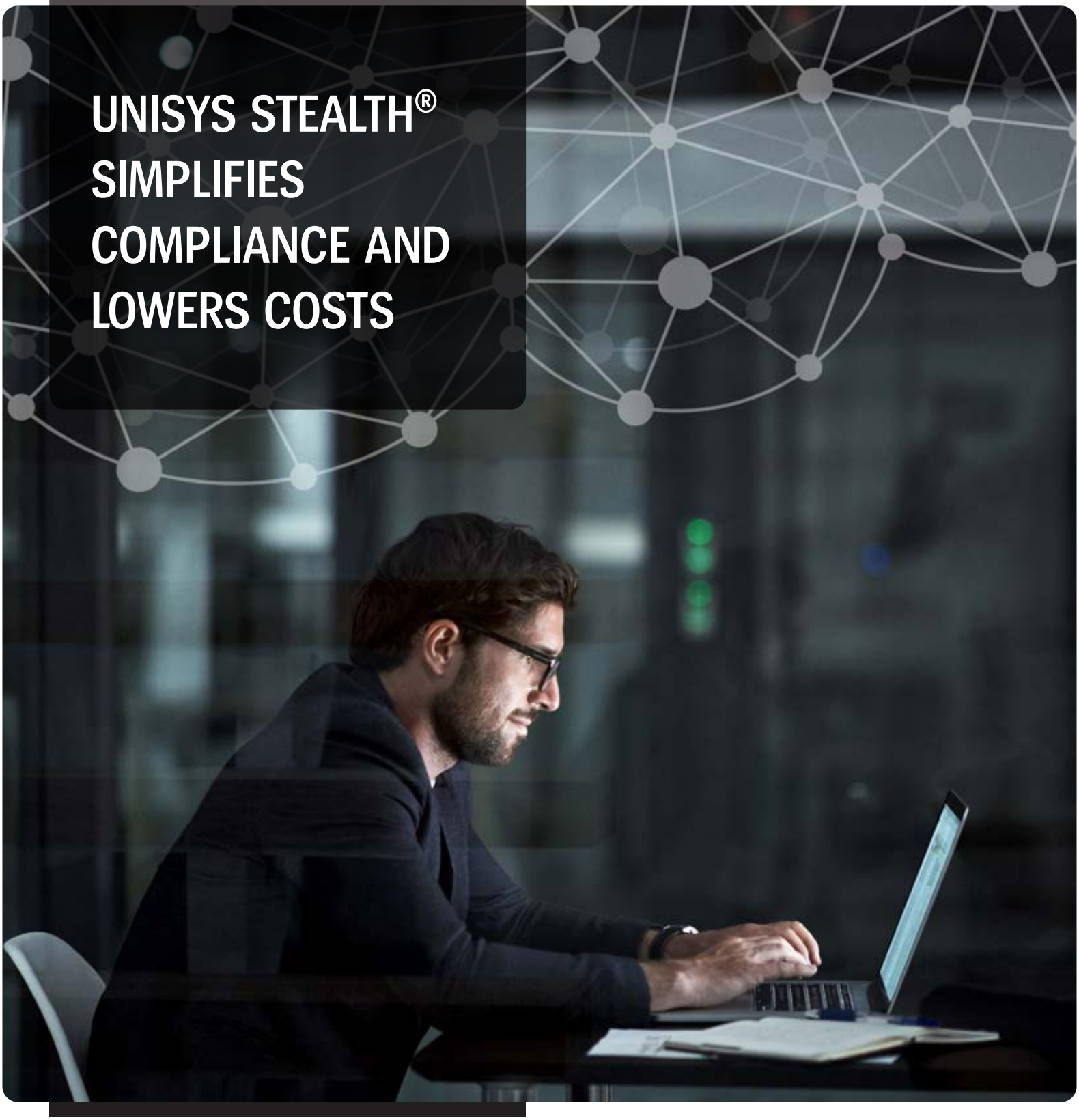
UNISYS STEALTH® SIMPLIFIES COMPLIANCE AND LOWERS COSTS



STEALTH™

Regulatory compliance is a constant challenge for your organization, even in more tranquil times. In a post-pandemic world – where you have had to reinvent how you operate virtually overnight – meeting or exceeding the cybersecurity and data privacy controls mandated for specific types of data or to do business in regulated industries may seem impossible.

