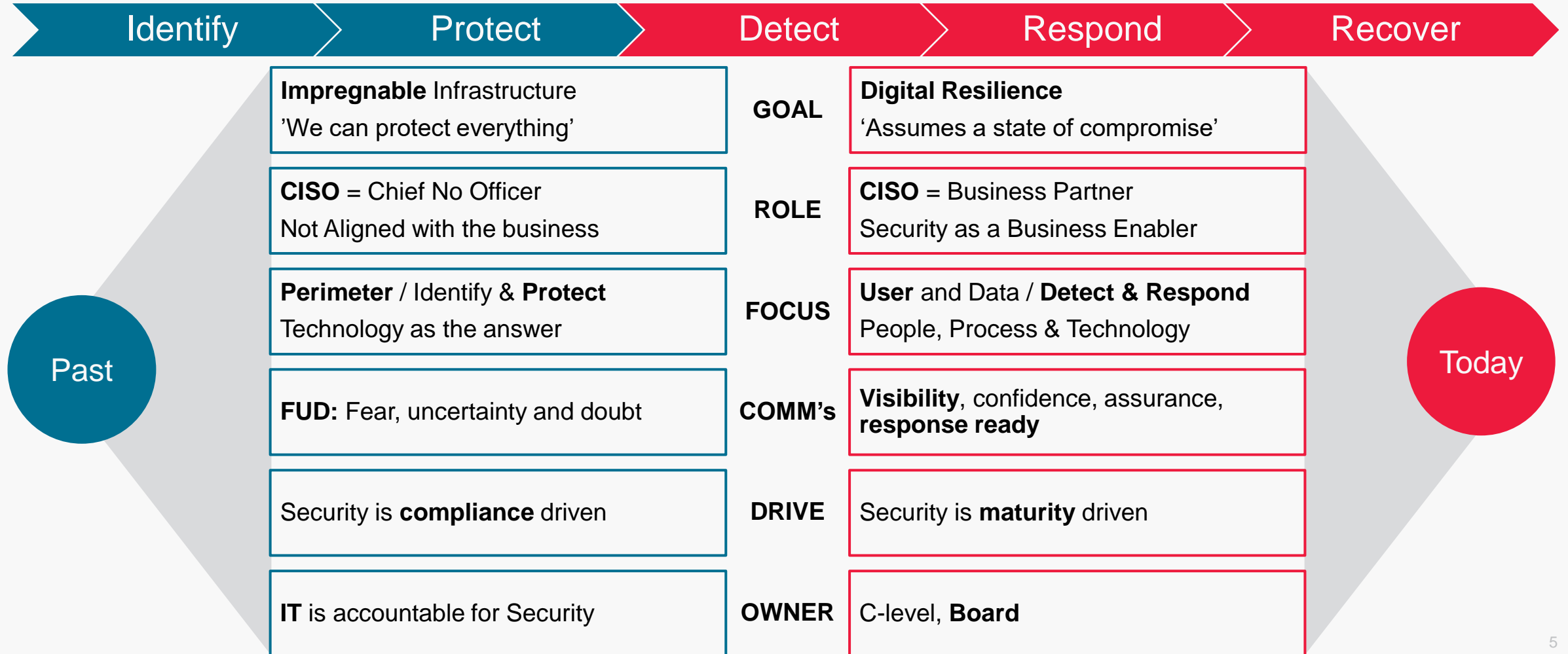
5
SpiderLabs Research Centers

1
Trustwave Fusion Platform

About Digital Resilience

Predicated on an assumption of compromise, digital resilience is the solid foundation that can be built upon to maximise the success of digital transformation by enabling rapid threat detection and eradication.

