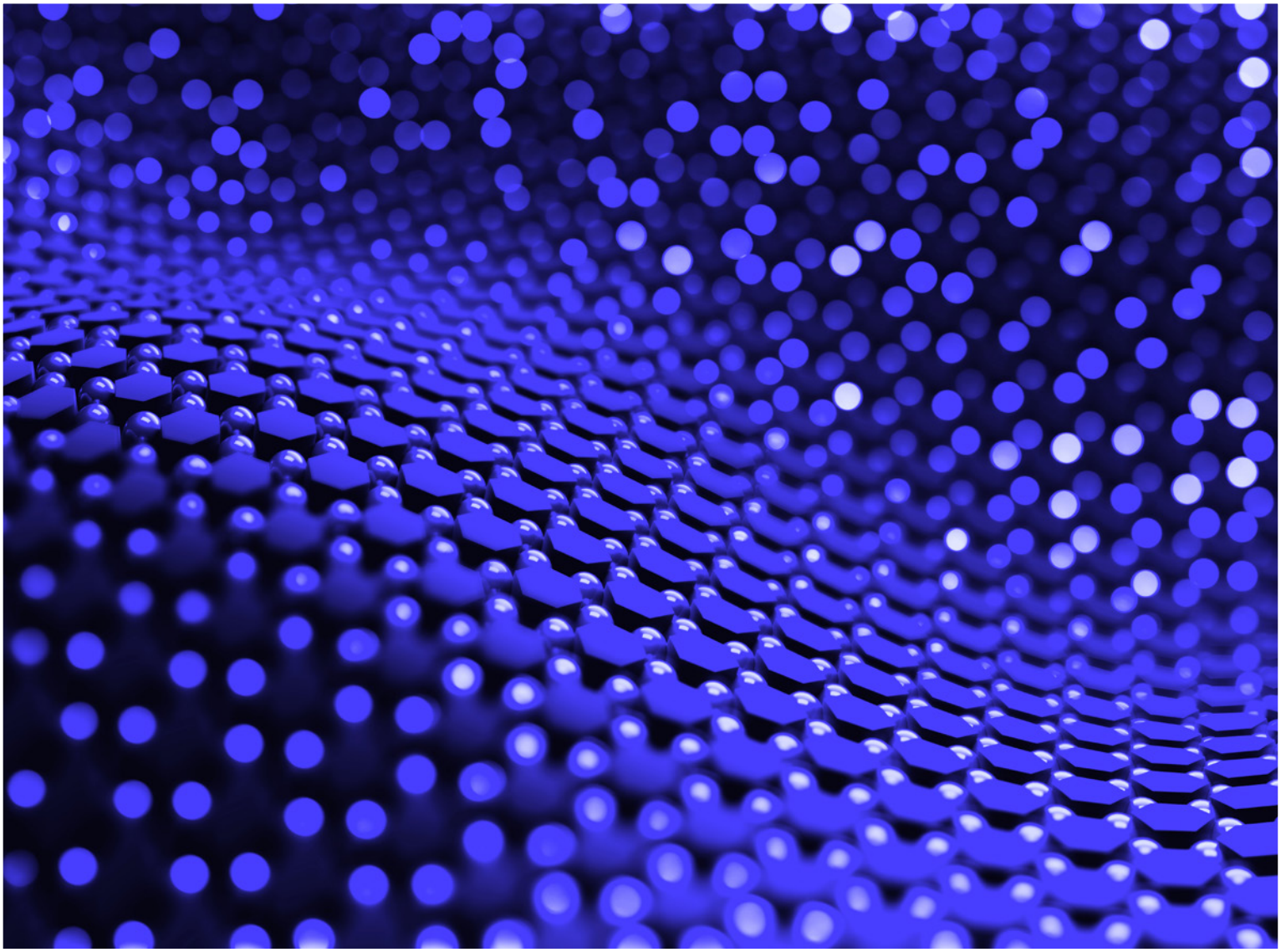
Secureworks®

WHITE PAPER

Evolving Your Security Architecture to Meet Current and Future Needs



The security posture of an organization is heavily dependent on the quality of its enterprise information security architecture.

A security architecture should be designed for the specific organization it's going to protect. This requires a solid understanding of the organization itself: its mission and goals; high-level business strategy; products and services; and sector. Having this understanding is critical to defining the organization's unique set of security needs. Defining these needs can be much more challenging than it may sound, but these challenges can be addressed by a combination of several actions, including understanding the organization's assets, implementing robust risk management practices and taking changes in the security environment into account over time.

