



AVIGAIL OFFNER | DESIGN STUDIO

Portfolio 2024



Hello! :)

I am Avigail, a seasoned graphic designer and design lead with a rich background in assisting hi-tech companies and startups over the past 8 years. My expertise lies in guiding rebranding initiatives and addressing daily design requisites with precision.

My collaborative journey involves seamless coordination with marketing teams, product marketing specialists, and HR teams, ensuring a holistic approach to design solutions.

Specializing in Web Design, Graphic Design, Art Direction, and Print Design, I bring proficiency in tools such as Adobe Creative Suite (XD, InDesign, Illustrator, and Photoshop), Figma, Sketch, and Powerpoint, facilitating versatile and high-quality outputs.

My portfolio boasts collaborations with esteemed clients including Cyberproof, Silverfort, Panorays, Cynet, Imperva, Papaya Global, Cato Networks, Amdocs, CiValue, Indegy, Incapsula, VDOO, and many others.

Contact Info

avigailoffner@gmail.com

050-9495755

[linkedin](#)

www.avigailoffner.com

Brand Escort On-going Design Services

Comprehensive ongoing design solutions covering websites, social media and advertising materials, company documents, PowerPoint presentations, booths, and pavilions.

Web Design Process

Methodical approach initiating with Art Direction, followed by meticulous design development, and concluding with rigorous Quality Assurance (QA) processes.

Brand Refresh/Rebranding

Tailored services for creating Brand Books and Brand Styleguides, ensuring seamless adjustments of all design assets to align with a refreshed or rebranded identity.

Professional Collaborations

Strategic partnerships with pre-vetted professionals in complementary fields. Collaborative expertise includes messaging strategists, content writers, web developers, and animators, facilitating comprehensive solutions that seamlessly integrate with diverse design needs.



Search

Blog

Login

Panorays

Platform

Solution

Pricing

Resources

Partners

About

Start Free Trial

Get a Demo

Control Third-Party Cyber Risk

Seamlessly evaluate and manage your third-party risk from a single, unified platform.

Get a Demo

Risk Assessment

Risk Rating

False

Business Impact

External Assessment

83

Industry Range

Rating History

Security Questionnaire

40

Payoneer

cimpress

Gett

bob

QUANTUM

Taboola

AppsFlyer

ARVEST

UBS

walkme

Automating Third-Party Risk Management

Get comprehensive third-party risk ratings with security questionnaires, external attack surface assessments, and automated workflows.

Learn More

67

230/245 answered

616

Service Hosting

3.1 / 5 Is there an established incident management program that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the program?

Yes

No

N/A

Conversations

Me 1 day ago

How often is access reviewed for standard and privileged account?

Norm Peterson (Robotics AI)

3 minutes ago

We perform an annual review for privileged accounts

Type a message

TASKS COMPLETION

19/27 Task

70%

PROJECTED CYBER POSTURE RATING

67

Current

85

Projected

Enabling Trust Between Companies

Confidently onboard new suppliers and efficiently monitor changes to their cyber risk levels.

Learn More

Reducing Supply Chain Risk

Stay ahead of real-time threats and respond to cyber risk events with complete visibility across your entire digital supply chain.

Learn More

New Zero-Day Vulnerability Detected

6

16

23%

Your Company

Direct Suppliers

Indirect Suppliers

Impacted Companies

CVE-2022-24521: Windows Common Log File System (CLFS) Logical Error Vulnerability

3

26

1%

Your Company

Direct Suppliers

Indirect Suppliers

Impacted Companies

Breach

Critical 0-Day Bug Widely Exploited by Hackers

12

21

18%

Your Company

Direct Suppliers

Indirect Suppliers

Impacted Companies

Vulnerability

New Vulnerability Detected in Several Devices

2

16

0.5%

Your Company

Direct Suppliers

Indirect Suppliers

Impacted Companies

Cyber Posture

Commonality

Industry

71

73

88

50

Consulting

Computer Hard...

Internet Softwar...

Insurance

Transportation

Real Estate

Telecommunica...

Customers Across the Globe Rely on Panorays to Manage Third-Party Risk

“Panorays has definitely made our process more efficient. We get our deals done faster, we’ve improved our success rate, and we don’t need an expert to process documents...If there is a problem, I am told about it. If there’s no problem, then there’s nothing I need to do.”