Unfortunately, the business and regulatory disruption caused by COVID-19 probably won't abate anytime soon. Far more likely, you are witnessing the beginning of a new era in which compliance challenges are ever-changing and increasingly complex. This is the new normal for organizations and entire industries – healthcare, financial services, education, pharmaceuticals, retail, manufacturing, and more. To successfully navigate this new compliance landscape, you must be able to recognize and rapidly respond to new risks.

Data protection and compliance present daily challenges. Despite good intentions, more than half of companies still struggle to design, implement and maintain a sustainable compliance program.

– Verizon 2019 Payment Security Report.[i]

Compliance Is Complicated

Anyone who must work with myriad and byzantine regulations will tell you that compliance is complicated. And while *attaining* compliance is hard, *maintaining* compliance is even more difficult. According to Verizon's 2019 Payment Security Report, when Visa launched the PCI DSS standards in 2004, industry watchers expected most organizations to achieve full compliance within five years. The experts were wildly optimistic: Verizon found that 14 years later (in 2018), only 37% of organizations "were actively maintaining PCI DSS programs." That was down from a high of 55% in 2016, and was the lowest full compliance rate since 2013.

There are several reasons for this downward compliance trend, Verizon concludes. Some organizations implement "inadequate or overly complex" data compliance programs that fail to hold up under real-world conditions. Others may lack "the review processes and revisions" necessary for compliance initiatives to be both effective and sustainable.

"Data protection should be approached like a chess game, with a sound strategy that includes assessing risks and planning several steps ahead," Verizon writes. "All too often, CISOs focus on keeping only baseline control activities in place instead of growing data protection competency and maturity."

Given all the complex regulations governing business today, it's no wonder that companies struggle to understand and meet their legal and ethical obligations.

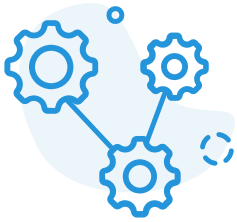
– Harvard Business Review.[ii]

That's a losing strategy in an environment where change (and thus risk) is constant, and where bad actors are relentlessly iterating new techniques to defeat old and ineffective defenses. Indeed, threats evolve more rapidly now than governing agencies and organizations can respond. Hundreds of thousands of new malware signatures are unleashed daily, while the lag time between detection of vulnerabilities and patches released and applied widens. Further, cyberattacks continue to become more sophisticated, even as managing a secure and compliant enterprise infrastructure becomes more complex.[iii]

Compliance Fatigue

Then there is human nature. People are bad at maintaining complex systems over time if there is no reward for doing so. In the case of a successful compliance program, the reward is a bit of letdown because, done right, nothing happens. The bad guys don't get in, data is not breached, and the network is not compromised. As nothing happens year after year, complacency (clearly we're doing this right!) can creep in, especially when higher-priority projects distract managers and divert resources.

Complex solutions to complex regulations also can lead to compliance fatigue where the constant upkeep and sheer number and intricacy of regulations outstrip your organization's ability to keep pace. Yet another risk is compliance "overlap," in which one set of regulations either complements or conflicts with a different set, resulting in confusion that makes simultaneously meeting the requirements of multiple frameworks a struggle even for the most dedicated compliance regimes. These problems are compounded by the often mundane and manual nature of collecting and analyzing data to stay within regulations and demonstrate that compliance is taking place.



