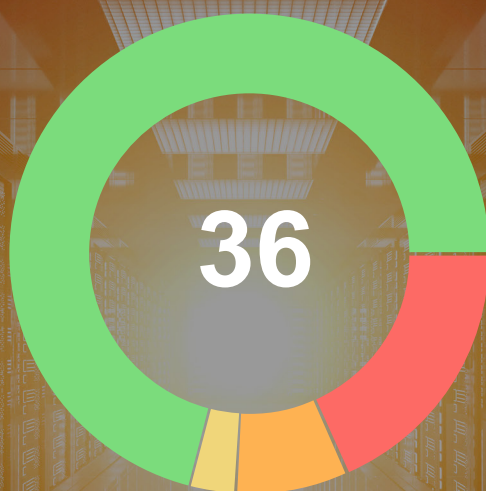




Cavirin Cyber Posture – Your Credit Score for Security

Why Enterprises Need a Cyber Posture Score

Who should Read this Whitepaper

Chief Information Security Officers (CISOs or CSOs) or Directors of Information Security looking to have a simple, single, and accurate view into their cybersecurity posture, that will span their entire hybrid infrastructure.

Why a Cyber Posture Score?

Many CISOs are in a bind, expected to deliver on security in the face of a skills gap, budget pressures, and more complex hybrid infrastructure deployments. They are also running scared, with 91% of organizations concerned about their cloud security, according to the Cybersecurity Insiders 2018 Cloud Security Report. Today's companies realize that the different cloud services, if not configured properly, introduce many potential attack points for hackers. Four specific cloud security concerns include **visibility, compliance, consistency of policies, and the pace of innovation** (see diagram below).

The solution? In the same way that a credit score offers a single view – a number – into the creditworthiness of an individual or organization, an equivalent in the cybersecurity space will offer the CISO a view into the 'Cyber Posture' of their organization. This score spans the hybrid infrastructure, including on-premise and cloud workload OS configurations, as well as the security posture of the different cloud accounts. Depending on the organization, it may also receive feeds from 3rd parties such as Threat Intelligence or may generate input to an existing enterprise dashboard. In any case, a score that offers actionable insight will help the CISO and their staff better secure their infrastructure, as well as focus budget and training.

The Cyber Posture score provides you with multiple advantages:

- Reflects the efficiency of your Information Security and Corporate Compliance program(s)
- Permits a better understanding of your risk/security/compliance posture and how to address the most important concerns
- Reviews your internal security/compliance controls against the most common threats
- Benchmarks and compares your security performance against industry peers and competitors
- Permits you to effectively report cybersecurity to the board



Source: Cybersecurity Insiders 2018 Cloud Security Report

Risk, Compliance & Posture

First off, a bit of terminology to clear the air between risk, posture, and compliance. Risk is a way to balance the impact of breach against one's business requirements, compliance is conformity to a set of regulations, guidelines, and best practices, and security's goal is to protect. One way to look at risk is to maximize the good and minimize the bad, while not impeding growth.

The goal of compliance is conformance and includes enforcement, risk mitigation, and assessment of the integrity of the infrastructure. Finally, security includes protection of confidentiality, integrity, and availability of assets.

One's posture reflects the 'strength' of the organization and is an inverse of risk. In the case of Cavarin's Cyber- Posture score, the maximum is 100. Compare this to a credit core that maxes out at 850. Using the same 100 point scale, a risk of 100 would be critical, further defined by mapping this to a risk assessment matrix. Compliance is also scored where a higher number is better. For example, if a given workload is assessed against PCI, a score closer to 100 infers that fewer tests failed. The same applies to cloud security posture assessment, where a higher score reflects a more secure cloud environment.

Now looking at the score in more detail, to be useful, it must meet the following five characteristics:

- **Comprehensible** to a user with minimal cybersecurity training
- **Meaningful** – represents risk adequately and helps drive prioritized action plans
- **Defensible** – based on industry-standard cybersecurity frameworks
- **Comprehensive** – incorporates all available platform risk signals
- **Extensible** – able to incorporate risk signals that are added in the future

The Cavarin Cyber Posture Score

The concept of the Cyber Posture score is to evaluate and report out on the overall security posture risk of an organization, and just like a credit score, which is comprised of a number of elements – on-time payments, length of credit history, types of credit used, and more – the Cavarin Cyber Posture score takes into account multiple inputs cross the hybrid infrastructure.

