The CISO's Guide to the Future of Enterprise Software Security

Rimini Street®

As cybersecurity threats become more frequent and advanced, chief information security officers (CISOs) are acutely aware that their business's enterprise applications are a prime target. In a recent Voice of the CISO report, half of CISOs reported that their organization may be the target of a significant cyberattack this year.[1]

The constant risks from natural disasters and the escalating sophistication of cyber-attacks and counter measures leave security professionals scrambling to skill up, a consequence that has contributed to cybersecurity topping the list of IT skill shortages in 2022.[2] Given the growing ubiquity of composable infrastructure, the de facto nature of remote work, and the complexities of reliance on cloud-based solutions, the race to secure enterprise applications is not slowing any time soon.

Securing your enterprise applications in this complex and fast-changing cybersecurity landscape can seem daunting. Building robust security for your applications from the ground up using internal staff requires deep expertise and the use of technologies that can strain an organization's resources and budget.

Leveraging best-practice approaches, focusing modernization efforts on higher-risk or higher-value resources, and cultivating a cyber-savvy workforce are table stakes. To achieve this, many organizations turn to trusted partners to help them do the heavy lifting of monitoring, response, and technology implementation.

Best Practice Approaches to Cybersecurity

Building a strong cybersecurity stance must be guided by best practices. Both a Zero Trust approach and a cybersecurity mesh architecture approach to security are gaining adoption. The two approaches have different areas of focus and are useful for all aspects of cybersecurity, including enterprise application security. But they are also complementary so that adopting both yields excellent results.

Supply Chain Security

The advent of Log4J and its propagation via SolarWinds' update progress exposed the risks associated with digital supply chains and the need to secure them. CISO's must implement standards and policies that ensure their vendors are meeting minimum requirements. For software and applications this would mean vendors must establish and follow secured software development lifecycle (SSDLC) processes to ensure that their digital assets are tested for vulnerabilities and secured before they are released.

A Zero Trust Approach

In traditional perimeter-based security, the corporate firewall kept untrusted people outside of the corporate network and away from vital assets. Typically, users would be given blanket-level privileges, enabling them to access resources they may not need. This violates the concept of least-privileged access, where users should only be given the minimal privileges necessary to perform a task.

Depending on the privileges granted upon successful authentication, users may be able to pass-through firewalls and other security controls as they are viewed as essentially trusted entities. In this environment, if a bad actor obtained legitimate login credentials (such as through phishing and similar activities), the bad actor would be able to gain unauthorized access to vital corporate resources and data.

> **"Zero Trust is a way of thinking, not a specific technology or architecture. It's really about zero implicit trust, as that's what we want to get rid of."**
>
> *– Neil MacDonald*
> *Gartner Distinguished VP Analyst*[3]

Once inside the firewall, bad actors could take actions, such as using known vulnerabilities to compromise enterprise applications and installing back-doors, to exfiltrate sensitive data. Similarly, they could introduce viruses known to harm particular applications.

One Key Opens Only One Door

The Zero Trust approach to cybersecurity views all entities and resources as untrusted by default. This means, for example, that having valid network login credentials will allow access to a specified area of the network but using any resources or accessing any data within that part of the network requires further authorization. Having the key to the front door gets you in, but when you get inside, you find that everything inside is independently locked and inaccessible.

The Zero Trust approach limits the damage that bad actors can cause by compromising a single set of credentials or a single point into a network. It also helps mitigate the threat to enterprise applications that may not yet be patched.

A Cybersecurity Mesh Architecture Approach

Where Zero Trust focuses on issues of identity, access, and trust; a cybersecurity mesh architecture (CSMA) approach aims to create a collaborative ecosystem of security tools and solutions. These tools should be capable of working together synergistically and extending security well past traditional perimeters.

The principles of CSMA also recognize that cybersecurity is not only about technology. It is equally about processes and people. As such, the CSMA approach calls for ensuring that both security and, where applicable, business processes are aligned.

