Stay Ahead of Security in an Unpredictable World

FedRAMP certified

Trusted and used by U.S. Intelligence Agencies

Winner of 2019 James S. Cogswell Outstanding Industrial Security Achievement Award

SAP NS2
NATIONAL SECURITY SERVICES

COVID-19 isn't the only problem disrupting our lives in 2020.

There's another invisible threat rapidly advancing: **cyberattacks**.

It's more important than ever to protect your organization's proprietary information on all fronts — as millions of workers settle into a new, work-from-anywhere life.

TABLE OF CONTENTS

Today's Challenges

Even in a world obsessed with predictive analytics — 2020 has been a year no one could predict.

A race to adjust. A race to the cure. A race to get ahead of new threats that could disrupt our operations — and livelihood — again.

Change is happening in multitudes, fast. Only a few months into 2020, the global pandemic left businesses of all sizes scrambling to transition millions of people to remote working, securely.

The challenge is, most organizations with legacy infrastructures didn't have the flexibility, agility, or capability to quickly and safely move work processes remotely — potentially opening the door for breaches.

The new reality brought new cybersecurity challenges, with increased levels of threats to manage and the need to migrate to the cloud with no time to spare.

Rising Risk Accelerates Timelines

Cybersecurity is a dynamic environment.

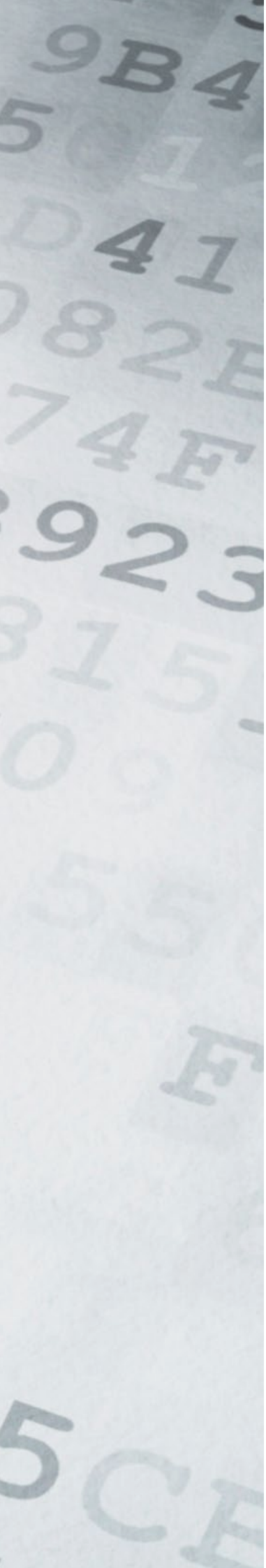
Threats continue to expand. Adversaries get stronger and smarter. And advancing threats must be met with advancing defenses.

Most organizations have the basics down: firewalls and digital signatures. This is the first necessary layer that keeps outsiders out of critical technical systems. This works by the system recognizing what is malware vs. not, by using a unique signature to identify and block unknown threats.

But firewalls aren't enough anymore.

- Bad actors are advancing their tactics, fast. They can bypass an organization's firewall with a signature that is unknown to the system, so that the malware is undefinable. This new malware is being created daily in order to circumvent more vulnerable, legacy cybersecurity systems that haven't been updated for years.
- Hackers are also using ransomware and social engineering, designed to infiltrate organizations through employees. This can come in the form of phishing emails, which can look like any other company branded email — making it near-impossible for an employee to recognize the threat before they already clicked on the link and compromised their system.

Monitoring and responding to these situations require day-to-day dedicated IT resources — and the right balance of people, processes, and technology to get ahead of the next risk. Innovation is needed to ensure defenses are ahead of the bad actors, who'll undoubtedly be working up the next, bigger attack.



TRENDS TO STAY AHEAD OF

Two cause-and-effect trends have grown in the past 10 years — a trend that's only amplified during the uncertainty of the pandemic:

1. **More threats. More sophisticated attacks.** The vulnerabilities, data handling scandals, and cyber exploits in today's cyber landscape continue to grow.
2. **More regulation to follow.** Cybersecurity compliance and regulatory requirements will only continue to increase in coverage, stringency, and volume.

The types of threats to guard against:

- **Threats against the business** – theft or malicious activity that threatens intellectual property, customer and supplier data, and business data.
- **Threats against the network and infrastructure** – internal or external actions that could damage or destroy software, configurations or processes as well as bad actors or bad configurations that could damage or disrupt supply chains.
- **Threats of content** – leaks or compromise of personal information, financial information, and customer or personnel information.

Vulnerable sectors include **government, healthcare, financial services, utilities, and the defense industry.** These are the same industries that have growing legal requirements, such as:

- FedRAMP
- International Traffic in Arms Regulations (ITAR)
- Defense Federal Acquisition Regulation Supplement (DFARS)
- Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG)
- DHS National Infrastructure Protection Plan
- NERC CIP
- Federal Financial Institution Examination Council handbook (FFIEC-IT)
- Health Insurance Portability and Accountability Act (HIPAA)
- ICD 503 Controls

Finding the Right Fit:

Your Ideal Cloud Security Solution

Trust. Security. Compliance.