Implementing Cyber Posture scoring in fact closely parallels the steps taken by many hackers, and results in a layered security framework that helps counter attacks.

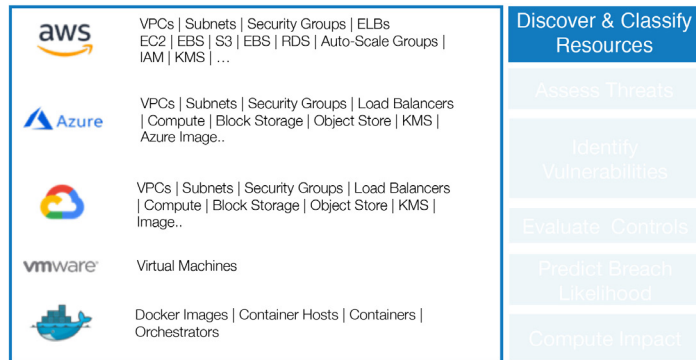
Consider WannaCry Ransomware from 2017.

We can map the Cyber Posture scoring approach to each of these steps:

Recon Resources	Hunt Internet-facing machines with TCP:445 (SMB) open
Threat Event & Actor	Ransomware: Shadow Brokers (North Korea?)
Exploit Vulnerabilities	Windows flaw in SMB protocol (on TCP: port 445) - allows remote code execution Internet facing machines with TCP:445 (SMB) open
Missing Controls	Microsoft patch (March 2017) - most victims had not applied Block TCP:445 (SMB) on Internet-facing machines
Breach	Ransomware – encrypts Windows file system
Business Impact	Huge: Unavailability of Critical Resources

Discover and Classify Resources

The first step is discovery, as well as determining asset criticality. Data discovery and classification provide a solid foundation by identifying risky areas in your IT network. Though Cyber Posture scoring focuses on information assets, a comprehensive risk assessment will also include software and physical assets, services, and people. One method of assessing criticality is to map to the CIA model – Confidentiality, Integrity, and Availability. This is further defined in the appendix. Information resources include servers, cloud services, and the container environment.



It's essential to automatically identify existing and new workloads as well as changes to existing ones across multiple cloud service providers, and have the ability to properly group these by function. This discovery should be a simple process, leveraging existing AuthN and AuthZ policies to avoid having to create a special IAM policy every time.

Assess Threats

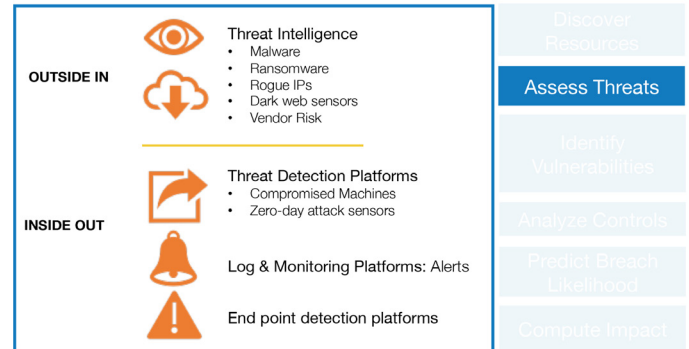
Next, you'll want to assess for threats, taking both an outside-in and an inside-out approach. This is really where you get an understanding of the potential threat environment.

Threats include the types of attacks and external conditions that may lead to a breach. Note that threat events fall into two categories – those that directly result from malice (e.g. a hacker trying to steal data), and those that are unintentional due to poor training or processes (e.g. an admin who change S3 bucket permissions without understanding consequences). In any case, threats target hybrid infrastructure vulnerabilities, by looking at the configuration and software of the asset itself, and as assessed against common regulations and benchmarks.

These include:

- Configuration related vulnerabilities
- Software defects related vulnerabilities
- Compliance framework related vulnerabilities

One important element of threat assessment is the use of Threat Intelligence (TI) feeds. This permits some of the assessments to draw data from across the Internet for more accurate scoring. For example, the latest logged vulnerabilities or zero-day attacks. Depending upon the deployment, this TI feed may play a role in Cyber Posture scoring or may be used as part of a larger enterprise logging system.



