FORTINET

WHITE PAPER

Proactive, Actionable Risk Management with the Fortinet Security Rating Service

Executive Summary

As enterprise networks become more distributed and the threat landscape increases in complexity, the CISO plays a crucial role in enabling the business. The Fortinet Security Rating Service, which is included in the FortiGate Enterprise Protection bundle, provides tools that allow security teams to improve their security posture over time in measurable ways, reporting those results to executive management, boards of directors, and auditors. Additionally, it helps organizations to understand where they stand in relation to peer organizations and accepted standards. At the same time, the Security Rating Service provides actionable insights into configuration changes and steps they can take to improve their risk posture.

As enterprise networks and the threat landscape become more complex, the role of the CISO has evolved beyond that of a technology provider. Today's CISO is expected to be a business enabler—preventing security events that would impact the business while minimizing obstructions caused by security technology and processes. A study by Deloitte[1] highlights the "four faces of the CISO":

1. **Technologist.** A CISO should understand security technology, regulations, and frameworks and be able to match those with the requirements of the individual organization.
2. **Strategist.** A CISO should be able to look at the big picture and know how to adjudicate among competing priorities according to the needs of the business.
3. **Advisor.** A CISO should be a trusted consultant to executive management and the board of directors on a host of information security issues—including new and emerging threats.
4. **Guardian.** A CISO needs to continually monitor operations and make sure there are no gaps in technology, processes, or human resources.

Tomorrow's CISOs will have to be on intimate terms with every aspect of the organization.[2]

The CISO fulfills four basic roles, and all of them are critical: technologist, strategist, advisor, and guardian.

While the first three roles are vitally important—and probably more interesting to most CISOs—the fourth role, the guardian or operations leader, is often underrated. Because it involves the operational side of cybersecurity, it is viewed as more tactical and less strategic than the other roles. However, the best strategy and technology will not protect an organization if processes are not optimized and if the people who execute them lack the requisite skills to ensure that best practices are followed. It could be argued that without his or her operational ducks in a row, a CISO cannot fully function as a business enabler.

Operational Complexity Can Impede the Business

Leadership of security operations becomes more important—and more difficult—as enterprise networks become increasingly complex. The CISO is faced with an IT network that is growing exponentially in size, in addition to the footprint that it covers.

At the endpoint, Internet-of-Things (IoT) devices are dramatically increasing the sources of new data.[3] In the network, data and services are housed in multiple cloud platforms rather than being confined to the on-premises data center.[4] Network traffic now travels on the public internet in companies using software-defined wide-area network (SD-WAN) technology.[5]

The challenges do not stop there. Many organizations have connected their operational technology (OT) networks to the internet or the IT network in recent years, exposing them to external threats for the first time.[6] And the increasing prevalence of edge processing means that some data may be collected and processed without ever being placed in a corporate data repository, increasing compliance risk.[7]

These are all examples of how a broadened network expands an organization's attack surface. Unfortunately, these trends have converged with another trend—an increasingly advanced threat landscape. In the third quarter of 2018, FortiGuard Labs detected almost 34,000 new malware variants, a 43% increase over the second quarter and a 129% increase over the first quarter.[8] But the problem is not simply with quantity. Threats now move at machine speed, enabling exfiltration of corporate data in minutes, while 68% of breaches still take months or longer to discover.[9] Such security incidents impede not only the IT security team but also the entire business.

The current cost of the typical data breach is $3.86 million, and there is a 27.7% chance the typical company will experience a material breach over a two-year period.[10]

The Security Rating Service relies on the integration provided by the Fortinet Security Fabric to deliver actionable threat intelligence.

Three Questions for Security Oversight

The CISO's security oversight responsibility is broad, but can be boiled down to three basic questions:

1. Is my network security set up properly?

The root cause of a large number of data breaches is configuration errors.[11] The complexity of networks—and the security technologies that protect them—means that it is easy to overlook a configuration detail during setup. Unfortunately, it is difficult for organizations to perform a single comprehensive check for configuration problems—let alone set up ongoing monitoring—when they operate in a widely distributed infrastructure.

