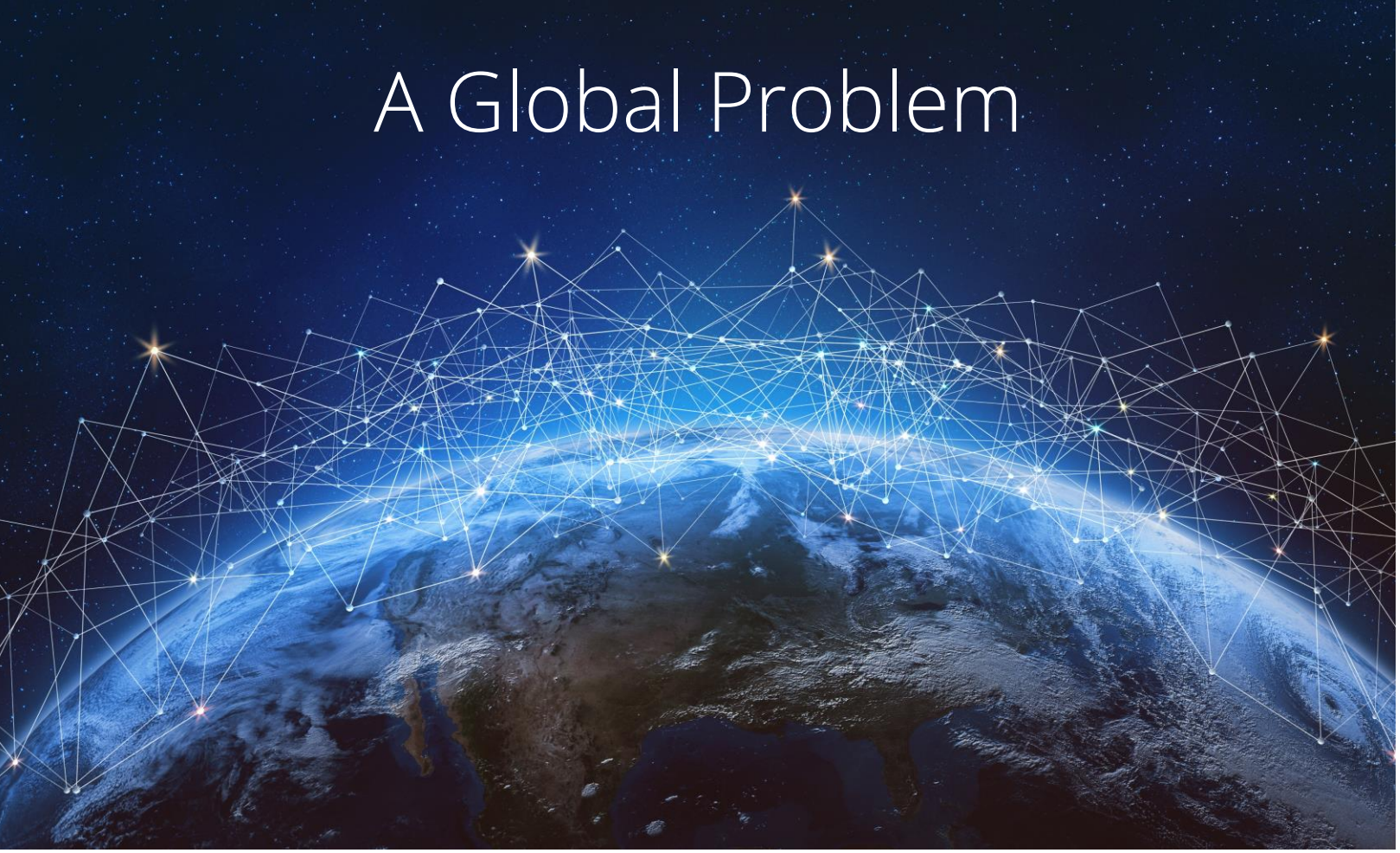

ISIGN
INTERNATIONAL
DIGITAL SECURITY SUITE
www.isignintl.com

A Global Problem



There are millions of servers today that are not properly protected and are vulnerable to RDP/SSH attacks. Once a hacker has connections to servers via RDP/SSH, they will cause havoc to a company as seen through multiple corporate data breaches.

User accounts are constantly under attack through weak passwords and phishing attempts. Once a hacker gets a hold of the account, they begin to wreak havoc by impersonating the user to steal money and other valuable digital assets. Everyday, the general public is losing millions of dollars through inadequate account protection.

Data Breaches

Data breaches are caused through inadequate server protection and/or using VPN that leaves data ports open to hackers.

Global Access

Hackers have access to cloud servers throughout the world and they can easily find your servers through IP Address and Port Scanning.

The Cost of a Breach

In recent years, hackers have broken through corporate servers and exposed hundreds of millions of accounts, costing companies tens of millions of dollars to protect their users through credit monitoring services. Even the credit agencies have been hacked.

Unsecured IOT Devices

A Hacking Nightmare

Devices are built without security in mind. They were pushed to market to gain wide adoption and security was overlooked.

If devices can be access remotely, hackers have full access to those devices.

The cost of a hack of a consumer device leads to privacy concerns, just like the Nest Camera that was recently hacked by a hacker who decided it was a good idea to talk to a toddler on the other end.