Elements of a Cybersecurity Mesh Architecture

To understand how CSMA comes together, it is helpful to break down the architecture into its constituent parts. The primary layers of a cybersecurity mesh architecture—which is distinct from, but has analogs in, both network and cloud architectures—include:

Security Analytics and Threat Intelligence

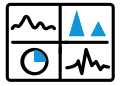
The key here is centralization and analysis of data, which requires access to that data from solutions that may create integration issues

Centralized Policy Management and Orchestration

While there are different ways of achieving orchestration, the basic precept is that every asset, hardware or software, should support and allow orchestration and avoid silos

Identity Fabric

In CSMA, the emphasis for identity is on context awareness, which coincides with a Zero Trust approach, and extends beyond people to systems and devices



Dashboards

Centralization here is again the key, with the mesh concept suggesting interconnectivity across all assets and resources to enable a comprehensive dashboard

Challenges CSMA Can Address

By 2024, organizations adopting a cybersecurity mesh architecture to integrate security tools to work as a cooperative ecosystem will reduce the financial impact of individual security incidents by an average of

90%.

– Gartner[4]

As CSMA matures, it drives benefits and capabilities that target some of the most difficult challenges security teams face today, such as:

- **Perimeter fragmentation**
  Growing numbers and kinds of mobile devices, remote workers, and cloud-based applications all combine to make the traditional security perimeter obsolete.
- **Security silos**
  Specialized security tools perform and report on specific tasks effectively in isolation, and teams who manage those tools often have no automated means of coordinating the activities and sharing data with other tools.
- **Inadequate integration**
  When choosing from among best-of-breed security solutions, it quickly becomes apparent that interoperability is not often a best-of-breed criterion.
- **Security team burnout**
  Cybersecurity is a twenty-four hour a day job. The consequences of breaches can be severe. Because security technology evolves rapidly, security professionals need to stay in a state of high-stakes perpetual learning. As such, professionals often find themselves burned out between staying ahead of technology and dealing with the consequences of 3:00 a.m. system alerts.
- **Coordinated response**
  Cybersecurity teams must be able to detect and respond to events and information that indicate corporate assets may be at risk. These could be related to natural events, like earthquakes or human-made events, like terrorism and cyber-attacks. CSMA utilizes automation, analytics, and artificial intelligence to monitor networks and resources. While rapidly identifying threats and enacting counter measures such as alerting cyber teams and invoking playbooks to minimize impact.
- **Inefficient Security Operations**
  The breath of CSMA compels security organizations, especially operational organizations to function at peak efficiencies. This is necessary to minimize the impact from disastrous and hostile intruders and to maintain business continuity. To stay ahead, security operations teams need innovative cybersecurity processes and tools such as a SIEM (Security Information Event Management), analysis, and related infrastructure. The teams managing these tools and processes must be highly trained for CSMA to be successful.
- **Elevated Risk**
  Because of the overall improvements achieved through CSMA, corporate security postures will increase, there-by reducing overall risk. Businesses that fully implement a CSMA framework will be less susceptible to vulnerabilities and exploits.

Reducing Technical Debt through Modernizing Security

Hardware and applications in use beyond its expected end-of-life can create an attack vector that modern machinery has closed. This is because dated hardware and applications may not be capable of supporting modern security approaches and technologies. Sensitive or important corporate data and databases hosted on legacy resources can be subject to attacks such as backdoors leveraging lowest hanging fruit exploits.

However, upgrading dated hardware and applications can be expensive and disruptive. The first step is to determine if your legacy resources are creating risk and assessing the degree of that risk. This is a matter of auditing equipment and applications using procedures such as penetration testing and vulnerability scanning to identify security holes that need to be closed.

Hardening and securing databases helps reduce the attack surface no matter where data resides. There are widely used hardening guides such as those offered by the Department of Defense.[5] These documents provide guidance for hardening databases from specific vendors such as Oracle, as well as more general guidance in the form of minimal acceptable baseline configurations applicable to many databases (e.g., DB2, MS SQL Server, etc.).

Cultivating Digital Citizens

In earlier discussions of CSMA, we noted that people are a critical component of cybersecurity. Human error is the source of most breaches. These errors take several forms. A common error is credential misuse, such as not periodically changing passwords, using the same password in multiple places, creating passwords that are not sufficiently complex, and sharing passwords.

Another common error arises from within IT. Networks, applications, devices, firewalls, and other forms of technology are subject to misconfiguration. This can result in vulnerabilities that would not ordinarily exist and once exploited, could have catastrophic consequences. This is especially true in multi-tenant, cloud environments.

Addressing the human element in cybersecurity begins with education. Plan activities outside of annual compliance training. Educating employees across the organization using methods such as phishing tests, provides baseline data for measuring the effectiveness of the training and keeps employees on their toes. You can also keep cybersecurity top of mind throughout the year by drawing attention to high profile breaches in the news.

