Cyber Security and the Energy Industry: Digital Identity Solutions from HID Global®


A malicious cyber attack on your company is a matter of when, not if.
Will you be ready?

#1 target for cyber hackers: oil and gas companies

Oil and gas companies are the number one target for cyber hackers, and the number of cyber criminal groups targeting the energy industry nearly doubled in recent years.[1]

Cyber attacks against the energy sector are growing in frequency, sophistication and severity.

As energy companies digitize operations, foreign nation-states intent on stealing secrets, disrupting production or worse are finding more ways to worm their way in.

How vulnerable are you?

Though 87% of natural resource companies reported a cyber incident in 2017,[3] most continue to underestimate or ignore their risk, viewing it on par with weather disruptions.[4]

In 2017, oil and gas companies in the U.S. and Canada devoted less than 0.2% of revenues, or roughly $50 million, to cyber security measures.[1]

Proportionately, oil and gas companies in the Middle East and North Africa are prepared to spend $1.9 billion on cyber security in 2019.[2]

A facilities breach can halt operations, put production at risk, and jeopardize revenue. Oil and gas companies need a solution that balances security with smooth, efficient business operations.

Sources:

1 Naureen S. Malik, "Energy Companies Aren't Doing Much to Defend Against Soaring Cyber attacks," Bloomberg, bloomberg.com/news, (April 30, 2018).

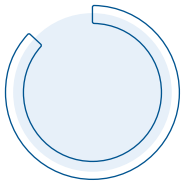
2 Sony Shetty, "Gartner Says Middle East and North Africa Enterprise Information Security Spending Will Grow 9.8 Percent in 2019," Gartner, gartner.com/en/newsroom, (October 22, 2018).

3 "Global Fraud and Risk Report: 10th Annual Edition," Kroll, kroll.com/en/insights, (2017-18).

4 Collin Eaton, "Hacked," The Houston Chronicle, houstonchronicle.com/news.

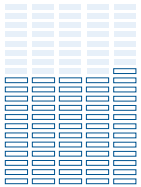
What's your risk? A closer look.

Oil and gas companies have largely shrugged off the threat to their industry—and to their bottom line.



87%

of natural resource companies in the United States reported a cyber incident in 2017[3]

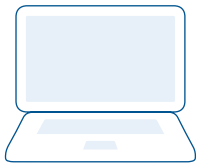


61%

increase in number of cyber criminal groups targeting the energy industry (2015-2018)[1]

61%

of energy industry cyber security specialists say that their companies lack adequate protection.[4]

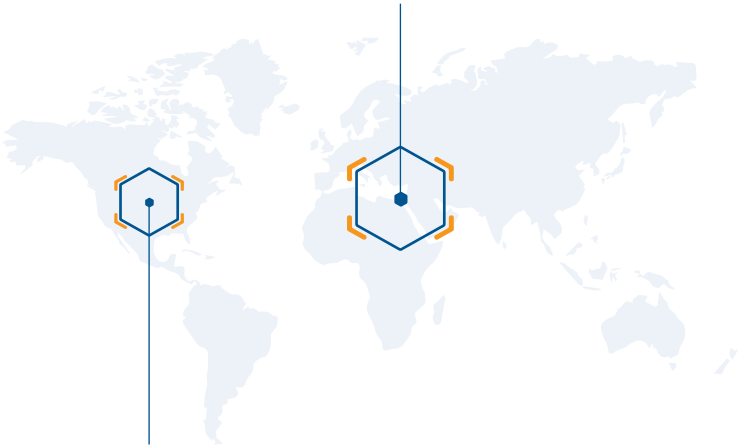


350

Most of the 350 cyber security incidents that the Department of Homeland Security investigated between 2011-2015 involved infiltrated control systems.[4]

$1.9 BILLION:

amount oil and gas producers in the Middle East and North Africa are expected to spend on cyber security in 2019 (an increase of 9.8% over 2018)[2]



$50 MILLION:

amount oil and gas producers in the U.S. and Canada spent on cyber security in 2017[1]

3X: the financial services industry spends triple what the energy industry does on cyber security[1]

How can a cyber attack affect your business?

Cyber hackers backed by foreign nation-states steal sensitive information by surreptitiously installing **malware** on computers and servers, or tricking employees into giving it up through **phishing**. The effects can be far-reaching.

Clear and present danger

In 2017, cyber hackers attacked a petrochemical plant in Saudi Arabia. Is one of yours next?

These cyber criminals weren't hunting for data or trade secrets—they planned to trigger an explosion. Instead, a bug in the code initiated a shutdown.

Officials, who later tied the hackers to the Russian government, believe they have fixed their mistake and are actively pursuing their next target.[5]

Sophisticated and highly coordinated cyber attacks like this are on the rise. What's at stake? Stalled operations, production slowdowns and revenue losses, as well as potentially devastating environmental damage and the loss of human life.

Sources:

1 Naureen S. Malik, "Energy Companies Aren't Doing Much to Defend Against Soaring Cyber attacks," Bloomberg, bloomberg.com/news, (April 30, 2018).

2 Sony Shetty, "Gartner Says Middle East and North Africa Enterprise Information Security Spending Will Grow 9.8 Percent in 2019," Gartner, gartner.com/en/newsroom, (October 22, 2018).

3 "Global Fraud and Risk Report: 10th Annual Edition," Kroll, kroll.com/en/insights, (2017-18).

4 Collin Eaton, "Hacked," The Houston Chronicle, houstonchronicle.com/news.

5 Nicole Perlroth and Clifford Krauss, "A Cyber attack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try," The New York Times, nytimes.com/2018, (March 15, 2018).

Protect your business

Some energy companies have begun to mitigate their risk with cyber security measures. But federal officials find that most have cut corners.[4] In fact, most are unable to detect malicious activity inside their control systems, and thus are unable to fight it off.[4]

Given what's at stake in the event of a cyber security breach, it's critical to ensure your company is fully protected.

How do you keep bad actors out? By ensuring that the people seeking access to your system are who they say they are.

Traditional usernames and passwords or access key cards alone are not enough to keep determined cyber criminals out. To verify a user's identity, companies must create a highly sophisticated digital identity for each user.

Source:

4 Collin Eaton, "Hacked," The Houston Chronicle, houstonchronicle.com/news.

Modern risk-based authentication is the key

The FBI and Department of Homeland Security both recommend multi-factor authentication for verifying the identity of employees, contractors and visitors, as well as IoT devices like tablets and smartphones. Modern, risk-based authentication takes this to the next level by using artificial intelligence (AI) to combine MFA with real-time risk factors.

Multi-factor authentication begins with three pieces of information to confirm a user's identity:

- What you are: fingerprint or retina scan (biometrics)
- What you have: smartcard or similar device
- What you know: PIN or password

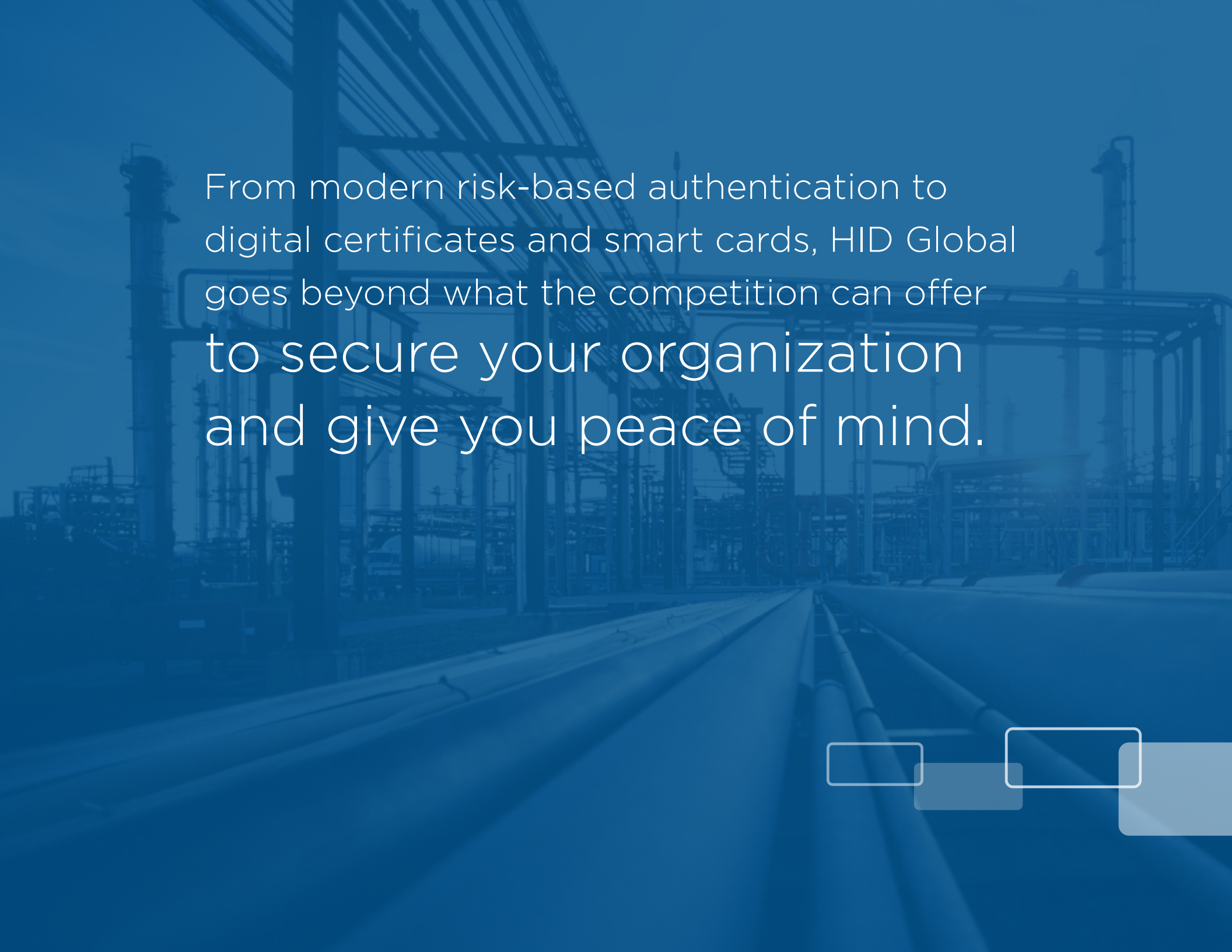
This data is then combined with risk-based factors that further narrow down who may and may not gain access to your system:

- Physical gestures
- Geo-location
- Time of access

Together, this information lets the system make a highly-informed, highly-accurate determination about the identity of the person trying to get in.

It's simple and effective. It lets the right people in and keeps the wrong people out.

It also balances the need to maintain efficient day-to-day operations with high assurance cyber security. And it meets industry and government-issued compliance requirements.


From modern risk-based authentication to
digital certificates and smart cards, HID Global
goes beyond what the competition can offer
to secure your organization
and give you peace of mind.

Digital identity management solutions designed for oil and gas

HID Global's ActivOne® is the world's most comprehensive identity management platform, including multi-factor and risk-based authentication.

Our customizable identity credential management solution keeps hackers out while making it convenient for employees, partners, vendors and visitors to conduct business.

Backed by decades of experience supplying government-grade security, HID Global offers the energy industry high assurance security that flexes to meet the needs of your company —and delivers substantial ROI.

Convenient, integrated security

HID Credential Management Service (CMS)

Protect access to networks, workstations and servers inside a firewall, VPNs, public and private cloud applications, building facilities, and other resources

- Easy to install and fast to deploy
- Integrates with existing systems
- Single sign-on
- Scalable so you can manage a large number of users in locations all over the world

Crescendo® C2300, Crescendo® Key and Crescendo® Mobile

- Convenient access via smart badges, smart USB keys and a mobile app
- Secure login to workstations, laptops, web-based cloud applications or VPN gateways
- Grant physical access to buildings, rooms and cabinets

DigitalPersona®

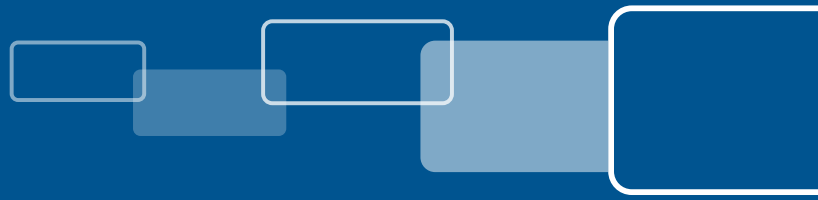
- Award-winning next generation authentication software
- Secure all your applications including web, cloud, Windows, mobile, VDI, VPN and legacy mainframe apps
- Customizable security requirements let you flexibly authorize each user

IdenTrust™

- Digital certificates guarantee secure email, data encryption, digital signing and more
- Authenticate identities in more than 175 countries
- Recognized by financial institutions, government agencies and enterprises around the world

HID Global. Simple. Secure. Smart. All from a single trusted source.

HID Global Cyber Security Solutions for Oil and Gas at **hidglobal.com/iam**



Powering Trusted Identities

2019-07-03-iams-oil-gas-sols-eb-en PLT-04568