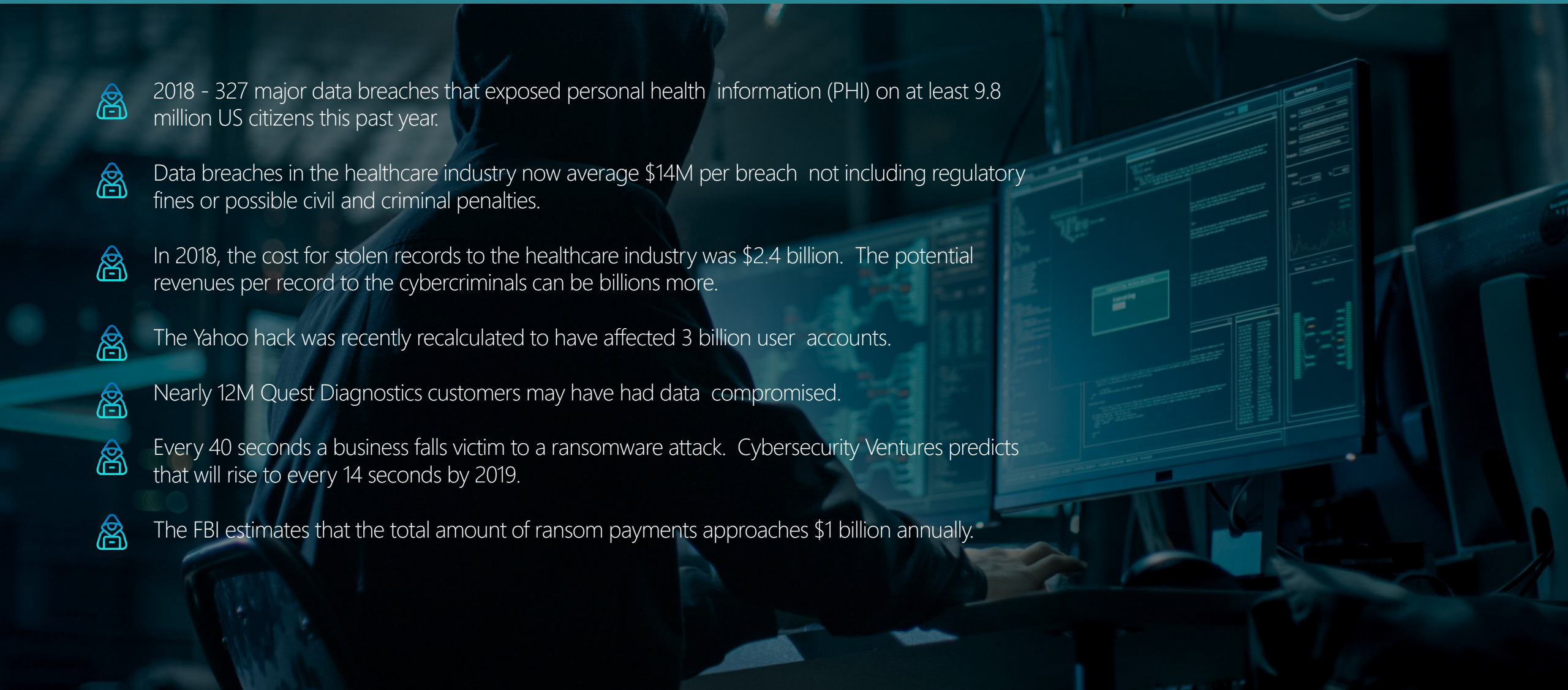
For an enterprise, the cost of a breach is devastating. Should the hackers infiltrate the core infrastructure of any entity, they can literally shutdown an entire city, state, or country.

Millions of devices are in use today without the proper security. From web cameras that are accessible through the Internet to critical devices such as SCADA that powers the electric grids.

Through brute force and/or phishing attacks, hackers have gained access to device devices from afar. As more and more devices are powered on and being used for daily life convenient, hackers will take advantage of the unsecured devices through the Internet or WiFi access points and routers.

The Impact Of Cyber Criminals

The Year-Over-Year Trend of Significant Cyber Attacks Is Increasing Dramatically



- 2018 - 327 major data breaches that exposed personal health information (PHI) on at least 9.8 million US citizens this past year.
- Data breaches in the healthcare industry now average $14M per breach not including regulatory fines or possible civil and criminal penalties.
- In 2018, the cost for stolen records to the healthcare industry was $2.4 billion. The potential revenues per record to the cybercriminals can be billions more.
- The Yahoo hack was recently recalculated to have affected 3 billion user accounts.
- Nearly 12M Quest Diagnostics customers may have had data compromised.
- Every 40 seconds a business falls victim to a ransomware attack. Cybersecurity Ventures predicts that will rise to every 14 seconds by 2019.
- The FBI estimates that the total amount of ransom payments approaches $1 billion annually.

Why Today's Technology Has Not Deterred Cyber Criminals

These multi-billion-dollar companies have not embraced the future

- Most are addressing cyber security with 1990s technology
- Single/Point Solutions are of the past

Solutions now and in the future need to tackle customer security demands across the enterprise

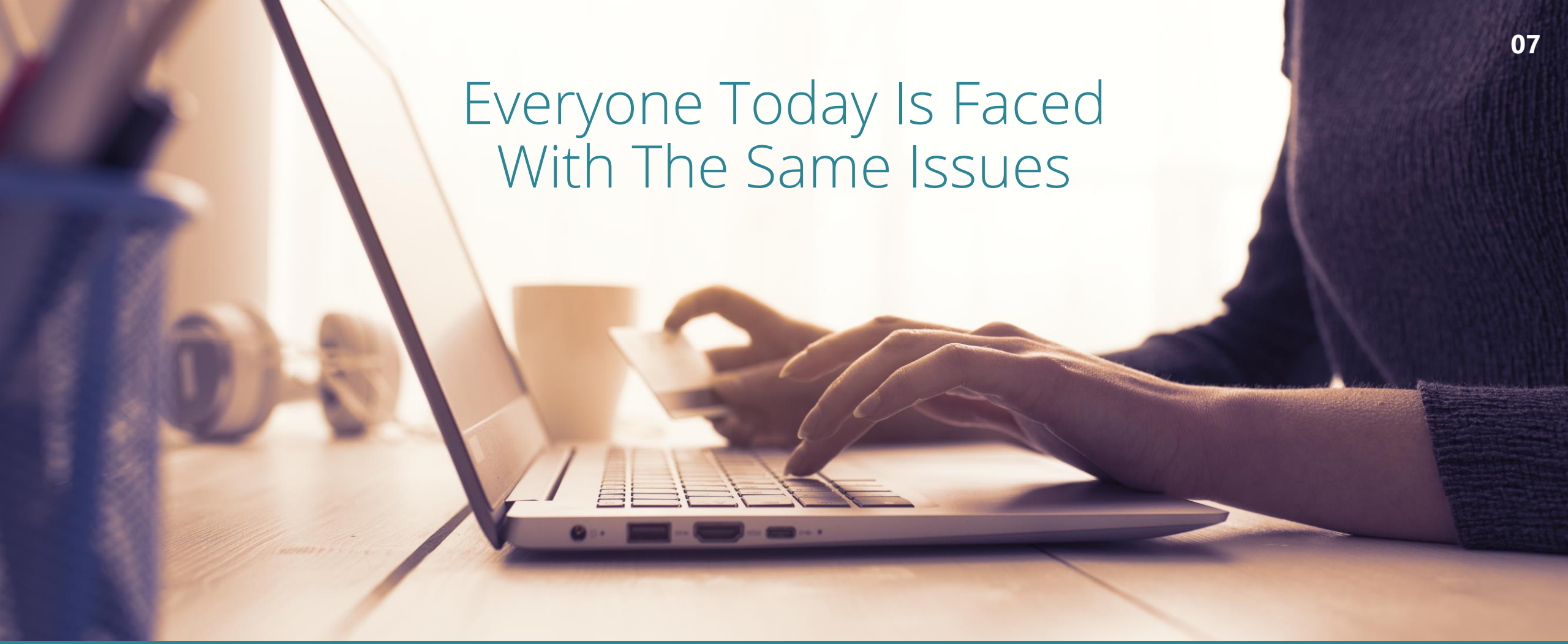
- Secure Browser
- Advanced MFA to ANY Device
- Secure Servers (onprem or in the cloud)
- Secure Access Points/Routers
- Frictionless Experience

DUO
Lookout
SECUREAUTH
RSA SecurID®
Ping Identity
acuant
Check Point SOFTWARE TECHNOLOGIES LTD
Symantec
gemalto security to be free
tripwire
GUARDSQUARE Mobile application protection
okta
Centrify ZERO TRUST PRIVILEGE
FLASHPOINT
2FA TWO-FACTOR AUTHENTICATION
SailPoint The Power of Identity
FireEye
Barracuda

About iSign

- Digital security hardware and software company focusing on Biometric Signature, Threat Detection and Prevention.
- Proprietary 6-Factor Authentication including username, dynamic token, device, GEO location, blockchain, and biometric signature.
- Solutions that identify rogue activity on your network, block unauthorized traffic (both inbound and outbound), and protect against internal and external attacks with total control given to the user.