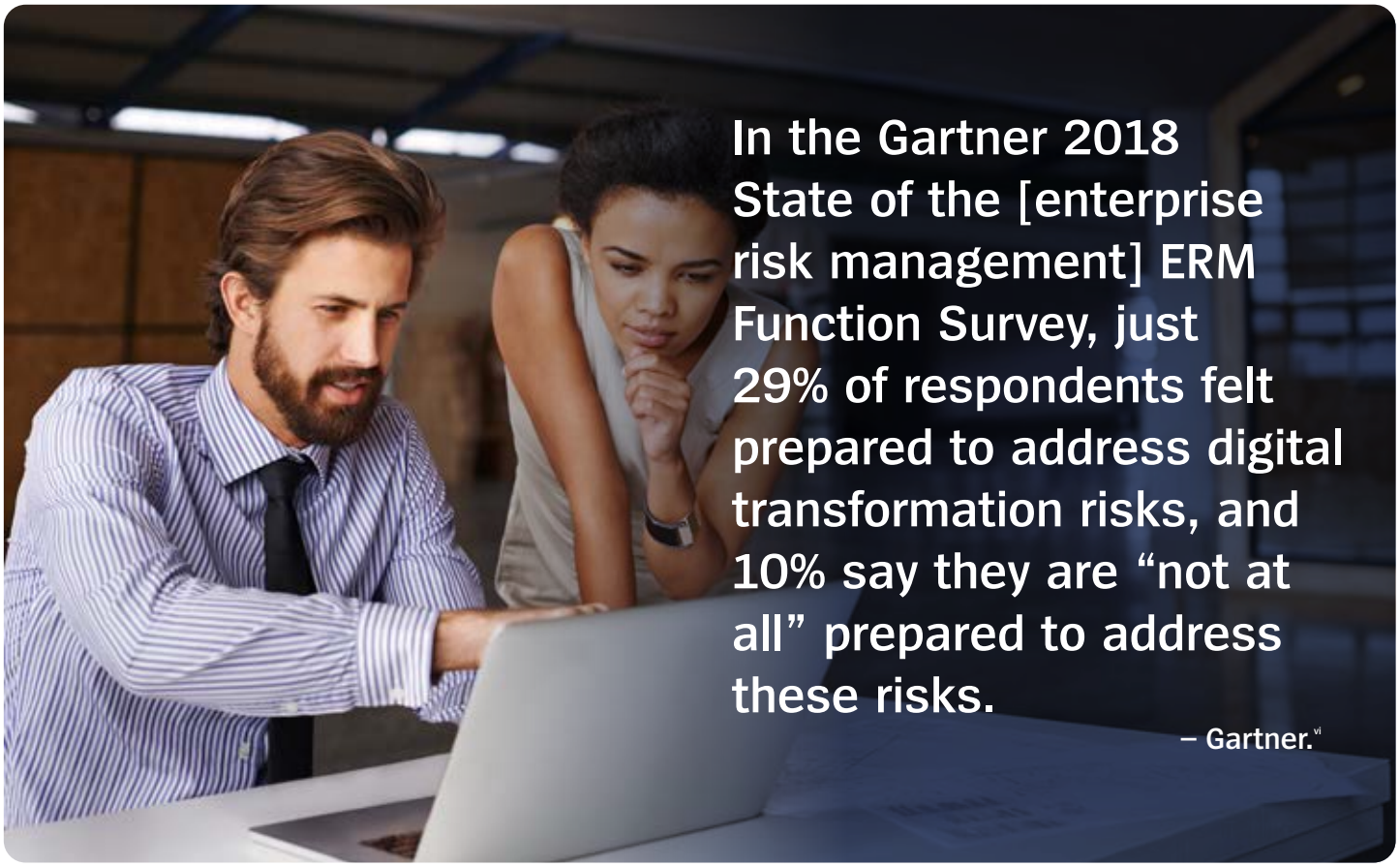
The manual nature of the current approach to compliance is in itself creating risk, and there are not enough people with the skills to manage the processes sustainably.

– Marion Leslie, managing director, Thomson Reuters Enterprise.[iv]

By lacking a holistic view of compliance activities, you run the risk of duplicating your efforts. The "status quo approach to compliance does not allow for an integrated view across the enterprise," McKinsey & Co. writes. "The approach to risk assessment is fragmented: some risks are covered by multiple assessments and others not at all."[v]

The post-pandemic world has forced your organization to dramatically accelerate digital transformation initiatives to support remote workers and engage with customers, partners, vendors, and suppliers. In doing so, you have expanded the attack surface of your networks, applications, data centers, and data. Each new technology, platform, remote connection, or opening-up of back-end systems to outsiders and the Internet introduces more complexity and potential vulnerabilities.

To keep up, you can add more VLANs, access control lists (ACLs), subnets, and firewalls to secure this growing cyber footprint. But this additional connectivity expands the number of domains that must be audited. And that increases audit complexity, time, and cost.