2. How can I show the organization that we are secure?

With so many valuable business assets now in the IT network, cybersecurity is no longer a niche topic at most organizations. In fact, it is discussed in 89% of board meetings,[12] and fewer than 15% of corporate boards are satisfied with the quality of cybersecurity information provided by CISOs.[13] There are multiple reasons this is the case, but a major one is that providing a global view of the security posture in a consumable format can require significant manual work in some organizations.

3. How can I demonstrate compliance to my auditors?

New regulations and standards have impacted almost every organization in the past decade, and some of them are daunting. Data complaints increased by 37% after the EU's General Data Protection Regulation (GDPR) went into effect,[14] and 80% of organizations are not yet GDPR compliant.[15] And North American organizations now face similar requirements when the California Consumer Privacy Act (CCPA) comes online.[16] Even when an organization is compliant, auditors do not simply accept the word of the CISO, but need proof of compliance in a particular format.

Fortinet Security Rating Service: A Clear View with Actionable Recommendations

The Fortinet Security Rating Service provides actionable information to help organizations design, implement, and maintain the security posture to fit their business needs. Included in the comprehensive FortiGate Enterprise Protection bundle, the Security Rating Service is built on the security best practices that underlie the Fortinet Security Fabric.

By accessing the various features of the Security Rating Service, security teams can:

- Understand their organization's security posture compared with peer organizations, recognized standards, and what is important to the business
- Identify critical vulnerabilities and configuration weaknesses in their Fortinet Security Fabric setup and prioritize and implement best practice recommendations
- Provide up-to-date risk and vulnerability data to corporate leadership in the context of what is important to the business
- Run compliance checks to ensure that operations run in a way that satisfies auditors
- Keep pace with the evolving threat landscape with updated recommendations