Everyone Today Is Faced With The Same Issues



You access the internet via an unsecure browser

Your device is talking to an unsecure Access Point or Router

Your application or company is running unsecure Servers in the Cloud on Premise

WAVE BROWSER

100% SECURE AND ANONYMOUS BROWSER

FEATURES

Multi-Factor Authentication

Single Sign-On

Personal File Storage and Sharing

End-to-End Encrypted Communication

iSign International

iSign Provides A Solution At Every Potential Point Of Failure

Wave Browser

iSecure Protector IOT
6 Factor

iSecure Protector SE

An Integral Cure For The Global Hacking Epidemic

iSecure Protector SE Protection

IOT 6-Factor Authentication

iSecure Protector Server Edition Dynamic PKI Encrypted Communication 6-Factor Authentication

iSecure Protector Server Edition

3rd Party Validated

Arizona State University validated technology to cut bandwidth costs and eliminate all hacking attempts.

Cost Effective

We want to protect your digital infrastructure and eliminate the cost barrier.

Digital Asset Protection

Arizona State University validated technology to cut bandwidth costs and eliminate all hacking attempts.

Technology that Works!

iSecure Protector Server Edition is the ONLY product that protects your server; NOT VPN!

Easy Configuration

Configure using White List, Keywords, and Port Restriction

Immediate ROI

Once installed, you will see an immediate Return-of-Investment through bandwidth and access costs.

Protection starts at the server. Regardless if it is in the cloud or a physical server, iSecure Protector Server Edition dynamically opens and closes RDP/SSH ports to prevent hackers from infiltrating your core infrastructure.

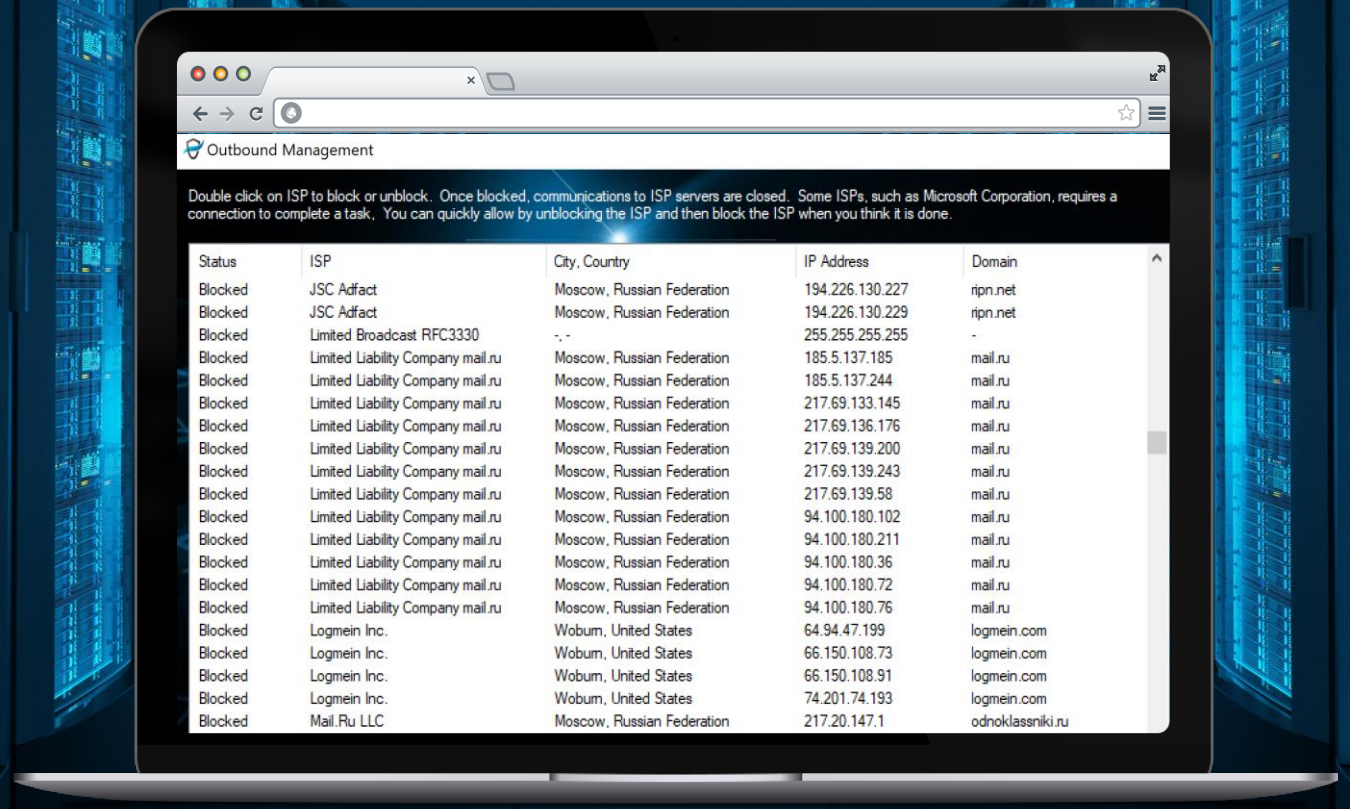
50%

Bandwidth Reduction

100%

Prevented Hacking

iSecure Protector Server Edition In Action



Status	ISP	City, Country	IP Address	Domain
Blocked	JSC Adfact	Moscow, Russian Federation	194.226.130.227	ripn.net
Blocked	JSC Adfact	Moscow, Russian Federation	194.226.130.229	ripn.net
Blocked	Limited Broadcast RFC3330	-, -	255.255.255.255	-
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	185.5.137.185	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	185.5.137.244	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	217.69.133.145	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	217.69.136.176	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	217.69.139.200	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	217.69.139.243	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	217.69.139.58	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	94.100.180.102	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	94.100.180.211	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	94.100.180.36	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	94.100.180.72	mail.ru
Blocked	Limited Liability Company mail.ru	Moscow, Russian Federation	94.100.180.76	mail.ru
Blocked	Logmein Inc.	Woburn, United States	64.94.47.199	logmein.com
Blocked	Logmein Inc.	Woburn, United States	66.150.108.73	logmein.com
Blocked	Logmein Inc.	Woburn, United States	66.150.108.91	logmein.com
Blocked	Logmein Inc.	Woburn, United States	74.201.74.193	logmein.com
Blocked	Mail.Ru LLC	Moscow, Russian Federation	217.20.147.1	odnoklassniki.ru

iSign Proprietary 6-Factor Authentication

Protect your users and employees with
6-Factor Authentication that goes beyond the standard
WebAuthn/FIDO2 authenticators.