Identify Vulnerabilities & Evaluate Controls

According to owasp.org, a vulnerability is a weakness in an application, operating system, or other component, that allows an attacker to cause harm or compromise. The weakness can be a design flaw, misconfiguration, operational lapse (ineffective security practices), or other attack vector. It's critical to identify where the infrastructure is vulnerable, by assessing and monitoring the different assets, implementing controls to mitigate the different threats. The actual assessments rely on different regulations, guidelines, and best-practices, while cloud account monitoring is continuous and leverages the real-time tools provided via the different public cloud provider APIs. Note that this monitoring also aligns with the CIA model, in that one cloud service may require more availability or confidentiality than other. The output of this phase is a 'raw' score that reflects the current vulnerability of your infrastructure.



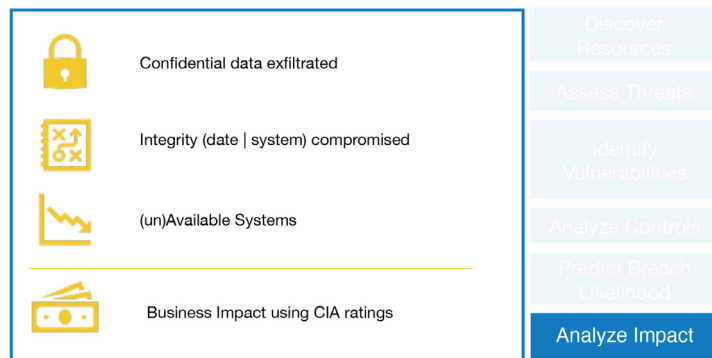
Determine Likelihood

The output of the previous step is now combined with an understanding of the likelihood of breach. This relies on historical trends, the industry in question, the current patching regimen, and what types of attacks are actually possible against the identified vulnerabilities.



Analyze Impact

Taking into account the likelihood, the final step is analyzing the impact of the attack. Closing the loop with WannaCry, the impact of the attack was grave to those organizations that were unprepared, costing more than one upwards of hundreds of millions of dollars.



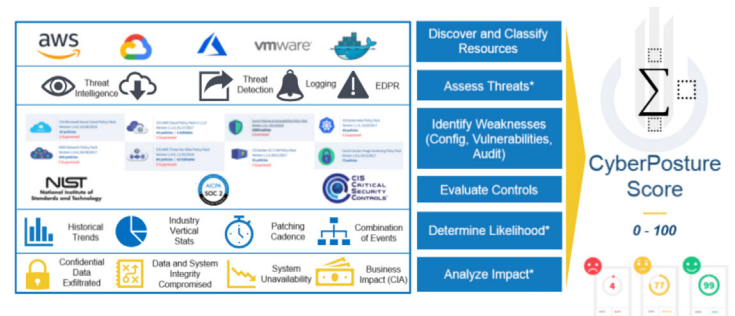
In many cases, likelihood and impact are combined into a combined matrix that reflects overall risk.

The Likelihood is the probability of the asset being compromised due to threats exploiting the specific vulnerabilities above, while the impact is the business loss resulting from an unanticipated breach.

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

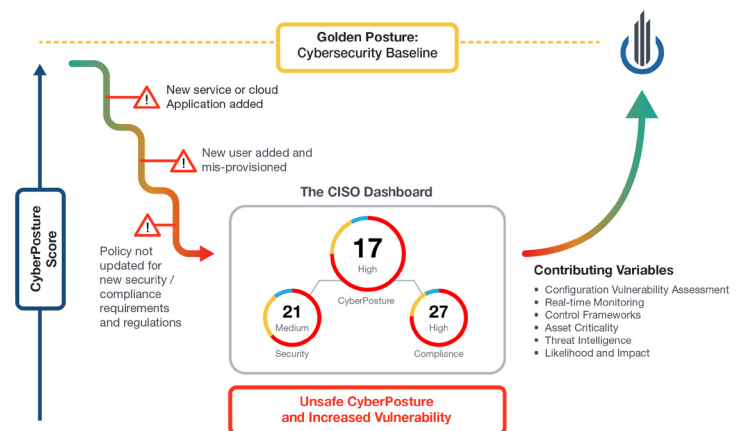
Bringing it all Together

Developing the Cyber Posture score builds on each of the steps identified in this paper. The hybrid infrastructure consists of both workload assets and cloud services. Cavarin has visibility into the OS, both VM and container, of the workloads, as well as a key set of cloud provider services. IT now applies assesses the external threats, and identifies any vulnerabilities as evaluated against the different controls. The combination of the threat analysis and vulnerability assessment permits one to evaluate the likelihood of a given threat impacting the infrastructure, as well as its expected impact. Remember that the faithfulness of the score is directly related to the rigor and honesty that goes into each phase of the process.