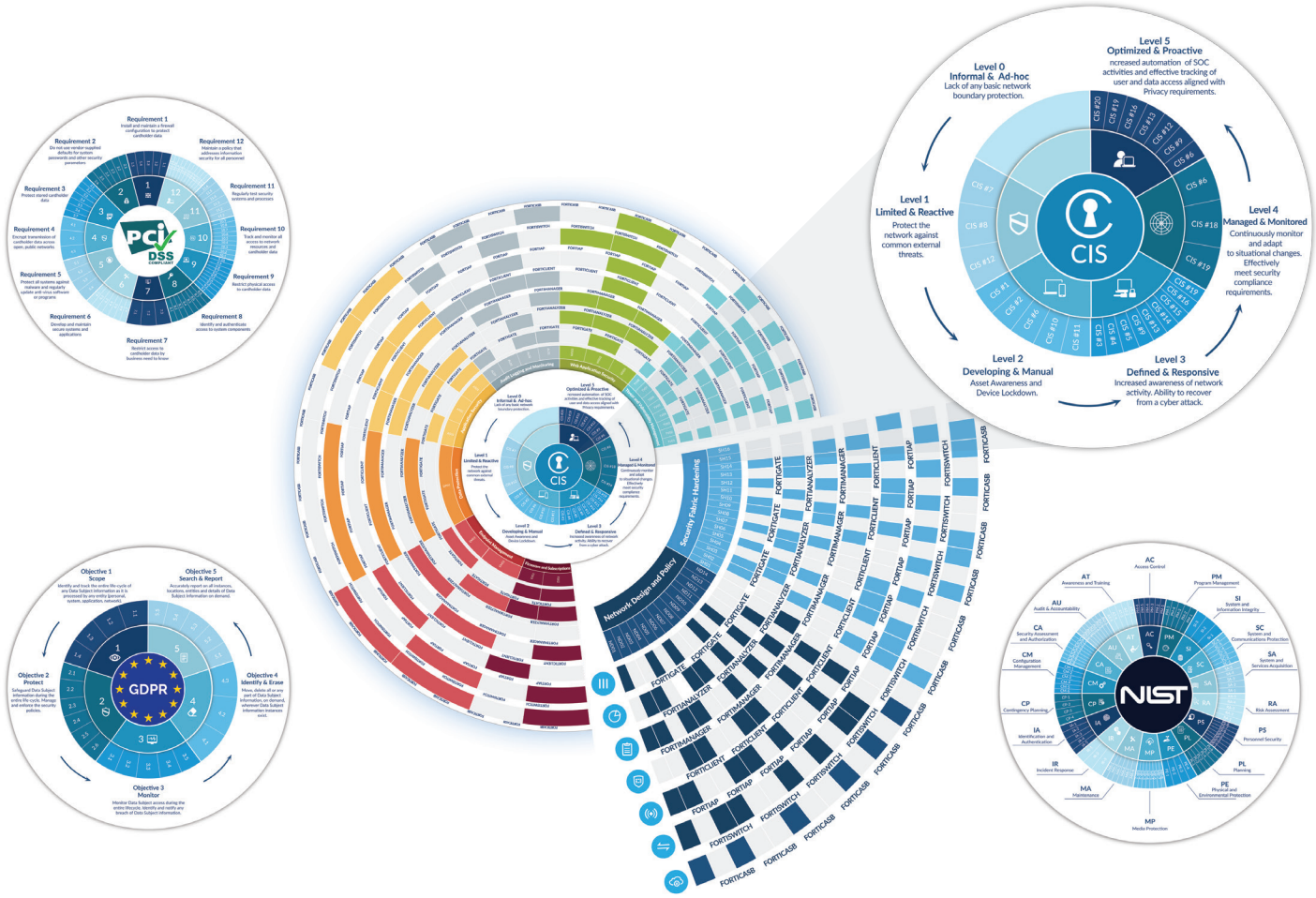

Figure 1: Fortinet Security Rating Service maturity model.

The Security Rating Service is based on a program maturity model that involves five milestones:

- Protection against common external threats
- Control over entities on the network, and device lockdown
- Heightened awareness of network activity, and ability to recover
- Continuous monitoring, ability to adapt to changes, and effective compliance
- Increased security operations center (SOC) automation and user tracking

Answering the Three Security Oversight Questions

The Fortinet Security Rating Service equips organizations to answer the three aforementioned questions of security oversight:

1. Is my network security set up properly?

The Fortinet Security Rating Service includes a self-assessment that helps organizations catch configuration problems before they result in a security incident. It provides network operations center (NOC) and security operations center (SOC) teams with an ongoing technical view of configuration issues and vulnerabilities across the Fortinet Security Fabric infrastructure—on a single pane of glass. It also facilitates NOC-SOC collaboration and communication as both teams are able to access the same configuration recommendations.[18]

Board of directors' interest in cybersecurity issues increased 23% from 2017 to 2018.[17]

The cybersecurity skills shortage makes it more difficult for security teams to remediate vulnerabilities proactively.

The assessment provides measurable and meaningful feedback on configurations based on key performance and risk indicators, helping organizations stay on track to achieve their target security maturity level. It also provides actionable information that helps NOC and SOC teams prioritize which configuration updates are the most urgent to complete, based on the needs of the business.

2. How can I show the organization that we are secure?

The dashboard in the Security Rating Service provides a single view of the organization's overall security posture, compared with peer organizations and accepted security standards. It highlights the effectiveness of security investments over time and helps CISOs to understand the logical next steps in the development of their security architecture. It also provides an easy way to keep executive management and the board of directors informed about high-level trends in a consumable format.

3. How can I demonstrate compliance to my auditors?

In addition to the above, the Security Rating Service helps organizations comply—and document compliance—with accepted standards. It continually analyzes and reports changes to network topology, simplifies identification and remediation of high-risk and noncompliant devices, and provides action plans and progress reports for both technical- and management-level stakeholders. It also enables organizations to provide auditors with proof that they are meeting Center for Internet Security (CIS) standards. And as additional security frameworks and standards are added to the Security Rating Service, compliance tracking and reporting for those will be possible.