User Name

Associates you to your account

Device

It's what you have in your possession

Dynamic Token

Locks you down to the ownership of the device

Profile Blockchain

Account integrity and non-repudiation

Geolocation

Are you in the zone

Biometric Signature

It's what you know and have

iSign Advantage

3rd Party Validated

Arizona State University validated technology to eliminate hacking by unauthorized users.

Cost Effective

Costs depend on the application features and client requests. However, we can price it to fit your needs

Front End Protection

Stop hackers right from the start. With 6-Factor, it looks at the username, GEO location, dynamic token, device, and biometric signature to eliminate hacking.

Easy to Use

6-Factor is faster than 2-Factor. We made it easy for the user. Enter username and sign your biometric signature.

Seamless Configuration

No configuration required! We provide you with the hardware and software to fully integrate with your current infrastructure.

Immediate ROI

No password reset. No customer calls. No technical requests. You will see immediate ROI.

Dynamic PKI Encrypted Communication

Protect your communication with End-to-End patented Dynamic PKI Encrypted Communication where each message uses different PKI Key Pairs.

End-to-End Encryption

All messages are encrypted at the end point with different PKI key pairs. Making the communication un-hackable. Whether it is banking transactions, sending messages, or other highly confidential data, iSign's DPKI Encrypted Communication is the solution to prevent hackers from infiltrating your communication channels. When a hacker is detected, the communication link is terminated, an email and SMS alert is sent to the administrator.

Value Priced

Every application is different. We provide you with competitive pricing on this patented technology without breaking the bank.

Easy to Use

User's will not notice anything. It is seamless and frictionless.

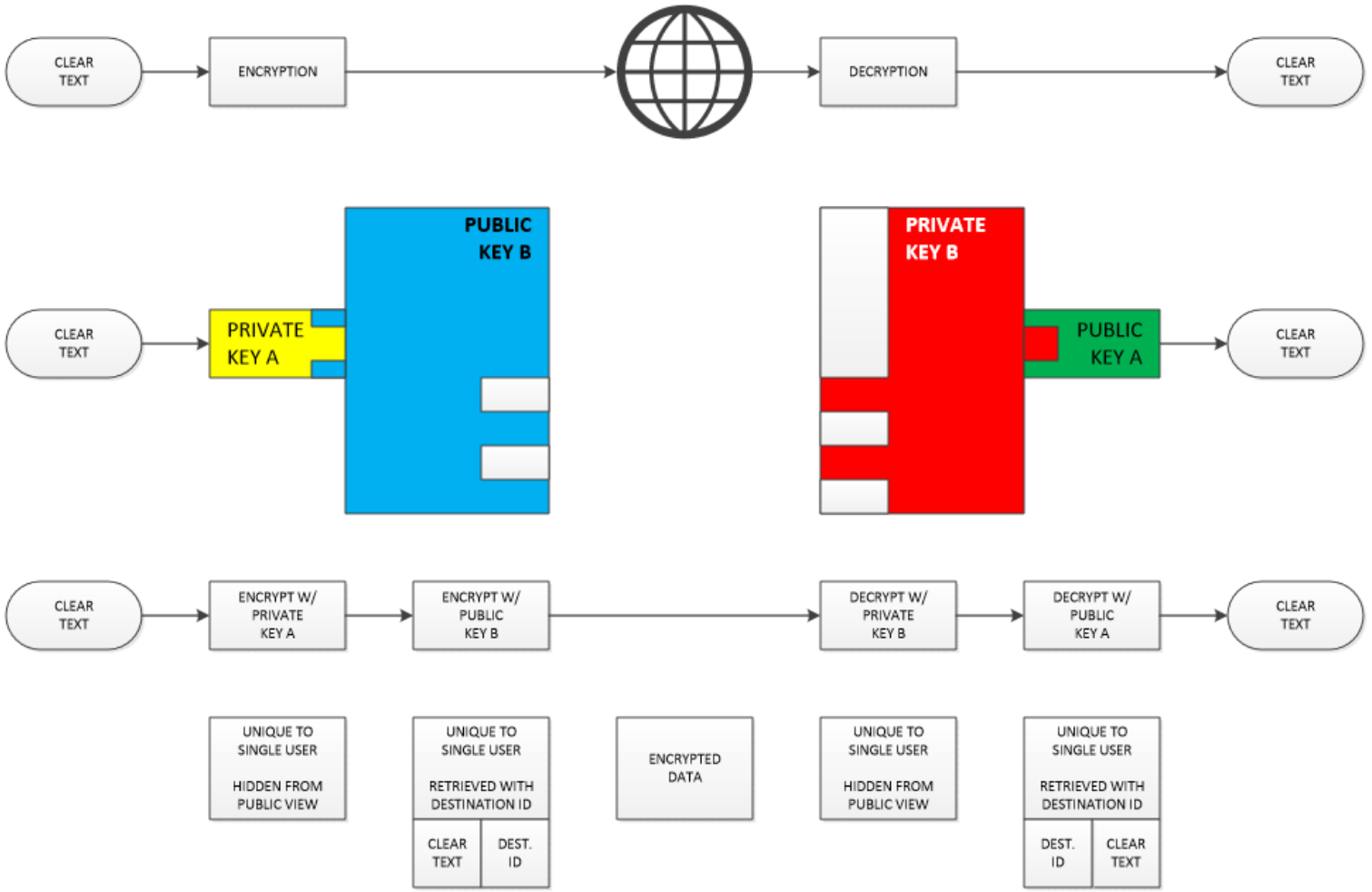
Simple API

JavaScript based API means securing your communication channels with end-to-end patented Dynamic PKI Encrypted Communication