The defined needs serve as inputs into the partial or complete redesign of the security architecture. All organizations should regularly reassess their security architecture and adjust it accordingly to handle the latest threats and take advantage of new security technologies. It is also important to ensure that the security architecture is robust and flexible, so that it can meet future needs with minimal adjustments. The keys to security architecture design and deployment include achieving security awareness and buy-in throughout the organization, acquiring intelligent next-generation security technologies, and being proactive against threats. By following these recommendations and working to constantly improve its security state, an organization should be able to significantly reduce its risk and focus on its core mission.

Defining Your Security Needs

Nearly every organization is struggling to effectively mitigate the current threats against its data and applications. There is usually a common root to this problem: deficiencies in the design, implementation and maintenance of the organization's enterprise information security architecture. Security architecture involves understanding the big picture for the organization's security needs and deciding how those needs can best be met in terms of people, processes and technologies.

Ideally, every organization should already be fully addressing its current security needs and proactively adjusting its security architecture to take into account expected future needs. In reality, this is rarely the case. Most organizations don't even have a current, comprehensive list of their security needs defined. Creating such a list is the critical first step toward evolving your organization's existing security architecture to better safeguard the organization's data and applications.

Defining your organization's security needs involves several actions, most notably the following:

- **Identify your business critical assets,** including data and applications that may need to be secured.
- **Use risk management practices** to identify and quantify the risks of security weaknesses being exploited by threats.
- **Identify security compliance requirements** that the organization's data and applications are subject to.

Performing actions such as these to define your organization's security needs can pose a variety of challenges. Here are three of the most important measures that organizations should take to help overcome these challenges:

1. Understand your assets.

The whole point of security is to safeguard your organization's assets. Assets include not only infrastructure and data but also processes and people. Unfortunately, many organizations don't keep a current inventory of all of their assets, and even those that do often do not capture enough information about each asset to allow for informed decision making. Without an accurate and detailed inventory, an organization cannot effectively perform risk management functions and select, implement and configure security controls properly.

Organizations need to identify their assets, and then classify them into groups based on their value to the organization. This is critical to risk management. Examples of ways to help support asset identification and inventory maintenance include the following:

- Implement inventory management systems and/or automated asset discovery and management tools to automate computing device inventory tracking
- Use role-based access control systems to categorize people and restrict their access to data and applications
- Use data classification techniques and tools to group and label data

Estimating the value of each asset to the organization requires an understanding of the organization's mission, goals, business strategy, products and services, business sector and other major characteristics. Even two organizations with very similar assets may value those assets quite differently because those assets play different roles within each organization. This also helps to explain why the security architecture must be customized for every organization.

The whole point of security is to safeguard your company's assets. Unfortunately, most companies don't keep a current inventory of all their assets. Without an accurate and detailed inventory, an organization cannot effectively perform risk management functions and select, implement, and configure security controls properly. According to the 2018 GSISS, only 39% of Board members are very confident their company has identified its most valuable and sensitive assets.[1]

2. Implement robust risk management practices.

For the past several years, many organizations have been heavily focused on meeting security-related compliance requirements, such as the Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and Sarbanes Oxley (SOX). And while it's certainly important for an organization to comply with all applicable requirements, it's unfortunately led to a check-the-box mentality. Many organizations simply ensure that they meet each requirement, but they do not take a step back and assess overall risk. This may easily lead to weaknesses that attackers can exploit to gain unauthorized access to the organization's sensitive data.

Instead of checking boxes, an organization needs to be focused on adopting a risk management program and integrating it into the organization's security planning efforts. An important part of a risk management program is defining the organization's risk appetite – basically, how much risk the organization is willing to accept. All other risk must be mitigated through a variety of risk management strategies. By focusing on risk management, an organization can achieve a superior security posture, and typically most compliance requirements will already be taken care of, leaving only a small number of additional measures to be addressed.

3. Take changes in the security environment into account.

For example, when there is an increasing shift of organizational data and applications from traditional IT systems to cloud infrastructures it is common that organizations do not to adequately consider and quantify the changes in risks posed by these transitions.

An organization must ensure that its risk management program takes into account major changes in IT that have security implications, such as the adoption of cloud infrastructures or the migration of data and applications from one type of cloud to another (e.g., private to public). Other security environment changes – for example, emerging threats and newly identified classes of vulnerabilities – are also critically important to address. Risk management should be ongoing, and an organization

should design its risk management processes to take into account security trends and security-related IT innovations. This allows the organization to adjust its security posture accordingly, thus ensuring that sensitive data and applications continue to be safeguarded effectively.