The Fortinet Security Rating Service helps organizations optimize their security posture with objective, actionable insights based on accepted standards and comparisons with peer organizations. It helps security teams answer some of their most important operational questions:

1. Is my network security set up properly?

- Are configurations optimized according to my organization's specific needs and targeted at my industry's most common threats?
- Among things that need to be changed, which are the most important to my specific business?

2. How can I show the organization that we are secure?

- What is the maturity level of our security architecture and processes?
- How does our security posture compare with other organizations in our industry?
- How does our security posture compare with accepted standards and the needs of our business?
- What are the most important next steps in the development of our security architecture?

3. How can I demonstrate compliance to my auditors?

- What are the specific compliance holes that need to be addressed immediately?
- How can I compile compliance data continually in a format that auditors will accept?
- By helping answer these questions in an automated way, the Fortinet Security Rating Service enables companies to move onto a path of meaningful and measured security transformation that is automated, proactive, predictive, and verified.

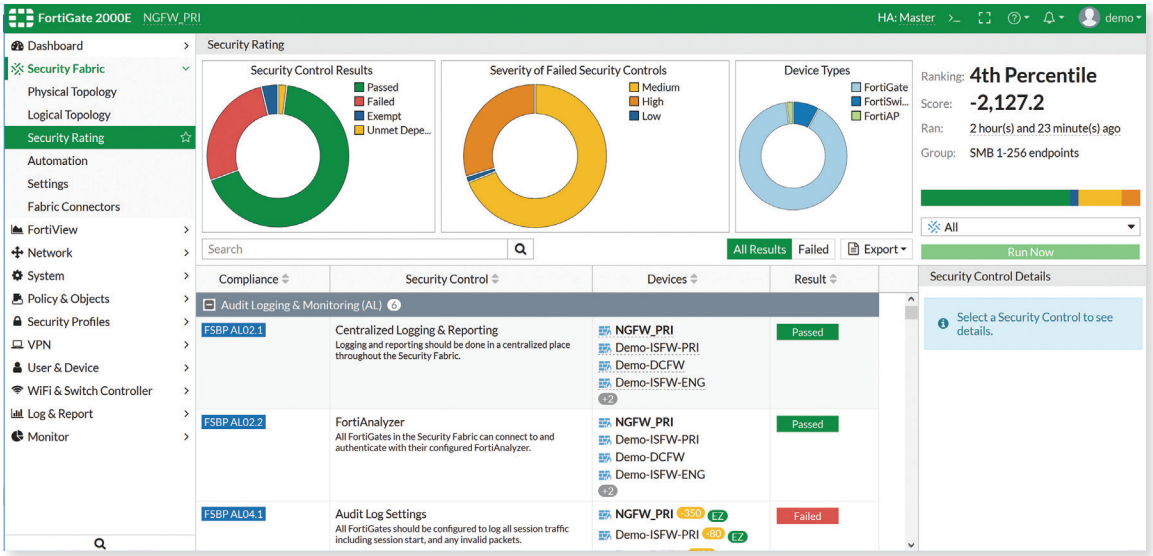

Figure 2: Security configuration self-assessment.