Identify	Protect	Detect	Respond	Recover

Past

Today

Past		Today
Impregnable Infrastructure 'We can protect everything'	**GOAL**	**Digital Resilience** 'Assumes a state of compromise'
CISO = Chief No Officer Not Aligned with the business	**ROLE**	**CISO** = Business Partner Security as a Business Enabler
Perimeter / Identify & **Protect** Technology as the answer	**FOCUS**	**User** and Data / **Detect & Respond** People, Process & Technology
FUD: Fear, uncertainty and doubt	**COMM's**	**Visibility**, confidence, assurance, **response ready**
Security is **compliance** driven	**DRIVE**	Security is **maturity** driven
IT is accountable for Security	**OWNER**	C-level, **Board**

Building Digital Resilience

Digital Resilience: Penetration Testing

Trustwave SpiderLabs is an elite group of researchers and ethical hackers that deliver a fresh set of eyes and a deeper knowledge to the assessment of ever-proliferating threats.

There is no single best way to defend against compromise. In addition to the millions of vulnerability assessments Trustwave SpiderLabs performed in 2019, Trustwave security professionals conducted thousands of manual penetration tests and red team exercises that helped customers identify and secure weak points in their computer infrastructures.

Test, Assess and Assure

- Trustwave SpiderLabs was one of the industry pioneers conducting remote testing.

- We have a Virtual Remote Pen testing (VRPT) appliance that creates a seamless testing experience.

- Utilising one of our state-of-the-art virtual remote pen test (VRPT) solutions, we can securely increase assurance for all areas of your organisation.

- The Trustwave SpiderLabs Blog contains technical breakdowns of the latest threats, critical vulnerability disclosures and cutting-edge research.

Security Testing Maturity

SpiderLabs Research Centers
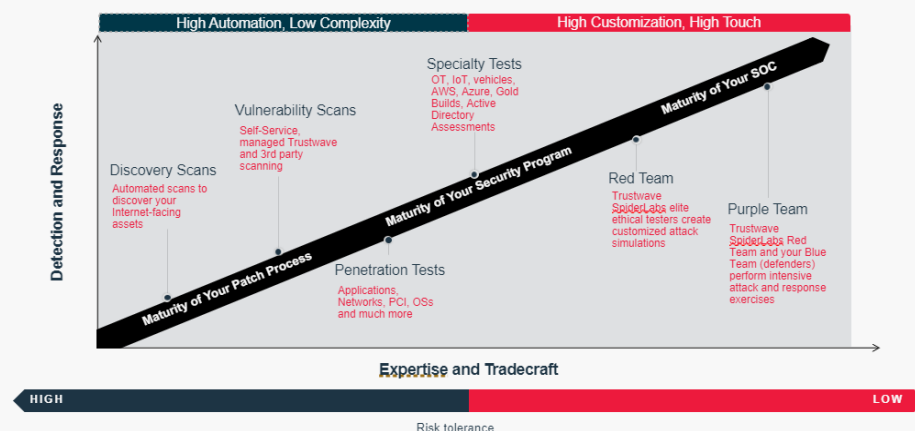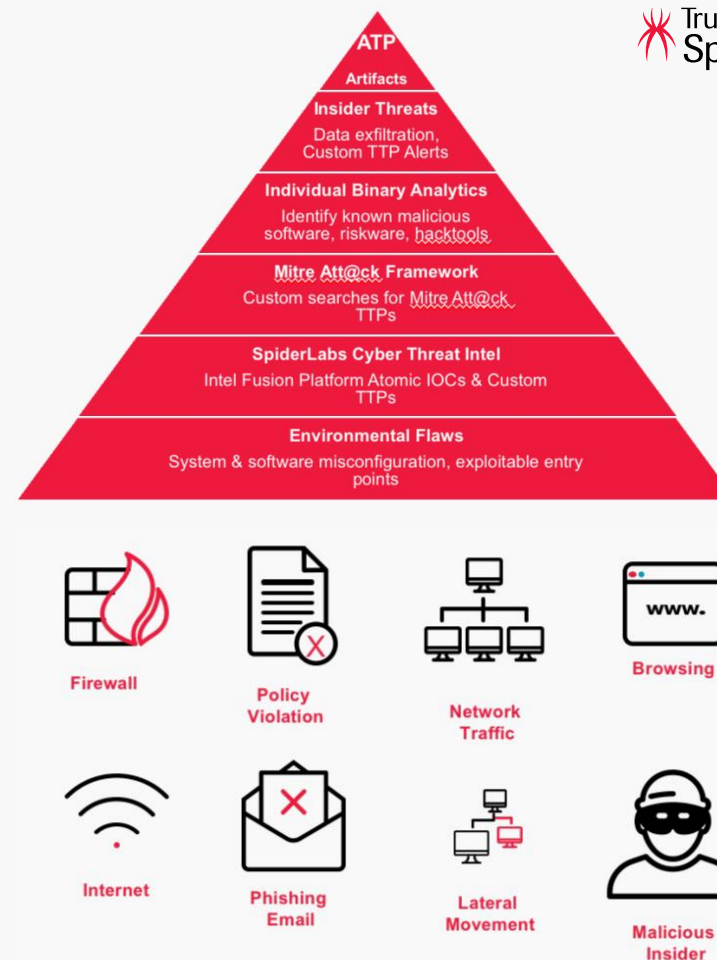
Digital Resilience: Proactive Threat Hunting