Choose a provider you can trust — that meets *your* standards.

Some baseline questions to ask your provider: How do we know your environment is secure? If there's an incident, how soon will we know? What happens then, and what information will you share with us?

You can also ask questions and narrow down cloud solutions providers through FedRAMP's program. It tracks quality of solutions through rigorous and objective third-party assessments. This can build trust with your provider, knowing there's continuous transparency into their process and checkpoints led by outside industry experts.

Look for access to unique threat intelligence.

Security monitoring starts with an understanding of deep, everchanging threats — as well as the regulatory landscape. With security monitoring in place from your provider, you (and your legal team) can rest assured that your organization's adhering to the strictest standards.

Get proof of tireless innovation and problem-solving.

Your cybersecurity defenses are only as good as your provider's latest innovation. Ask for proof of success. Know who their partners are. Commitment is best shown through direct praise from customers.

Find a system that strikes a balance of people, process, and technology.

Some solutions focus solely on technology and completely miss the people component. This is a big mistake. Cybersecurity problems should be approached by your provider programmatically, utilizing the best and brightest minds in the field — with diverse thinking from every angle, every day.

SAP NS2 Security Solutions

Take uncertainty out of migrating to the cloud. Close the gaps — and be prepared for the next potential threat.

NS2 cyber defense solutions was created with the federal, state, local, and tribal government agency needs in mind — to help protect our nation's most sensitive networks and data from the world's advancing cyber attackers.

NS2 cloud technology is a CDM program-approved product (APL). This means a streamlined procurement process and access to funding for quick deployment.

NS2's solution was built and is continually updated based on insights from government and commercial datasets.

NS2 mitigates risks by monitoring threats using machine-learning, predictive analytics and user behaviors — prioritizing actions based on potential impacts. We also perform endpoint detection and response to protect servers, PCs, and mobile devices across your workforce.

Protect your organization's most sensitive information

Secure business and technology information, PII, and stay compliant with SAP NS2:

Business Information

- Intellectual Property
- Trade Secrets
- Customer and Supplier Information
- Cardholder Data

Personal Identifying Information (PII)

- Personal Health Information (PHI)
- Financial Information
- Educational Information

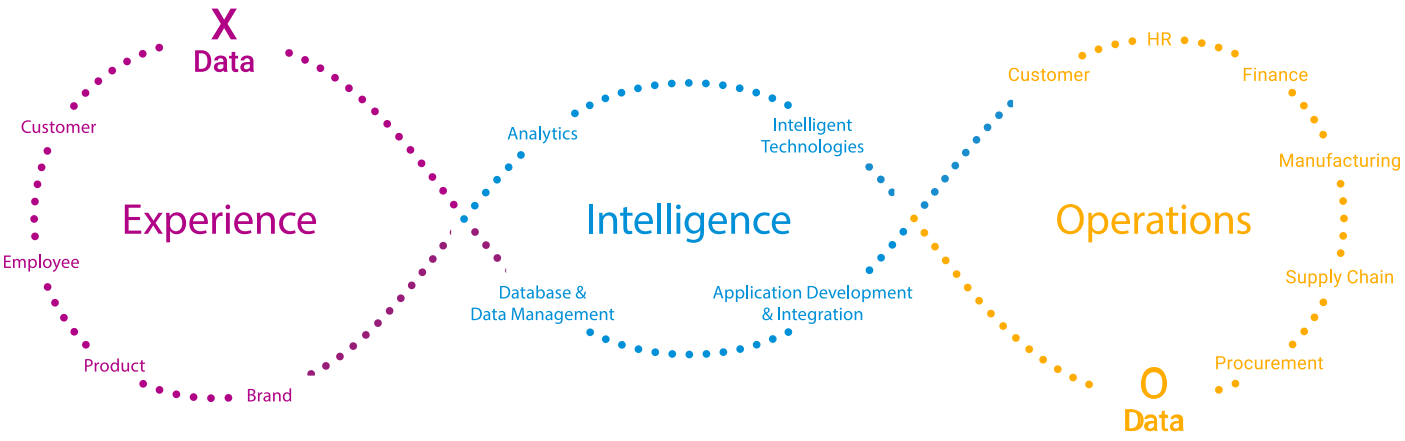
Technical Information

- Software architecture
- SAP product configurations
- IT Infrastructure Details

SAP NS2 HELPS GOVERNMENT, BUSINESS AND REGULATED INDUSTRIES TACKLE THE COMPLEXITY OF MIGRATING TO THE CLOUD.

How it Works

With people, process, and technology — we have you covered.