Redesigning Your Security Architecture

After an organization's security needs have been defined, it's time to design a security architecture to meet those needs. The extent of the redesign can be dependent on many factors, of course, but it should be aligned to a standard security architecture framework and be driven largely by the difference between the current security maturity level and the desired level.

Organizations at a low level of security maturity typically do not expend significant resources on security planning, security controls, formalized security policies and processes and the necessary personnel. These organizations will most benefit from a redesign of their entire security architecture. The organization's security needs should drive its allocation of resources, rather than the available resources driving which security needs can be met.

Organizations at a mid level of maturity may be better at planning and staffing, but generally still lack an integrated, holistic security architecture and adaptive security capabilities. These organizations may benefit most from planning how to refine their security architecture to increase its efficiency and effectiveness, instead of performing a complete redesign. Even organizations with the most mature security programs must work to constantly improve security, reviewing their security architecture as the organization changes and implementing architectural adjustments as needed to cover those changes.

Regardless of your organization's security maturity level, regularly reassessing your security architecture and keeping it relevant is the only way to ensure that the organization's security needs are being met. The way an organization has to address future needs is to have a robust and flexible security architecture, such that meeting future needs will generally require relatively minor adjustments to it.

Every organization faces its own unique set of challenges in redesigning its security architecture, but certain challenges are common to nearly every organization. Here are three recommendations that should help to address them:

1. Achieve security awareness and buy-in throughout the organization.

Although organizations have increased security awareness efforts, they are usually not effective enough. At lower levels of an organization, the lack of buy-in to security policies and practices negatively affects use and implementation of security controls (for example, users being socially engineered, or users circumventing security controls). At higher levels, the lack of buy-in to the security program negatively affects funding and resource allocations.

Organizations need robust security awareness programs that cover the entire organization, from the board and C-level to the users. Buy-in goes hand-in-hand with security awareness. It's not enough to make people aware of their roles and responsibilities; people need to understand the risks that the organization faces and how their cooperation with security policies and practices can have a positive effect on the organization and their coworkers. They need to understand not only the "how" and "when" but also the "why."

2. Acquire intelligent next-generation security technologies.

Attackers' tactics, techniques and procedures are evolving much faster than defenders' technologies. Most defensive technologies are highly dependent on humans for proper functioning. Without constant human intervention – for example, monitoring alerts and rewriting security rules – most security technologies won't provide enough value to justify their expense. And most organizations can't afford to hire the necessary staff.

The best way to address this challenge is to buy more intelligent tools that can make better decisions faster than humans can. For example, next-generation security controls offer new and innovative ways to detect and stop threats. An example is purchasing security technologies that utilize threat intelligence services, so that the technologies have the latest and most comprehensive information possible on current threats.

For the past several years, many organizations have been heavily focused on meeting security-related compliance requirements, such as HIPAA, PCI, DSS, and SOX. And while it's certainly important for an organization to comply with all applicable requirements, it's unfortunately led to a check-the-box mentality. According to PwC's 2018 GSISS, 37% of organizations surveyed reported that IT security policies are not monitored for compliance.[2]

3. Be proactive against threats.

Organizations are often reluctant to be proactive against threats, such as severing connections or blocking IP addresses. This is usually caused by fear of disrupting availability because of error-prone security controls. This may be the result of using outdated security technologies, or it may be caused by a failure to adequately configure, monitor and adjust security technologies to take the unique characteristics of the organization into account. By not being proactive, more attacks will succeed and increased damage will occur.

As threats continue to escalate, proactive handling of threats becomes even more important. Organizations need to increase the sophistication, accuracy, automation and integration of their security controls so that the controls can work together to detect and stop threats more quickly. Controls need to be linked together so that one control can automatically reconfigure another to block traffic, shut down services and make other changes to prevent attacks from succeeding, thus reducing damage.

Even organizations with the most mature security programs must work to constantly improve security, reviewing their security architecture as the organization changes, and implementing architectural adjustments as needed to cover these changes.

Conclusion

Improving the security of an organization's data and applications relies on increasing the organization's security maturity level. And doing so almost always necessitates a partial or full redesign of the organization's security architecture. It has become absolutely critical for each organization to ensure that its security needs are well defined, and then to redesign the security architecture to ensure that these needs are being met.

The most important actions that organizations should be taking to improve their security posture are:

- Understand your assets – this includes infrastructure, data, processes, and people
- Implement robust risk management practices
- Take changes in the security environment into account
- Achieve security awareness and buy-in throughout the organization
- Acquire intelligent next-generation security technologies
- Be proactive against threats

Sources:

[1] PwC, 2017 US Annual Corporate Directors Survey.

[2] PwC, The Global State of Information Security® Survey 2018.

Secureworks®

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp