Cutting-edge software solutions to protect your organization's infrastructure and data

Cyber Defense Solutions from NS2, powered by GoSecure, are available to federal, state, local, and tribal government agencies to help protect your networks and data from cyber-attacks. This cutting-edge technology is on the CDM program Approved Products List (APL) and is available for acquisition using the CDM Request for Service process, which streamlines procurement and augments access to funding to deploy critical capabilities to your organization.

RESOURCES

Securely Migrate to the Cloud with SAP NS2 Video
carah.io/SAP-NS2-Cloud-Migration

SAP NS2 Secure Cloud Whitepaper
carah.io/SAP-NS2-Secure-Cloud

Innovations In State And Local Cybersecurity
carah.io/SAP-NS2-SL-GovLoop

SAP NS2: Enhancing Enterprise Endpoint and Inbox Security

TECHNICAL SUMMARY

Federal agencies continue to be threatened by increasingly sophisticated cyberattacks that target organizational data and infrastructure. Phishing attacks targeting user credentials quadrupled since 2018, and session hijacking and insider attacks can wreak havoc on an organization's day-to-day operations, as well. When it comes to data breaches, ransomware attacks effectively target organizations with rich data to hijack, while malware and botnets can result in the hemorrhaging of data and records.

The ways in which bad actors attempt to infiltrate an organization's digital infrastructure are constantly evolving, making it difficult to educate end users on cyberthreats and time-consuming to protect servers and endpoints from the latest attack vectors. Automating these processes takes the load off of IT analysts, allowing them to address more pressing matters.

NS2, a subsidiary of SAP, offers two cyber defense solutions, powered by GoSecure, that address both endpoint security and email security. NS2's GoSecure Endpoint Detection and Response and GoSecure Inbox Detection and Response protect enterprise systems at their most vulnerable areas: endpoints and emails. Both solutions are available on NS2 Secure Cloud, and EDR can be conducted on-premise as well.

SAP NS2 Cloud solutions adhere to the strict guidelines set forth to protect International Traffic in Arms Regulations (ITAR) and Export Administration Regulations (EAR) related data. The security controls are reviewed and audited by a 3rd Party Audit Organization (3PAO) in order to independently assess that the necessary precautions are implemented correctly. SAP NS2 was also the winner of the 2019 Defense Security Service James S. Cogswell Outstanding Industrial Security Achievement Award.

AVAILABLE CERTIFICATIONS ACROSS CLOUD SOLUTIONS

- FedRAMP
- DoD SRG for IL 2 and 4
- CJIS Security Policy
- ITAR
- Export Administration (EAR)
- FIPS 140-2
- IRS-1075

THE CHALLENGE

The threat of cyberattacks is nothing new to IT analysts, and several wide-ranging tools have been developed over time to prevent such attacks. Tools such as firewalls and digital signatures have been traditionally used by organizations to build technical barriers that keep bad actors out of critical systems. The successful use of these tools implies knowing what the malware threats look like in order to stop them, using the unique signature in the software to identify and block known threats.

However, this traditional approach leaves organizations open to zero-day attacks, which can bypass an organization's firewall structure because their signature is unknown to the system, allowing the malware to operate without detection. Bad actors are increasingly using new malware to circumvent legacy cybersecurity systems, carrying out attacks on unsuspecting organizations long before the malware is identified and its signature added to firewall software.

Breaches are not only conducted by external bad actors via malware—savvy adversaries are turning to ransomware or social engineering to infiltrate organizations via unsuspecting employees, as well. A common tactic involves an email

that appears to come from a valid sender and asks the receiver to click on a link, which then surreptitiously downloads malware that is introduced into the enterprise environment. These phishing emails are effective because they are sent at such a high volume and can look so genuine that many users don't have the expertise to identify every phishing attempt they come across.

Even if an employee suspects that an email in their inbox is suspicious, what next steps should they take? The best case scenario in most organizations often involves the user forwarding the potentially malicious email—hopefully without clicking on any links—to the company's IT department, which then has to assess the message for malware and respond appropriately. This process can take days to weeks and is a drain on IT resources.

THE SOLUTION

NS2 offers two cyber defense solutions that can be used individually or together. 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. And GoSecure Inbox Detection and Response (IDR) automates email threat resolution in the user's inbox.

Endpoint and server security.

NS2's EDR solution 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. This approach monitors operations to identify evidence of criminal activity within the environment, including threats running in memory that have never been written to the disk memory of the system.

The program sends all gathered information to the GoSecure centralized threat analysis server—a central database of all behaviors that have been sensed in the endpoints. The centralized server uses predictive analytics with machine learning algorithms to sense anomalous behavior across endpoints. The GoSecure server has a breadth of visibility three times larger than the industry average and integrates with other leading tools in the enterprise.

EDR is made more effective with machine learning and predictive analytics to support the investigation and mitigation of threats—if it identifies a potential breach, it will cut off communication between the compromised endpoint and the rest of the network, and shut down the suspicious process.

One strength of connecting the endpoint sensors to the centralized analysis server is the ability to conduct real-time user behavior analysis—it can flag users that are copying files to a USB thumb drive, for example, or conduct continuous threat collection of malware behavioral data in a secure environment.

Inbox security.

NS2's IDR program empowers employees to securely report suspicious emails with the press of a single button. The potentially malicious message is then quarantined and routed to the GoSecure active response center, where it is investigated by the program and either returned to the user as valid or permanently deleted in just minutes. This seamless approach empowers employees to be part of the solution, not the problem, and automates a process that can be time consuming and a drain on organizational resources.

Once an email is submitted to the active response center, automated machine learning engines investigate the email for malware or suspicious links. The message is also routed to an IT analyst who can conduct their own investigation and confirm whether the message should be verified or removed. Real-time reporting of message analysis also allows the IT department to have a well-rounded understanding of the threats employees are encountering in their inboxes.

CONTACT US **info@sapns2.com** • **888 - 727 - 1468** • **sapns2.com/security/** • **sapns2.com/contact-us/**