Cyber Posture and “Golden Posture”

The Cyber Posture score is only half of the solution. To be really effective, it needs to be associated with what we call the “golden posture”. This is the target Cyber Posture score that an organization wishes to achieve and is a function of a number of factors, such as costs incurred, time required, regulatory and corporate policy requirements and their risk tolerance abilities. One approach to developing this is to leverage the NIST CSF to assess and plan one’s security program.



For example, based on a risk assessment, an organization sets their golden posture at 85. After the first assessment, the Cyber Posture score is 75. The Cavarin solution provides remediation guidance to raise the score from 75 to 85. Later, the score slips from 85 to 82. Here, the CISO is immediately made aware of what negative changes impacted the score.

Every Company Needs a Credit Like Score Rating

Much like a “Credit Rating” the Cyber Posture score combines multiple factors into providing you a real-time view of your overall cybersecurity posture risk. Factors include:

- Configuration + Vulnerability Assessment
- Real-time Monitoring
- Control Frameworks
- Asset Criticality
- Threat Intelligence
- Likelihood and Impact

If your organization is not looking at all these factors across the entire IT infrastructure, when calculating the algorithm of your cybersecurity posture, you will be misguided into a level of security that is only part of your entire picture. With Cavin's Cyber Posture Intelligence, you will be provided a score that incorporates all the factors and permits you to better fend off attacks and breaches and their potential costs and disruption to your business. It also helps your organization to better align internal resources, including budgeting and training, to more effectively address the most important threats that you expect to face.

About Cavin

Cavin delivers an Enterprise-Class Cyber Security framework that presents up-to-the-minute knowledge of system-wide security strengths and weaknesses. Whether in the cloud, or the corporate data center, our agentless CyberPosture Intelligence solution enables cross-platform security monitoring, reporting, remediation, and compliance. Our focus is to provide concise views into the security framework of Enterprise systems to empower CSOs and their teams to respond to threats rapidly and decisively.

Cavin Systems, Inc.
2114 Ringwood Ave,
San Jose, CA 95131,
USA.

sales@cavin.com
www.cavin.com

APPENDIX

Asset Criticality and CIA

Determining asset criticality is the first step in developing an overall risk assessment. Assets fall into the following categories:

- **Information Assets:** This includes databases & data files (including important data in local desktops/laptops), system documentation, user documentation, training materials, operational/support procedures, continuity plans, archived information, etc.
- **Software Assets:** This includes application software, system software, development tools, utilities, etc.
- **Physical Assets:** This includes computer equipment (e.g. processors, monitors, laptops, modems, and printers) etc.
- **Services:** This includes general utility services such as power, lighting, and air conditioning, etc. for IT equipment.
- **People Assets:** This includes people performing roles for the IT department.

Each asset is now rated on a scale of 1 (negligible) to 5 (very high) for Confidentiality, Integrity, and Availability ("CIA"). The legends are explained in detail in the table(s) below. These ratings are set by experts in the organization, and one approach to keeping a balanced view is to have two sets of assessments, one internal to the department or business unit, and the other from a cross-functional team, and then average the results. The overall criticality of a given asset is a sum of the sub-scores, in this case, a total of 3-15.

Confidentiality / Integrity

Negligible (1)	No impact if the asset is compromised.
Low (2)	Insignificant impact if the asset is compromised. Typically, this includes information which will not result in a financial/business loss to the organization, if made available publicly.
Moderate (3)	Some impact if the asset is compromised. This may result in some level of business/financial loss, if disclosed to unauthorised users.
High (4)	Significant impact if the asset is compromised. This will probably result in significant business/financial loss to the organization.
Very High (5)	Severe / highest impact if the asset is compromised. This will most probably result in very high business/financial loss, which may be disastrous to the organization. Think of the Sony and Equifax breaches as examples.

Availability

Negligible (1)	No impact if the asset is compromised.
Low (2)	Non-availability of the asset will have minimal / insignificant impact to the organization.
Moderate (3)	Non-availability of the asset may have some impact on the organization if prolonged for a long period of time.
High (4)	Non-availability of asset will result in a significant impact to the organization.
Very High (5)	Non-availability of the asset will result in very high consequences--severe loss to the organization.

More information on the CIA triad is here.

Generic Risk Model