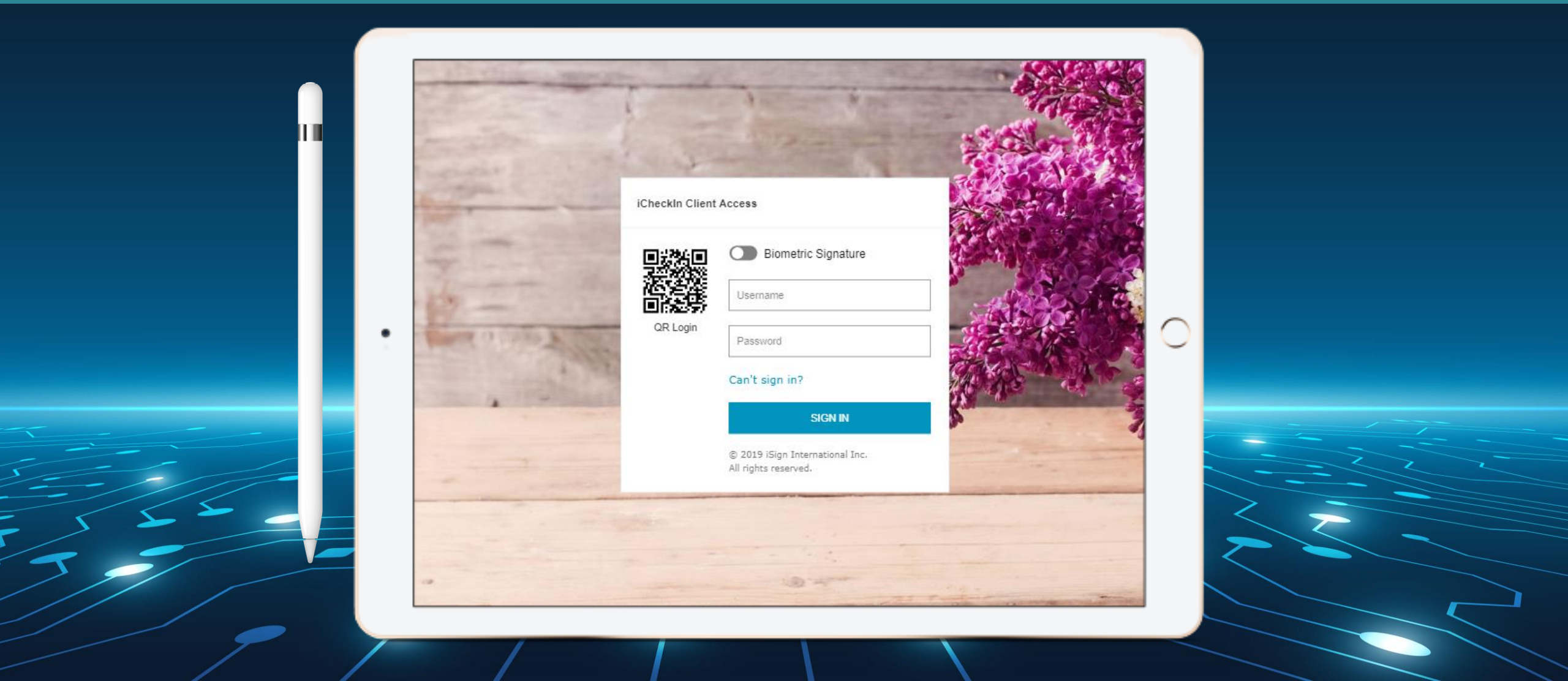
Immediate ROI

No more hacking. No more stolen data. Immediate ROI!

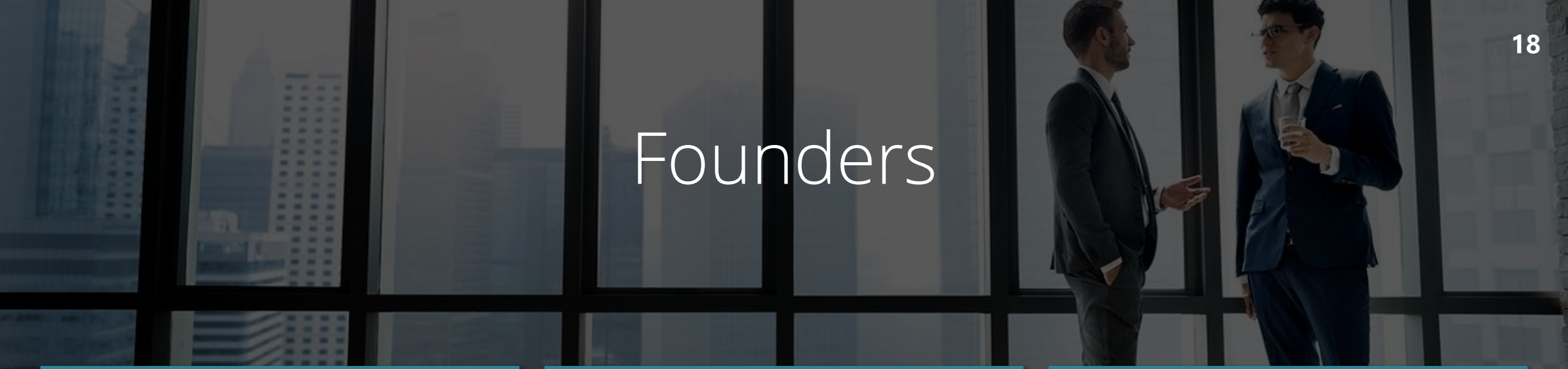
Dynamic PKI Encrypted Diagram



Action QR


iCheckIn Client Access
Biometric Signature
Username
Password
QR Login
Can't sign in?
SIGN IN
© 2019 iSign International Inc.
All rights reserved.

Enterprise Partners



Founders

GERARD MUNERA
CHAIRMAN

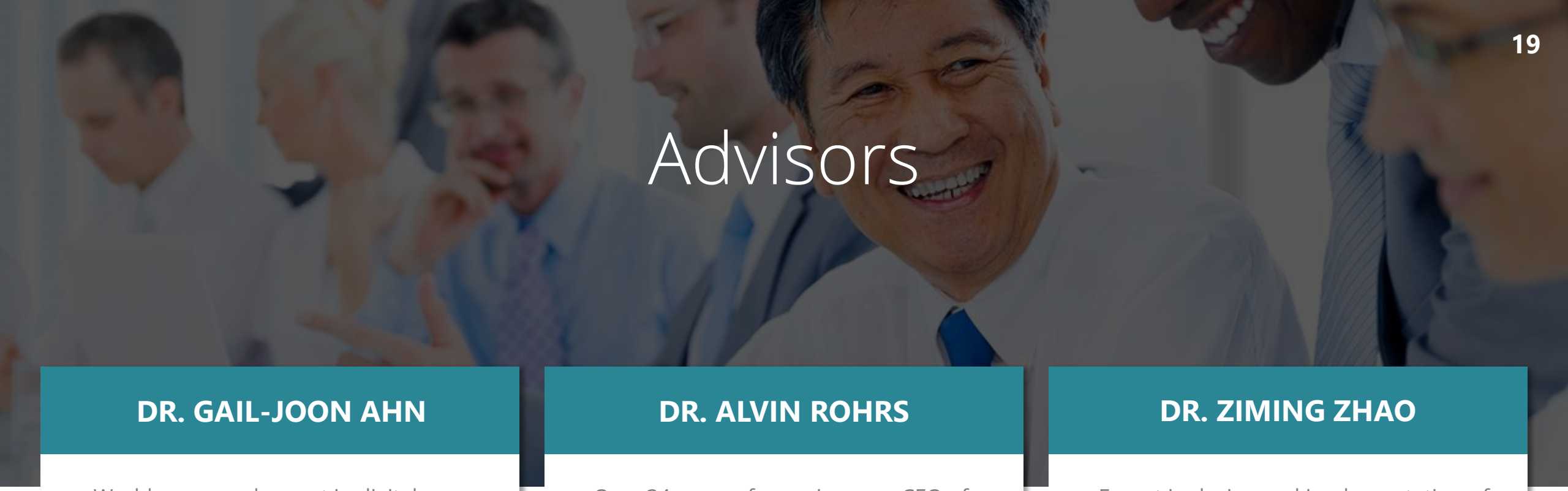
- 50 years of experience: finance, sales/marketing, engineering and operations
- Track record in building management teams, developing new businesses, and implementing restructurings and turn-arounds

WAYNE TAYLOR
CO-CHAIRMAN

- Mr. Taylor has over 35 years of experience in the fields of credit and insurance. Over the past year, he has arranged over $200 million in senior debt, and has helped restructure a number of deals, putting his clients back on normal banking terms.