82%

of breaches involved the human element, whether it is the use of stolen credentials, misuse of credentials, phishing, or simply human error, in 2021.

– Verizon[5]

Talent Strategy

As noted earlier, cybersecurity skills are a top IT hiring need. When it comes to staffing your internal security team, develop a multi-prong strategy that addresses your needs today and helps you grow into the skills you'll need in the future.

Once you understand the skills that you need, develop existing talent through retraining and reskilling. Also, consider building partnerships with schools to get the best new talent. If you're unable to recruit the skills that you need by recruiting or retraining, seek out a trusted managed security service providers (MSSPs) able to not only provide the security expertise that you need, but also able to help you evolve your security strategy over time.

An MSSP can offer services that support an enhanced client security strategy and will help companies of all sizes achieve protection in a cost-effective manner. Use a trusted MSSP to acquire the cybersecurity talent that you need and to provide innovative, powerful cybersecurity tools to help you evolve as cybersecurity and threat tactics evolve.

"By using more modern security approaches we found we would be able to better protect our systems using Rimini Street Advanced Security Solutions. Taking this approach has enabled us to redirect our resources to focus on higher-value work for the university."

— Scott Lawry
Associate Director, Solution Design and Delivery, Queensland University of Technology

Endnotes

1 Proofpoint. "2022 Voice of the CISO," May 05, 2022
2 CXOtoday.com. "Most In-Demand Tech Skills for 2022 and Beyond," January 09, 2022, Sohini Bagchi
3 Verizon. "2022 Data Breach Investigations Report," June 03, 2022
4 Gartner, Inc. "New to Zero Trust Security? Start Here," June 02, 2021, Susan Moore
5 U.S. Department of Defense. "Security Technical Implementation Guides (STIGs)"

Conclusion

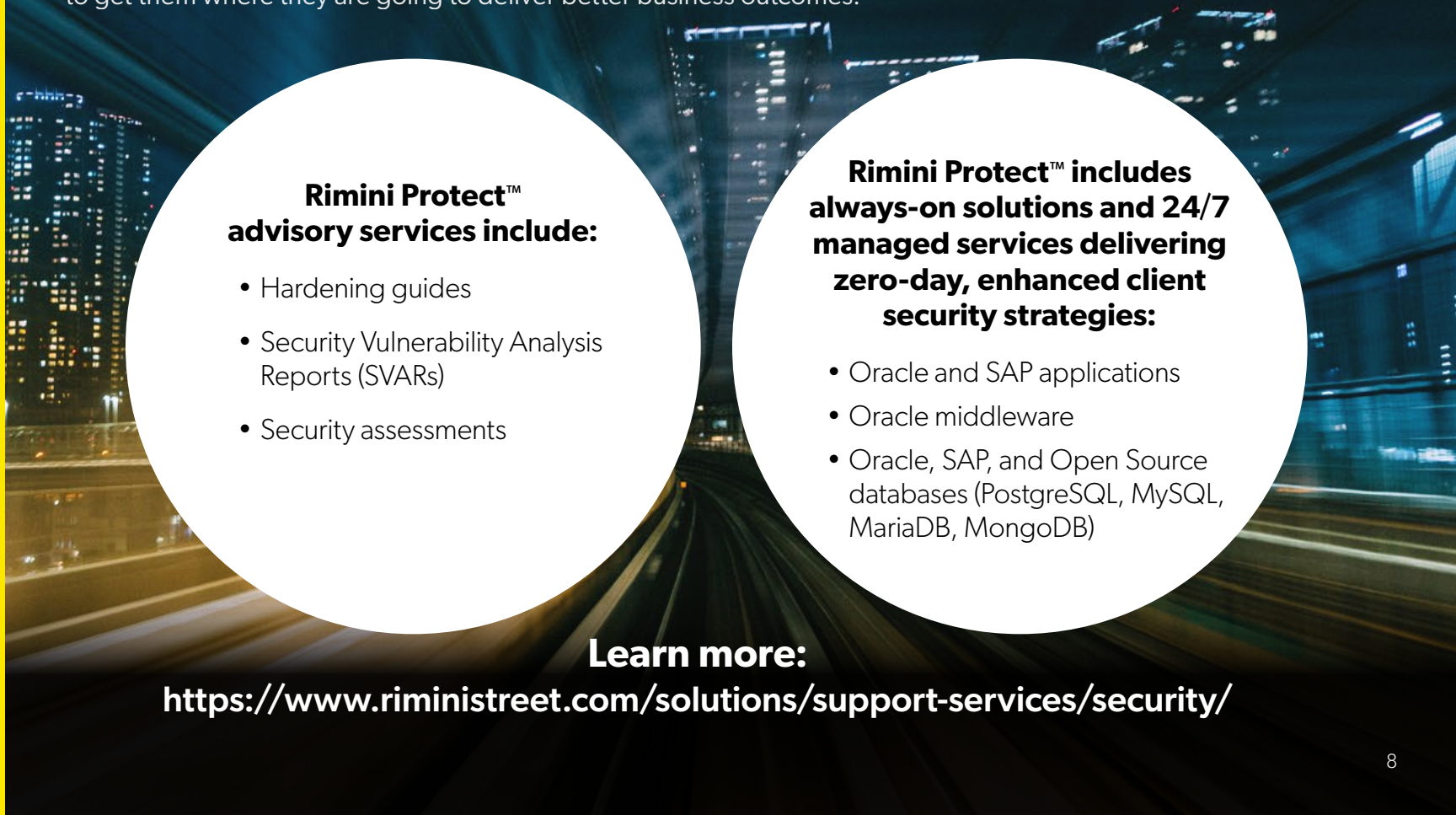
Enterprise applications are a prime target for bad actors, and about half of CISOs anticipate a near-term cyberattack. Forward-looking CISOs are moving to build enhanced client security strategies that protect against known and unknown vulnerabilities. Enhanced security models help teams provide zero-day protection to reduce the chance of costly breaches and bad press due to attacks.