Qualtrics

- Qualtrics

Business Technology Platform

- SAP Analytics Cloud
- SAP Cloud Platform

Intelligent Suite

- Secure HANA Cloud
- S/4HANA Cloud, Extended Edition
- SAP SuccessFactors
- SAP Integrated Business Planning

Boost Your Defenses with Industry-Leading Predictive Multi-Vector Detection, Prevention, and Response Tools

Together, these capabilities provide the most effective response to increasingly sophisticated malware and malicious insiders.

Common approaches to cyber defense, like passive threat management, are dependent on recognizing the signatures of known malware binary code.

This is key to protecting your organization against malware with new and unknown variants, as well as malware that runs in the RAM memory of servers and endpoints.

- Specialized handling of sensitive data
- Restricted and air-gapped areas
- Secure remote access to your SAP environments
- 24/7/365 global support
- Dedicated SAP Secure Support Advisor
- U.S. credentialed support personnel (background checks, cyber security certifications, etc.) Secure back office staffed by U.S. citizens, located in the U.S.
- Special handling of sensitive data and filtering of support messages to limit exposure when needed
- Restricted / secure areas when viewing customer information with infrastructure isolated and air gapped from the rest of SAP
- Technology control plan customized for secure remote access

NS2's Cyber Defense Solutions

Understand real-time user behavior analysis with machine learning and predictive analytics

GoSecure

Endpoint Detection and Response (EDR)

Conducts active investigation and mitigation to identify both known malware and new malware variants, as well as fileless attacks.

+

Inbox Detection and Response (IDR)

Automates email threat resolution in the user's inbox. Endpoint and server security. Inbox security.

How EDR Works

Loads a unified endpoint agent on endpoints within an organization—from computers to servers and mobile devices—that constantly monitors the behaviors of the devices via real-time, on-disk and in-memory behavioral analysis.

If a potential breach is identified, it cuts off communication between the compromizsed endpoint and the rest of the network.

How IDR Works

Empower employees to be part of the solution. Now they can securely report suspicious emails with the press of a single button.

The potentially malicious message will be quarantined and routed to an active response center, where it's investigated by the program and either returned to the user as valid or permanently deleted in minutes.

Large-scale, complex migrations are where we shine.

Cost controls, streamlined

Challenge:

An Aerospace & Defense agency couldn't get visibility on the volume and cost of additional external resources.

Result:

Captured and consolidated potential resource costs on a system that now serves 36,000+ users.

Massive migration? No problem

Challenge:

A large Federal Agency needed to migrate to the cloud —using a FedRAMP certified data center (while replatforming to SAP's in-memory solution).

Result:

Migrated over 200 systems | 15,000 users | >15TB Source Data; converted from Oracle to HANA.

Tax system for a statewide agency network

Challenge:

A state government needed a FedRAMP cloud environment to host their federal tax id information and comply with IRS Publication 1075.

Result:

Rolled out the cloud solution to over 50 agencies within a rapid timeline.

About SAP NS2

At SAP NS2, security is never an afterthought. It's in everything we do.

We build tailored solutions that leverage some of industry's best software tools and the most-talented humans.

We are a wholly owned subsidiary of SAP, founded with the mission of security in mind.

SAP spends $3.5 billion annually in Research and Development (R&D), which allows SAP NS2 to bring tremendous technology and innovation to our customers across government and regulated industries.

SAP NS2 is 100% U.S. based and U.S. staffed, with expert personnel working around the clock to keep data safe and solutions running.

At SAP NS2, we bring leading analytical insights and data fusion technologies from SAP and apply them to mission-critical workloads. We believe that innovation and security should go hand in hand.

Through the incorporation of the Intelligent Enterprise, we leverage emerging technologies to enable customers to focus on high-value outcomes.

WE CRUSH COMPLEX PROBLEMS
WE OBSESS OVER SECURITY
WE MAKE A DIFFERENCE

We deliver cloud and software solutions built on the fundamental principles of security, privacy, control, compliance and transparency. In addition, we offer secure consulting and support services from credentialed experts in the national security space.

Our goal is to create an avenue for our customers to revolutionize their overall business models while remaining compliant and protected.

SAP NS2 HONORED WITH 2019 COGSWELL AWARD FOR OUTSTANDING INDUSTRIAL SECURITY

The Cogswell Award is the most prestigious honor the Defense Security Service may bestow on cleared industry.

Of the more than 13,000 cleared contractors, less than one percent are annually selected to receive this award.

The award recognizes the partnership between industry and government to protect classified information – which ensures the greatest protection for the U.S. warfighter and our nation's classified information.

Scale with a secure infrastructure

Organizations using SAP NS2 Secure Cloud include:

The NS2 Difference

FedRAMP certified

Trusted by U.S. intelligence agencies (U.S. persons on U.S. soil only)

No additional cost from your current SAP Enterprise Support Program

2019 James S. Cogswell Outstanding Industrial Security Achievement Award

Get Started

sapns2.com/security

SAP NS2
NATIONAL SECURITY SERVICES

Already an SAP customer?
Get Secure Enterprise Support, free.