Add in the ever-growing number and variety of edge devices and cloud deployments auditors will explore, and you face a multilayered, multifaceted compliance nightmare. What your organization needs is a simpler, more cost-effective way to meet the demands of multiple regulations using a single technology that is time-tested, highly secure, and simple to deploy and manage at scale.

To achieve this simplified and more secure end-state, many organizations today are relying on Zero Trust architectures that assume all endpoints accessing your network—be it a user, application, or device—are compromised. To ensure application integrity, Zero Trust limits access to just the applications and data needed to carry out a specific set of functions or for a user to do their job. This is where Unisys Stealth® comes in.

Unisys Stealth Zero Trust Compliance Solution

Unisys Stealth is software-defined security. It simplifies yet improves network security and serves as the backbone of your whole-network Zero Trust strategy. Stealth™ provides a fast, simple way to wrap a protective shell around all your systems, no matter where they are. It can respond to any breach in 10 seconds or less via dynamic isolation.

Stealth makes improving data privacy easy, right out of the box and with almost zero impact on operations. Stealth blankets every corner of your organization's computing environment with one holistic, consistent, and unwavering security policy—from mobile phones and desktops, to servers, to cloud, and even IoT. In fact, Stealth orchestration and deployment are highly automated and centrally managed. And where other solutions fail to scale, Unisys Stealth expands globally with ease.

The successful deployment of technology and the ability to automate future compliance activities is one of the greatest potential innovations for the next 10 years.

– Thomson Reuters Regulatory Intelligence Cost of Compliance Survey 2019.[vii]

As your security policies evolve, changes can be made and instantly propagated across the enterprise. Meanwhile, Stealth monitors and enforces all your Zero Trust policies, automatically isolating violators and alerting administrators. With Stealth Zero Trust, compliance is seamlessly woven into the fabric of your entire network. It's the engine that drives your speed to security.

Stealth delivers Zero Trust through micro-segmentation, compartmentalization, and the creation of communities of interest (CoIs). These secure enclaves rely on hyper-secure IPsec tunnels between CoI end points that encrypt data from end-to-end. Outsiders cannot gain access into the CoI, and data cannot be exfiltrated out.

Thanks to Stealth's patented SCIP "cloaking" protocol, applications and servers within the CoI will not respond to pings, scans, or other means of network reconnaissance, thus offering attackers no glimpses into network topology and application dependencies. All elements within the CoI are invisible to outsiders. Best of all, Stealth scales quickly, easily and works on any existing TCP/IP network—on-prem, in the cloud, or integrated into a partner's network.

Because data is isolated in highly secure, cloistered enclaves, with access limited to only the users and applications that must have it, Stealth gives auditors the ability to narrowly focus on just the users, applications, and devices that have access to sensitive data. This reduces the number of people and endpoints interacting with the data, shrinking both the attack surface and the number of places auditors have to check for compliance. This makes your audits less complex, cutting down on the time it takes to certify compliance and lowering costs. In addition, Stealth activity logs give auditors a clear path to follow while confirming network protection guidelines in certain frameworks.

A valuable compliance tool is Stealth Reporting Service, which provides enterprise-class features for robust reporting and logging to increase operational effectiveness. You can obtain pre-defined standard reports such as Tunnels Blocked Report, Authorization Report, License Usage Report, and Isolated Users/Devices Report. In addition, the tool's custom reporting capability allows report generation with custom type and number of fields for focused data analysis and selective data reporting. You can pre-create and save custom report templates for quick data access. Its Log Viewer offers flexible data search and analysis support, and it also supports report templates that provide quick data access.

During the Target breach of 2014, for example, an HVAC vendor was granted wide-ranging network access to manage HVAC systems at certain stores. Hackers infiltrated this provider, island-hopped over to Target's network, and used the vendor's unrestricted network access to penetrate the point-of-sale system, stealing millions of credit card numbers. With Stealth this never would have happened. The vendor's access would have been limited to just the HVAC systems they were responsible for. The rest of the network would have been completely inaccessible and unresponsive.

As an added bonus, knowledge of partner compliance controls is completely unnecessary since Stealth cryptographically isolates their users and applications right alongside your own, giving you a secure, encrypted connection between you and your partner's authorized users.