TestFairy

Yair Bar-On
CEO & Cofounder, TestFairy

Read the Case Study

What We Deliver

+60%

Faster Third-Party Assessments

9 Days

To Onboard New Vendors

99.4%

Risk Rating Accuracy



Navigating Third-Party Security Risks in 2023:
Mid-Year Insights and Trends

[DOWNLOAD REPORT →](#)





The CISO's Guide to Third-Party Security Management

[DOWNLOAD GUIDE →](#)





The CISO's Guide

Third-Party Security Management



[Download Guide ↓](#)



The CISO's Guide to Third-Party Security Management

[DOWNLOAD GUIDE →](#)





10 Key Questions to Include in Your Vendor Security Questionnaires

[DOWNLOAD GUIDE →](#)





CISO's Guide to Evaluating Third-Party Security Platforms:
Top Questions to Ask

[DOWNLOAD GUIDE →](#)





RSAConference2023

We Get Third-Party Security. Done.

Meet us at RSA 2023

Booth 5272 North Hall
Expo Hall

BOOK A MEETING →



RSAConference2023

Panorays Name: _____

Lead First Name: _____

Company Name: _____

Phone Number: _____

Country: _____

Hot Lead?: ☐

Current process in place? Manual / Solution in place

If so, which solution: BitSight / SecurityScoreCard / OneTrust / UpGuard / Prevalent / RiskRecon / Whistic / CyberGRX / Other: _____

Authority: Influencer / Decision Maker

Who else should be involved: _____

Number of vendors: _____

Timeline: Urgent / 3 months / 6 months / Other: _____

Budget: Yes / No

Pain Points: _____

Next step: Nurture / SDR / AE

Lead Last Name: _____

Title: _____

Email: _____

State: _____



RSAConference2023

Thanks for stopping by the Panorays booth.

Leave us your business card
for a chance to win
a Meta Oculus Quest.






By giving us your business card, you consent to receive marketing information from Panorays. You can opt out at any time and can view our privacy policy at <https://panorays.com/privacy-policy/>

RSA
Conference™
2023

Meet with me at RSA 2023


Booth 5272 North Expo

LET'S TALK →



Dov Goldman
VP Risk Strategy










Meet Us At RSAConference2023

San Francisco | April 24-27 | Moscone Center

Panorays quickly and easily automates third-party security risk evaluation and management—handling the whole process from inherent to residual risk, remediation and ongoing monitoring. With Panorays, you can:

- Dramatically speed up your third-party security evaluation process
- Streamline collaboration and remediation between teams and suppliers, creating a transparent, efficient and effective process
- Eliminate the hassle of manual questionnaires in assessing third-party security
- Gain continuous visibility and actionable insights into evolving supplier risk

Automate, accelerate and scale your third-party security evaluation and management process today with Panorays.

Share:     


First name*

Last name*

Work Email*

Company Name*

Job Title*

Country* 

Phone number*

Anything else to share with us?

BOOK A MEETING

By clicking submit, I consent to the use of my personal data in accordance with Panorays [Privacy Policy](#). You can unsubscribe from emails at any time, and we will never pass your email on to third parties.




Inf0security Europe
20 - 22 June 2023, ExCel, London

Meet with Team Panorays

Infosecurity Europe 2023

Booth S65

BOOK A MEETING →



Meet Us At Infosecurity Europe

June 20 - 22, 2023 | ExCel London
Booth S65

Will we see you there?

Meet with a Third-Party Risk professional and learn how you can leverage Panorays to help your organization:

- Reduce risk
- Simplify third-party security management
- Improve your overall security posture

First name*

Last name*

Work Email*

Company Name*

Job Title*






Country* ▼

Phone number*

Anything else to share with us?

BOOK A MEETING

By clicking submit, I consent to the use of my personal data in accordance with Panorays [Privacy Policy](#). You can unsubscribe from emails at any time, and we will never pass your email on to third parties.

Share:     



Panorays Name: _____

Lead First Name: _____ Lead Last Name: _____

Company Name: _____ Title: _____

Phone Number: _____ Email: _____

Country: _____ State: _____

Hot Lead?: ☐

Current process in place? Manual / Solution in place

If so, which solution: BitSight / SecurityScoreCard / OneTrust / UpGuard / Prevalent / RiskRecon / Whistic / CyberGRX / Other: _____

Authority: Influencer / Decision Maker

Who else should be involved: _____

Number of vendors: _____

Timeline: Urgent / 3 months / 6 months / Other: _____

Budget: Yes / No

Pain Points: _____

Next step: Nurture / SDR / AE



Discover the benefits of partnering with Panorays.

Grab our exclusive on-site deal



Inf0security Europe
20 - 22 June 2023, ExCel, London

Let's Meet

Infosecurity Europe 2023

Booth S65



Matan Or-Ei
Co-Founder and CEO

Meet us at Infosecurity Europe 2023

June 20 - 22, 2023

Booth S65

BOOK A MEETING →



Come join us for happy hour

AT BOOTH S65

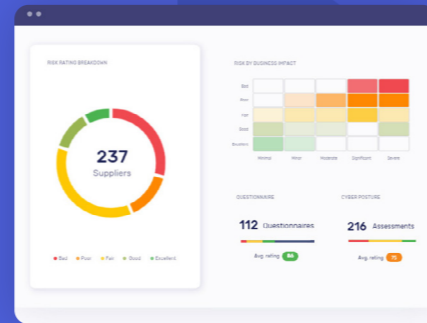
Monday, June 20 and Tuesday, June 21 3 - 5 pm





End-to-End Third-Party Cyber Risk Management

Take Control of Third-Party Cyber Risks



With third-party breaches composing nearly 60% of cyber events*, security teams are focusing on third-party risk management in order to detect, monitor and respond to digital supply chain threats. As businesses increasingly rely on cloud-based technology and SaaS applications, the threat landscape becomes more complex.

Panorays is changing the way teams do business together, making it safer and faster to onboard, evaluate, and monitor digital suppliers, from start to finish. Say goodbye to spreadsheets, tedious emails, and cyber uncertainties—with Panorays, you can confidently manage your entire third-party risk process from one unified platform.

Accelerating Third-Party Cyber Risk Management

Panorays enables trust between companies, allowing you to seamlessly evaluate new suppliers, continuously monitor all third and Nth party risks, and get a detailed view of your external attack surface.



Complete Visibility of Third-Party Risk

Make informed security decisions with all of the data you need to manage your third-party risks. From automated questionnaires to comprehensive external attack surface assessments and bottom-line risk ratings, Panorays gives you a detailed, contextualized view of evolving third-party risks.



Efficiency Without the Compromise

Seamlessly manage your third-party risks with automated, tier-based workflows, by prioritizing third parties based on inherent risk, and choosing the right process for each tier. With fully automated questionnaires and correlated insights emphasizing inconsistencies with cyber assessments, you can save time and focus your efforts where they count.



Reducing Exposure to Digital Supply Chain Attacks

From within the platform, you can easily collaborate to remediate security risks with your third parties, based on gaps identified in both questionnaires and external assessments. Confidently map out emerging threats with real-time alerts and view the impact of cyber events across your entire digital supply chain, allowing you to respond as needed.

+60%

Time saved to complete a
supplier's cyber risk assessment

9 Days

to onboard and evaluate a new supplier

99.4%

Risk Rating Accuracy

* [Forrester Report](#): Continued Uncertainty Forces Attention On Securing Relationships

Enabling CISOs with Confidence

Make informed decisions with complete visibility at your fingertips. From customizable reports to audit trails, Panorays enables CISOs to reduce third-party risks without the blind spots.



Executive Level Reporting

Present a full view of your third-party risk portfolio and make wiser security decisions with the data to back them up.



Compliance Across All Fronts

Ensure third-parties' compliance with regulations like NYDFS, CCPA, GDPR, and HIPAA with clear cyber risk metrics for both internal and external stakeholders.



Complete Visibility With Audit Trails

Be prepared for external and internal audits by tracking communication and remediation efforts between all teams.



Protecting From Third-Party Breaches

Decrease the likelihood of third-party breaches by monitoring your entire attack surface and taking immediate action to mitigate and respond as needed.

Panorays' End-to-End Process

Take complete control of your third-party security risk management process from prioritization to ongoing monitoring, remediation, and response.



About Panorays

We're on a mission to eliminate third-party security risks so that companies worldwide can quickly and securely do business together. With Panorays, our customers can easily manage, mitigate and remediate third-party security, reduce breaches, and ensure third-party compliance, resulting in efficient and effective risk remediation and improved cyber posture across the board.





Report

Navigating Third-Party Security Risks in 2023:

Mid-Year Insights and Trends



Executive Summary

In the dynamic business landscape where third-party relationships assume a critical role, organizations confront various risks that can profoundly affect their security and compliance requirements. Even amidst tough economic times, the crucial nature of these risks necessitates proactive management. This report unveils eye-opening statistics and trends that shed light on the pressing challenges and emerging strategies in third-party risk management. With 58% of companies managing over 100 vendors, 8% of which manage over 1,000, the need for a robust Third-Party Security Risk Management (TPSRM) process becomes abundantly clear.

Delve into this report to uncover key insights and discover how organizations prioritize third-party security, adapt to new regulatory compliance demands, and overcome obstacles to ensure a resilient and secure business ecosystem, regardless of economic conditions.

By the Numbers
Here are some of the study's key findings:

84%
of organizations prioritize third-party security risk management

44%
take three weeks or more to onboard a new third party

52%
find manual data collection and vendor communication cumbersome

Only 13%
continuously monitor their third parties' security risk

43%
have an insufficient view of 4th party vendor security risks

Background

In today's volatile economic climate, a critical challenge confronts businesses: the escalating risk of cyberattacks in the digital supply chain. As highlighted by Verizon's 2022 Data Breach Report¹, supply chain breaches are the source of a significant 62% of system intrusion incidents.

This report examines third-party security risks within the broader context of a strained digital supply chain. It synthesizes key insights from 2023 to provide an informed perspective on evolving trends and strategies in third-party risk management. This understanding is crucial for businesses seeking to secure their digital ecosystems against escalating threats.

¹Verizon's 2022 Data Breach Report

Methodology

The data and insights included in this report are based on an online survey that was conducted between February and April 2023 by Gatepoint Research. The survey garnered responses from 100 IT security executives representing various industries including senior decision-makers, with 30% holding CxO titles, 17% as VPs, 22% as directors, 20% as senior managers, and 11% as security analysts, architects, or engineers. All respondents participated voluntarily, with no engagement through telemarketing. The survey employed a structured questionnaire to gather insights, and the collected data was meticulously analyzed to provide accurate and comprehensive findings for this report.


Managing Third-Party Risk Is Top of Mind

In today's unstable economic environment, where businesses face escalating risks and vulnerabilities introduced by third-party relationships, the need for a delicate balance between cost-effectiveness and robust risk management becomes paramount. This pressing concern has propelled Third-Party Security Risk Management (TPSRM) into the top 10 risks, as revealed in [The State of Third-Party Security Risk Management Report in 2022](#).

84%

49%

\$4.3M



Guide

Managing Third-Party Security Risks with Maximized Efficiency

An end-to-end guide when budgets are tight.

Essential steps for an optimal TPRM end-to-end workflow | 5

Step 1

Prioritization

Map and classify third parties by inherent risk and criticality



The Problem
No single source of truth to manage all third parties' risks

- Working with multiple third parties, each with its own level of risk
- Managing a portion of your third parties in a TPRM platform and the remainder in a spreadsheet or other tool
- Inadequately managing lower-risk third parties
- Lacking a centralized solution to classify all third parties based on business impact

Real-Life Scenarios

- You want to add a third party to the system today and wait to do an assessment at a later date and time
- You don't want to waste time running assessments on third parties with minimal impact on your business (inherent risk) unnecessarily
- You want to add documentation to security controls of large corporations (like Google) who won't respond to your evaluation requests
- You'd like to add a third party with low business impact today, so as your company expands, you can automatically see its business impact increasing and then determine when and how to evaluate them



The Solution
TPRM platform as a single source of truth

- Evaluate and manage all third parties with varied risk levels in one platform, not just critical ones
- Get a full overview of third-party risk in your organization
- Use a risk-based approach and tier your third parties based on their impact on the business, choosing the appropriate evaluation process for each one
- Adjust the time and effort spent on evaluating each third party based on inherent risk



Once you have prioritized third parties by their inherent risk and selected the suitable approach for each, you can initiate the evaluation process.

Essential steps for an optimal TPRM end-to-end workflow | 4

Essential steps for an optimal TPRM end-to-end workflow

STEP 1 PRIORITIZATION

STEP 2 ONBOARDING AND EVALUATION

STEP 3 COLLABORATIVE REMEDIATION

STEP 4 CONTINUOUS MONITORING AND RESPONSE

STEP 5 OPTIMIZATION

Essential steps for an optimal TPRM end-to-end workflow | 9

Step 5

Optimization

Optimizing your TPRM program is crucial for effectively managing third-party risks. One key aspect of optimization is ensuring the flexibility of the tool used in refining your program and rating methodology. This flexibility allows you to adapt and fine-tune your approach as needed, aligning it with evolving industry standards and best practices. By continuously optimizing your TPRM program, you can enhance its efficiency and accuracy in assessing and mitigating risks associated with third-party relationships.

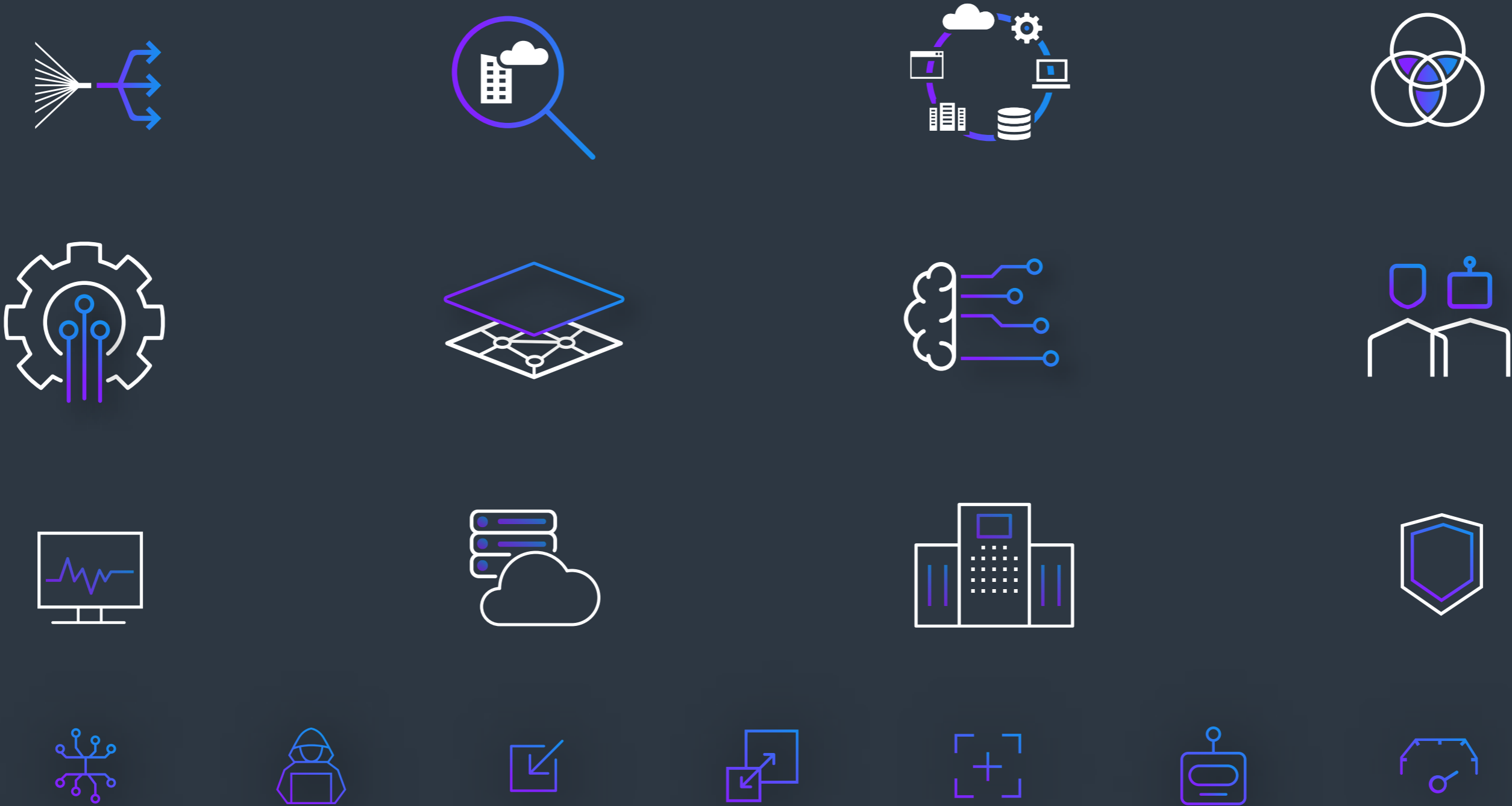
Summing Up

In conclusion, the modern era demands a robust and comprehensive approach to Third-Party Security Risk Management. Adopting an end-to-end process covering every aspect of the third-party lifecycle is crucial for effectively safeguarding your assets and business operations. By prioritizing Third Party Risk Management (TPRM) and continuously monitoring and reassessing your third parties, you can protect your reputation and stay ahead of evolving cyber threats.