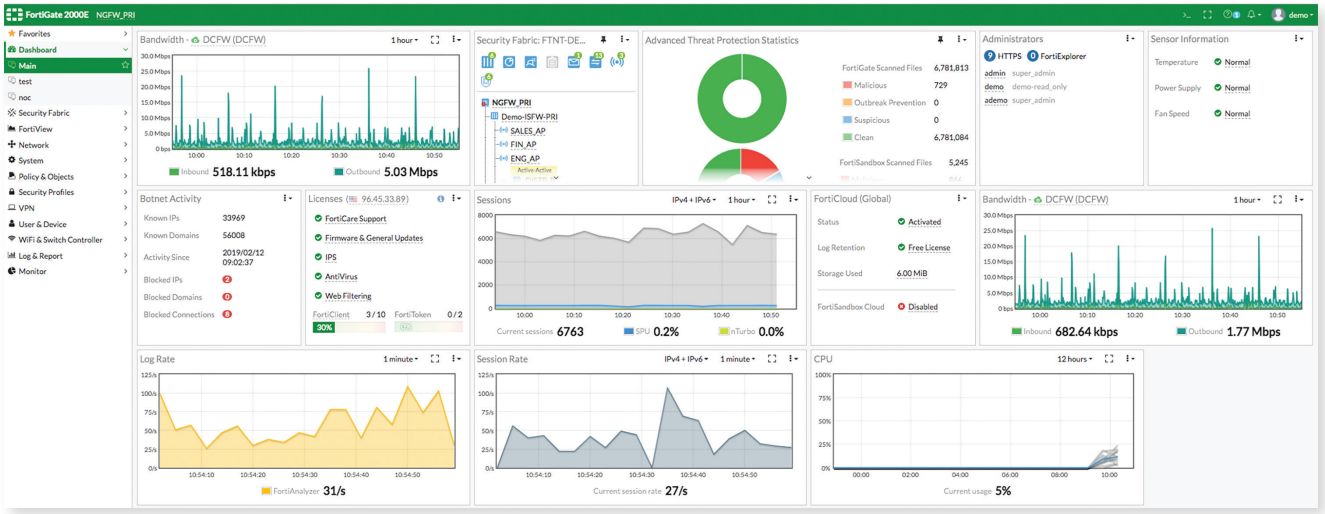

Figure 3: Security Rating Service dashboard.

[1] Khalid Kark, et al., "The new CISO: Leading the strategic security organization," Deloitte Insights, July 25, 2016.

[2] Justin Somaini, "The Evolving Role of the CISO: From Risk Manager to Business Enabler," Security Roundtable, July 31, 2018.

[3] "Edge Computing," G2 Crowd, accessed January 24, 2019.

[4] "Threat Landscape Report Q3 2017," Fortinet, accessed April 5, 2018.

[5] Andy Patrizio, "Enterprises are moving SD-WAN beyond pilot stages to deployment," Network World, May 7, 2018.

[6] "IT and OT convergence—two worlds converging in Industrial IoT," i-SCOOP, accessed January 10, 2019.

[7] "Edge Computing," G2 Crowd, accessed January 24, 2019.

[8] "Quarterly Threat Landscape Report Q3 2018," Fortinet, accessed November 13, 2018.

[9] "2018 Data Breach Investigations Report," Verizon, April 10, 2018.

[10] "2018 Cost of a Data Breach Study," Ponemon Institute, July 2018.

[11] Marty Puranik, "Data Breaches Caused by Misconfigured Servers," SC Magazine, December 26, 2018.

[12] "NACD Director's Handbook on Cyber-Risk Oversight," National Association of Corporate Directors, January 12, 2017.

[13] "Communicating with the Board about Cybersecurity—Making the Business Case," National Cybersecurity Alliance, accessed September 6, 2018.

[14] Mathew J. Schwartz, "GDPR Effect: Data Protection Complaints Spike," BankInfoSecurity, August 29, 2018.

[15] Edward Gately, "80 Percent of Companies Still Not GDPR-Compliant," Channel Partners, July 13, 2018.

[16] Kassidy Kelley, "CCPA compliance begins with data inventory assessment," TechTarget, December 26, 2018.

[17] "Board of Directors Interest in Cybersecurity Increases 23% Since 2017," Security Magazine, June 12, 2018.

[18] "Purpose-Built Integrated NOC-SOC Management and Analytics," Fortinet, September 11, 2018.

April 5, 2019 12:07 PM
D:\Fortinet\Work\April\040519\wp-security-rating-service-solution