The potential for technology to help modernize compliance is significant, although many organizations still are at the foundational level, just beginning to evaluate processes and plan improvements."

– Mike Juergens, a principal at Deloitte Risk and Financial Advisory.[ix]

The Benefits of Using Stealth in Compliance

By deploying Stealth, you get both speed-to-compliance and speed-to-audit—all with your existing infrastructure and applications. There is no need to rip and replace anything. By relying on secure, encrypted IPsec tunnels to establish CoI based on least-privilege access to networks, applications, and data, you can sleep well at night knowing you have deployed one of the most advanced cybersecurity platforms in the industry. Compliance is simplified and auditing is streamlined because Stealth™:

- Allows you to build a trusted and secure network on top of an existing infrastructure
- Reduces infrastructure attack surfaces while expanding network reach and access to partners, vendors, and suppliers
- Reduces the number of systems and users that are subject to audit
- Encrypts data in motion, meeting a key requirement of many compliance frameworks
- Prevents data exfiltration to non-approved systems, applications, and users—a key component of limiting data breaches and the spread of malware
- Enables adoption of Zero Trust architectures right out of the box by allowing only authorized access to your sensitive data and systems
- Integrates with enterprise directories and other access control systems via Identity Access Management (IAM) systems, enabling you to manage it day to day via these existing systems
- Delivers easily deployed role-based compliance protections for every user and endpoint on your network
- Provides an easy to use, manage, and orchestrate via a single pane of glass control console and PowerShell cmdlets as well as Unisys' extensive APIs (e.g., EcoAPI andRESTful API)
- Is designed for use by cybersecurity professionals and admins
- Isolates data, systems, and users– leveraging identity rather than complex firewall rules based on IP address, ports and protocols

In Summary

Unisys Stealth provides you with flexible, extensible security for public, private, hybrid, and multi-cloud all within one software-defined security fabric. Policies and role-based protections are propagated from one central console or fully integrated with existing identity and access management systems, eliminating complex management and the need for multiple security point solutions. Real-time proactive isolation of malicious devices and operations when threats are detected ensures you protection from both internal and external threats. In short, Stealth reduces the costs and complexity of compliance, improves security, and streamlines management of your entire environment.

The way the world works has changed, and it is certain to change again – and again. Unisys Stealth is more capable than any other security solution of helping you protect data privacy and ensure compliance now and in the future.

i. Version. “2019 Security Payment Report.” enterprise.verizon.com/resources/reports/payment-security/

ii. Chen and Solte. “Why Compliance Programs Fail.” Harvard Business Report. March-April 2018. hbr.org/2018/03/why-compliance-programs-fail

iii. Das. “When Every Attack is Zero Day.” April 23, 2019. www.darkreading.com/vulnerabilities—threats/when-every-attack-is-a-zero-day/a/d-id/1334468

iv. Thompson Reuters. “Transformation: The Automation of Compliance and Regulation.” December 5, 2016. blogs.thomsonreuters.com/answerson/automation-regulation-compliance/

v. Kiminsky, et al. “Sustainable Compliance.” February 2017. www.mckinsey.com/business-functions/risk/our-insights/sustainable-compliance-seven-steps-toward-effectiveness-and-efficiency

vi. Meulen. “Prepare for These 4 Business Risks.” Gartner. May 7, 2019. www.gartner.com/smarterwithgartner/prepare-for-these-4-emerging-business-risks/

vii. Hammond. “The Cost of Compliance Survey 2019.” Thompson-Reuters. June 27, 2019. blogs.thomsonreuters.com/answerson/cost-of-compliance-survey-2019/

viii. Vijayan. “Target breach happened because of a basic network segmentation error.” Computerworld. February 6, 2014. www.computerworld.com/article/2487425/target-breach-happened-because-of-a-basic-network-segmentation-error.html

ix. Jeurgens. “Technology: A Powerful Tool to Help Modernize Compliance.” The Wall Street Journal. deloitte.wsj.com/riskandcompliance/2018/12/02/technology-a-powerful-tool-to-help-modernize-compliance/

For more information or to request a demo,
contact us at www.stealthsecurity.unisys.com/contact-us/

For more information visit www.unisys.com

12/20 20-0604