Trustwave SpiderLabs Proactive Threat Hunting (PTH) iteratively searches through your architecture to detect and isolate advanced threats that evade existing security solutions.

Detect and Isolate

- There are many reasons to conduct a PTH; to demonstrate due diligence and due care ahead of a merger or acquisition; after a breach event to ensure the threat is gone; to ensure a partner's breach does not extend to your own network; to give a new CISO visibility to ensure there are no existing breaches.

- Using the Trustwave Threat Hunting Pyramid, which enables a systematic and thorough approach, and leveraging a variety of technologies and techniques best suited to your own context, Trustwave SpiderLabs threat hunters are able to identify both cyber hygiene issues and compromises, including advanced persistent threats (APT's), that purely automated PTH solutions often fail to discover.

- The end result is a security roadmap designed from intimate knowledge of every single network callout and binary on every endpoint in your network.

Trustwave
SpiderLabs®

ATP
Artifacts

Insider Threats
Data exfiltration,
Custom TTP Alerts

Individual Binary Analytics
Identify known malicious
software, riskware, hacktools

Mitre Att@ck Framework
Custom searches for Mitre Att@ck
TTPs

SpiderLabs Cyber Threat Intel
Intel Fusion Platform Atomic IOCs & Custom
TTPs

Environmental Flaws
System & software misconfiguration, exploitable entry
points

Firewall   Policy Violation   Network Traffic   Browsing

Internet   Phishing Email   Lateral Movement   Malicious Insider

Some of the items profiled in a Trustwave Threat Hunt

Digital Resilience: Application Testing

Trustwave SpiderLabs penetration testing is an authorized simulated cyberattack on computing environments that require security professionals who combine automation with advanced tools and their own expertise to find ways an attacker can compromise a target environment.

Review, Test and Uncover

- Pen testing uses techniques such as electronic social engineering, password brute-forcing and network-layer and legacy protocol attacks to demonstrate how those weaknesses can lead to compromise.

- Pen Testing can help identify issues including:
  - Business Logic Flaws resulting in international money laundering and theft.
  - Horizontal and vertical privilege escalation causing large scale data integrity issues.
  - API interaction leading to complete authentication or 2FA bypass.
  - (De)Serialization vulnerabilities opening up a command shell on the hosting infrastructure.

- Application penetration testing, coupled with our Secure Development Life Cycle (SDLC) training, cloud security offerings and consultancy services are designed to help regardless of where you are on your journey.

Digital Resilience: Cloud/Container Testing

A Trustwave SpiderLabs cloud or container penetration test predominately utilises the same approach as our more traditional testing, however allowances are made for data being housed in a shared environment, and the potential compromises that this can bring about.

Identify, Test and Assure

- Whether you are using a public, private, community or hybrid cloud solution, authentication mechanisms are critical to your security. In addition to our standard testing approach, we place additional emphasis on:

  o Reviewing authentication paths and privilege access management controls that enable data and resource access.

  o Assessing development operations processes that can introduce new security vulnerabilities.

  o Leveraging renown best-of-breed internal tooling to uncover specific cloud-based weaknesses.

- Cloud assurance, coupled with our application penetration testing, Secure Development Life Cycle(SDLC) training, and consultancy services can increase assurance regardless of where you are on your cloud journey.