THIEN PHAM
CTO

- 17 years of experience in digital security, biometric security and custom software build
- Built software companies and within 1 year were all acquired by both public and private companies
- Built custom software system that increased efficiency in workflow; in one typical example increased revenue from $3 to $30 million within first year.



Advisors

DR. GAIL-JOON AHN

- World-renowned expert in digital security management
- Led development of GFS Technology's proprietary technology
- Named a Fulton Entrepreneurial Professor at Arizona State University
- Led projects funded by Bank of America, the Department of Energy
- Expert in identity management, vulnerability assessment and security architecture for distributed systems

DR. ALVIN ROHRS

- Over 34 years of experience as CEO of Enactus
- Shaped a global entrepreneurial initiative that stretches more than 35 countries, 1,710+ university programs, 69,000+ students, and 550 corporate partners.

DR. ZIMING ZHAO

- Expert in design and implementation of secure systems for: attack mitigations, cybercrime & threat intel analysis, understanding structure of underground communities and economy and ecosystem of cybercrime, finding vulnerabilities in authentication and payment systems, and designing novel firewall and intrusion response systems for emerging software-defined networks

Case Study

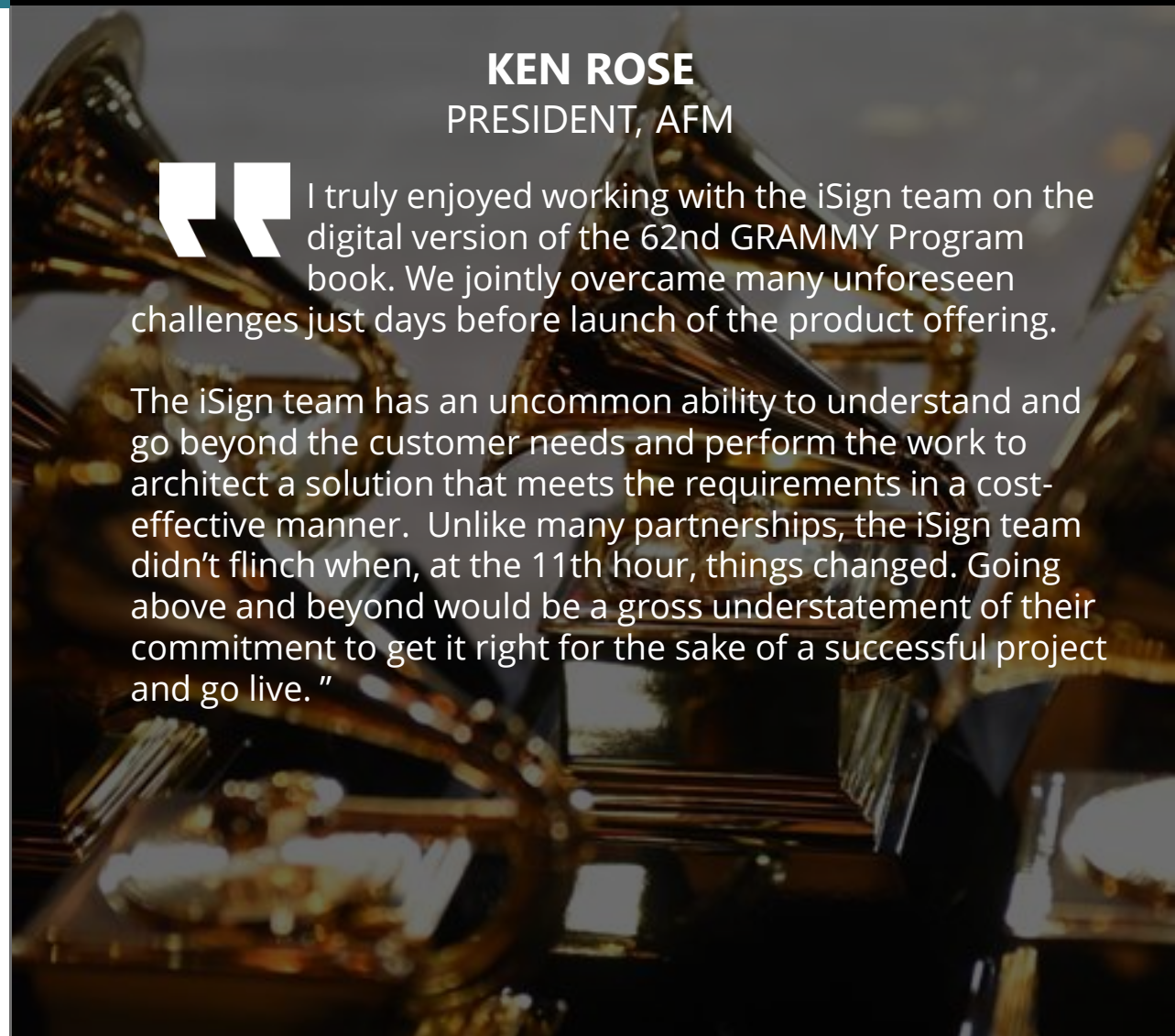
GRAMMY Awards® - The Recording Academy™

PROJECT:
62nd GRAMMY® Digital Program Book

RECORDING ACADEMY GRAMMY AWARDS®

The Challenge: Designing the first-ever, secure and searchable digital version of the 62nd GRAMMY Award® Program Book that would allow advertisers to share their celebrity-driven content confidentially.

The Solution: iSign used its vast cyber security knowledge to create a special software powered and protected by the iSign Solution Stack. iSign delivered this very sensitive, high-profile project on-time and within budget.



KEN ROSE
PRESIDENT, AFM

"I truly enjoyed working with the iSign team on the digital version of the 62nd GRAMMY Program book. We jointly overcame many unforeseen challenges just days before launch of the product offering.