Rimini Street®

Take the Smart Path to Application Security with Rimini Protect™

Rimini Protect™ is a family of security products and services that provide proactive, fast and cost-effective security protection, personalized to an organization's unique enterprise software environment and landscape.

Rimini Protect™ helps our clients take the smart path with their technology portfolio and provides the expertise to get them where they are going to deliver better business outcomes.



Rimini Protect™ advisory services include:

- Hardening guides
- Security Vulnerability Analysis Reports (SVARs)
- Security assessments

Rimini Protect™ includes always-on solutions and 24/7 managed services delivering zero-day, enhanced client security strategies:

- Oracle and SAP applications
- Oracle middleware
- Oracle, SAP, and Open Source databases (PostgreSQL, MySQL, MariaDB, MongoDB)

Learn more:
https://www.riministreet.com/solutions/support-services/security/

Rimini Street®

riministreet.com
info@riministreet.com
twitter.com/riministreet
linkedin.com/company/rimini-street

About Rimini Street

Rimini Street, Inc. (Nasdaq: RMNI) is a global provider of enterprise software products and services, the leading third-party support provider for Oracle and SAP software products and a Salesforce® partner. The company offers premium, ultra-responsive and integrated application management and support services that enable enterprise software licensees to save significant costs, free up resources for innovation and achieve better business outcomes. Global Fortune 500, midmarket, public sector and other organizations from a broad range of industries rely on Rimini Street as their trusted enterprise software products and services provider.

© 2023 Rimini Street, Inc. All rights reserved. "Rimini Street" is a registered trademark of Rimini Street, Inc. in the United States and other countries, and Rimini Street, the Rimini Street logo, and combinations thereof, and other marks marked by TM are trademarks of Rimini Street, Inc. All other trademarks remain the property of their respective owners, and unless otherwise specified, Rimini Street claims no affiliation, endorsement, or association with any such trademark holder or other. This document was created by Rimini Street, Inc. ("Rimini Street") and is not sponsored by, endorsed by, or affiliated with Oracle Corporation, SAP SE or any other party. Except as otherwise expressly provided in writing, Rimini Street assumes no liability whatsoever and disclaims any express, implied or statutory warranty relating to the information presented, including, without limitation, any implied warranty of merchantability or fitness for a particular purpose. Rimini Street shall not be liable for any direct, indirect, consequential, punitive, special, or incidental damages arising out of the use or inability to use the information. Rimini Street makes no representations or warranties with respect to the accuracy or completeness of the information provided by third parties, and reserves the right to make changes to the information, services or products, at any time. M_1920 | LR0022669 [346] | US-110923