The iSign team has an uncommon ability to understand and go beyond the customer needs and perform the work to architect a solution that meets the requirements in a cost-effective manner. Unlike many partnerships, the iSign team didn't flinch when, at the 11th hour, things changed. Going above and beyond would be a gross understatement of their commitment to get it right for the sake of a successful project and go live. "

Case Study

Southwest Electric Cooperative (SWEC)

PROJECT:
Protecting America's Power Grid from Data Breaches

The Challenge: Reports on the potential of cyberattacks on the United States power grid have made the news in recent months. Lloyd's of London has estimated the impact on the United States economy to be as much as $1 trillion. Southwest Electric Cooperative (SWEC) chose to participate in a pilot program with digital security experts iSign International. SWEC's goal was to find the best immediate solution in addressing existing cyberattacks on their email servers and to also realize a precautionary solution for possible electrical grid attacks in the future.

The Solution: iSign's iSecure Protector was installed on the email server to analyze network packets. This analysis found that the network had been hacked dozens of times from unauthorized IP addresses from around the world. All attacks were stopped immediately. iSecure Protector was then tested on the entire server network to protect regional electrical grids and recommended to all utility systems throughout the U.S.

RICK CONDREN
IT MANAGER AT SWEC

"Coming under attack from IP addresses all over Russia and Europe with hackers trying to access our server was a real wake-up call for us. With the help of iSign, we stopped all these attacks and are now confident our system is fully protected from hackers. Knowing that hackers had invaded our email server gives me serious concerns that they may have done the same to utilities across the country and may be much closer to attacking the power grid than anyone thought possible.

My experience with iSign tells me their system can quickly and easily identify these hackers, block them from stealing our data and stop future attacks. We will be using the iSign system and will help in introducing it to other electric cooperatives/ utilities to protect the American Power Grid. America's electric coops and hopefully all utilities will make every effort possible to protect the electric power grid and utility systems so uninterrupted services can continue for our members."

Case Study

Yavapai Regional Medical Center

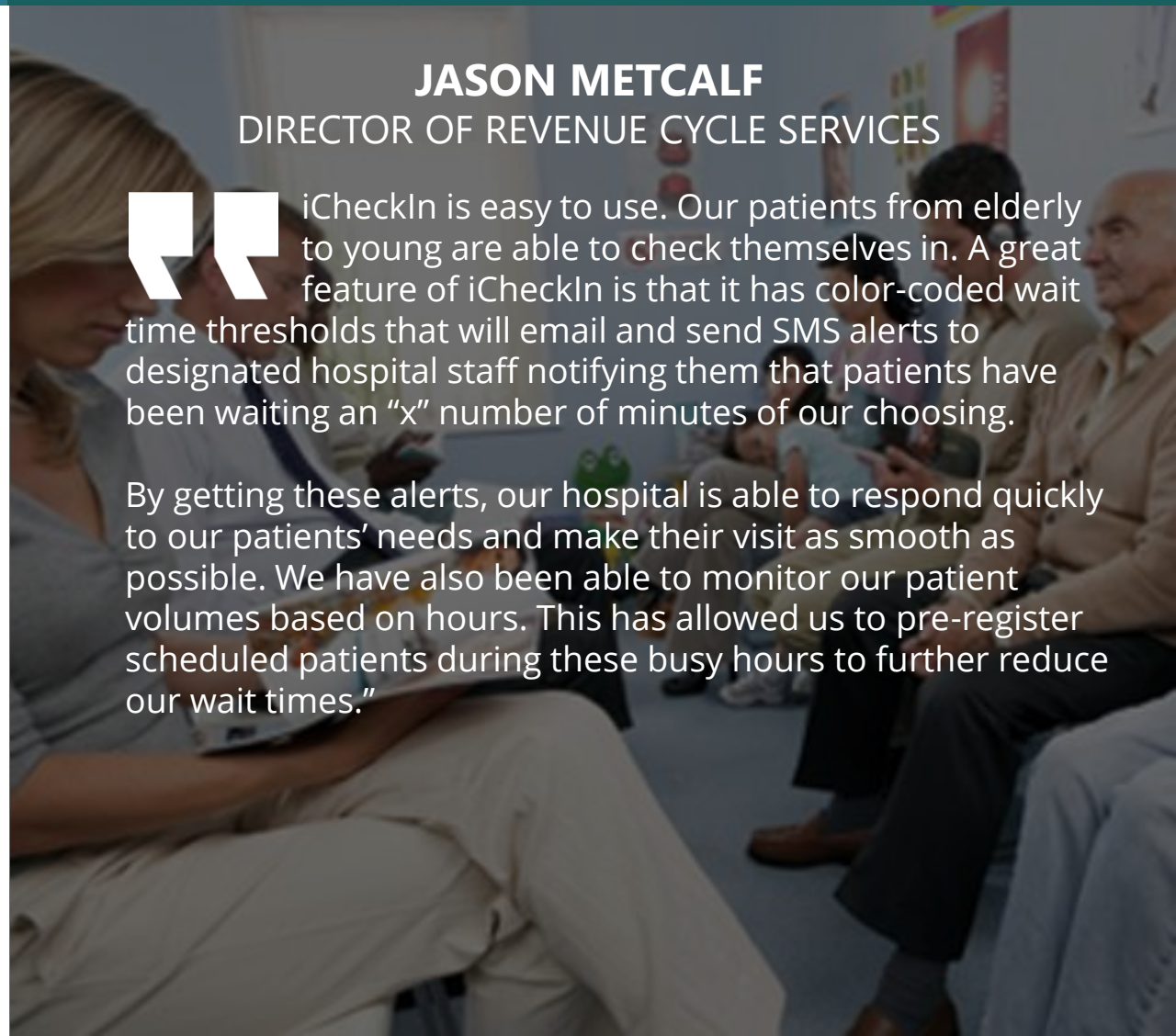
YAVAPAI REGIONAL MEDICAL CENTER

PROJECT:
Patient Registration and Health Records Safeguards

The Challenge: Improve the process for admitting patients and eliminate exposure of personal health information to the surrounding public at the reception desk, allowing patients to be more discreet about sensitive medical conditions. Trim the typical admission process time (avg 30 mins for each patient). Additional goals included decreasing long lineups, frustrated patients, and lessen the strain on the frontline staff.

The Solution: iSign installed its iCheckIn system (a secure patient check-in kiosk) at YRMC. Information is securely transferred to reception and cutting the registration time to 7 mins. Patients now spend less time waiting and can share information more discreetly. The hospital can process patients 4 times more quickly, allowing a more efficient deployment of staff to other areas of the hospital as needed.

The hospital also launched its own YRMC-branded app powered by iCheckIn allowing patients to register from home. iSign's proprietary End-to-End Dynamic PKI encryption ensures that patient data is safe from hackers and is fully compliant with the HIPAA.



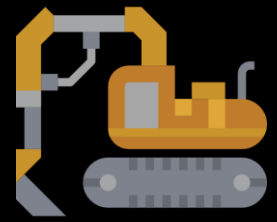
JASON METCALF
DIRECTOR OF REVENUE CYCLE SERVICES

"iCheckIn is easy to use. Our patients from elderly to young are able to check themselves in. A great feature of iCheckIn is that it has color-coded wait time thresholds that will email and send SMS alerts to designated hospital staff notifying them that patients have been waiting an "x" number of minutes of our choosing.

By getting these alerts, our hospital is able to respond quickly to our patients' needs and make their visit as smooth as possible. We have also been able to monitor our patient volumes based on hours. This has allowed us to pre-register scheduled patients during these busy hours to further reduce our wait times."

Case Study

Integrated Machinery, Inc.

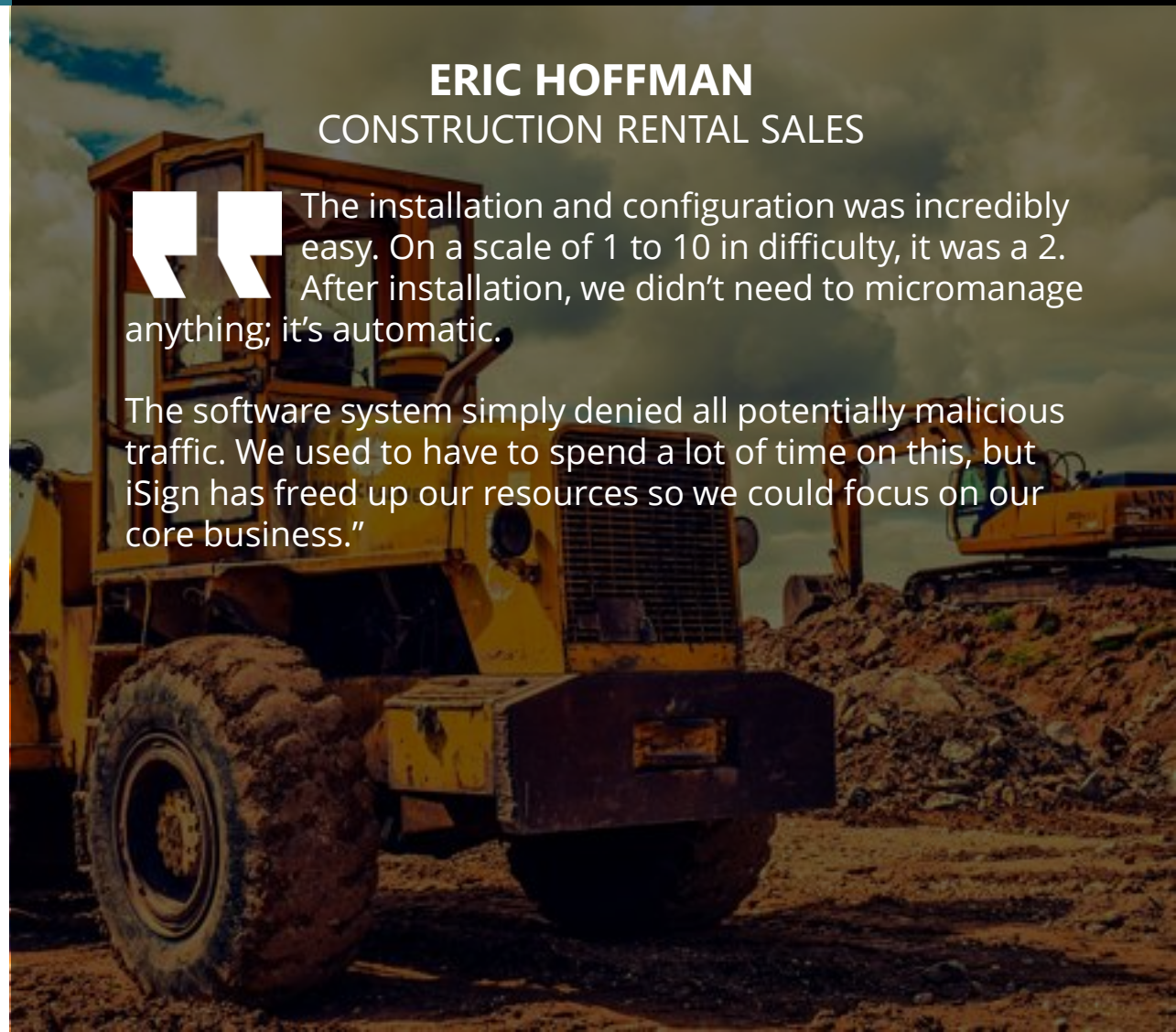


PROJECT:
Ransomware Containment & Removal

Prior to the attacks, the company had strong anti-virus and other mitigation methods in place to address the most common attacks and their servers were properly configured as per best practices. Unfortunately, these protection methods did not mitigate against some of the more sophisticated threats and vulnerabilities.

The Challenge: Deploy an end-to-end solution that not only mitigates malicious activity from accessing a network, but also neutralizes malware and deny destructive actors the ability to impact operations and extract critical data.

The Solution: iSecure Protector SE was deployed and performed an exhaustive review of all IPs that made connection with the company's network within the same time frame of the attack chain, detected all the malicious (or potentially malicious) actors and permanently denied them access. and a protective dome was placed over the enterprise, denying any potentially malicious traffic the ability to exfiltrate data or communicate outside of the network. The result was the complete mitigation of the threat to the company.



ERIC HOFFMAN
CONSTRUCTION RENTAL SALES

"The installation and configuration was incredibly easy. On a scale of 1 to 10 in difficulty, it was a 2. After installation, we didn't need to micromanage anything; it's automatic.

The software system simply denied all potentially malicious traffic. We used to have to spend a lot of time on this, but iSign has freed up our resources so we could focus on our core business."

Call us today for a demonstration.

If you like, we can give you a 30-Day Free Trial of our security suite.

Seeing is believing.

CONTACT

STEAPHAN WEIR

sweir@isignintl.com

iSign® Patents (8 showing, 63 total)

Docket No.	Patent No.	Title	Status
0706190.127-KR1	736856	System And Method For Payment Sharing	Issued
0706190.124-KR1	878039	Method And System For Payer-centric Settlement Using Mobile	Issued
0706190.126-KR1	896034	Method And System For Settlement Using Mobile In Wireless Internet	Issued
0706190.125-KR1	1015558	A Method And System For Managing Member By Central Institution	Issued
0706190.123-US1	8,073,771	Method And System For Payer-centric Payment Using Mobile Terminal	Issued
0706190.121-US2	9,069,948	Methods, Systems, And Media For Measuring Quality Of Gesture-based Passwords	Issued
0706190.131-US1	10,135,618	Method For Using Dynamic Public Key Infrastructure To Send And Receive Encrypted Messages Between Software Applications	Issued
0706190.131-US2		Methods, Systems, And Media For Using Dynamic Public Key Infrastructure To Send And Receive Encrypted Messages	Issued