By implementing the strategies outlined in this guide, you're empowering yourself to proactively identify, evaluate, and mitigate any security risks associated with your vendors, partners, subsidiaries, and other third parties. For companies with limited budgets, leveraging end-to-end tools becomes the preferred approach to managing TPRM effectively. By adopting the strategies outlined here and applying them to real-life scenarios, you can optimize your return on investment (ROI) while improving operational efficiency. Embracing the end-to-end TPRM process will not only enhance your organization's security but also bolster its resilience and pave the way for long-term success in the ever-changing landscape of cybersecurity.









Prevent Automated Propagation of Ransomware Attacks



How PassBleed Exposes On-Prem Workstations and Servers to Critical Risk



Service Accounts Likely Played a Key Role in the SunBurst Attack



Silverfort Proactively Prevents Exploitation of PrintNightmare Vulnerability





Silverfort Researchers Discover **KDC Spoofing Vulnerability** in F5 Big-IP



What is **Multi Factor Authentication (MFA)**?



Log4J Vulnerability Guidance



Ping Identity and Silverfort Unite to Deliver **Identity-Centric Zero Trust**

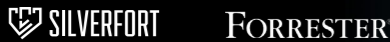


Webinar Series

Why Identity is a Crucial Component of Zero Trust Security

Part 1

Why Unified IAM
Visibility and Control
is Key for Zero Trust
Security

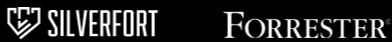


Webinar Series

Why Identity is a Crucial Component of Zero Trust Security

Part 2

The Importance of Risk Analysis
and Adaptive Policies in Zero
Trust Security

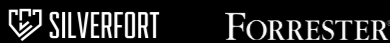


Webinar Series

Why Identity is a Crucial Component of Zero Trust Security

Part 3

Why Service Accounts and
Machine-to-Machine Access
Should be Part of Any Zero Trust
Initiative



Webinar Series

Why Identity is a Crucial Component of Zero Trust Security

Part 4

Enabling Cloud Migration with
Identity-Based Zero Trust





RETHINKING RANSOMWARE PROTECTION


It's the Propagation that Matters Most




THE ANATOMY OF RANSOMWARE ATTACKS

Ransomware attacks can be divided into three stages: **Delivery** of the ransomware payload to the target machine, **Execution** of the payload to encrypt or delete data files on the machine, and **Propagation** of the ransomware across multiple machines within the environment, to encrypt their data files as well.


DELIVERY




EXECUTION



PROPAGATION



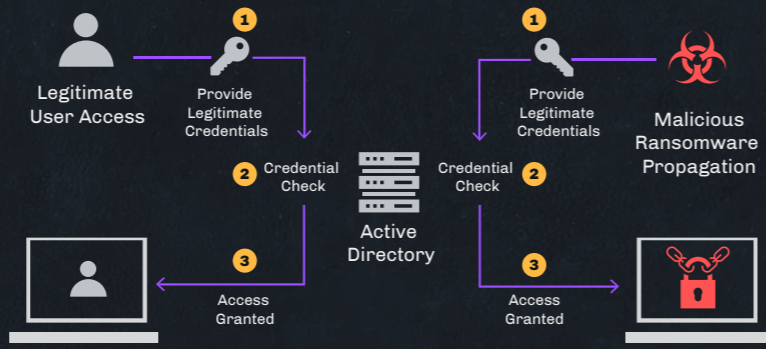


Rethinking Ransomware Protection | 4

WHAT MAKES PROPAGATION A BLIND SPOT?

In an enterprise environment, connecting from one machine to another involves the first machine providing Active Directory with a username and password. If these match, Active Directory approves the connection. Ransomware propagation is carried out by connecting to multiple machines with compromised admin credentials.

Since these credentials are valid, Active Directory treats it as a legitimate authentication and grants the ransomware access.



THE SILVERFORT WAY: UNIFIED IDENTITY PROTECTION PLATFORM

Silverfort Unified Identity Protection Platform integrates with all the Identity Providers (IDP) in the environment to perform continuous monitoring, risk analysis, and adaptive access policies on all access attempts, made by all users, to all on-prem and cloud resources.

In this way, access to resources is never granted based on credentials alone. Rather, the Silverfort's risk analysis determines whether or not to allow access, augment the authentication with MFA verification, or block the access attempt altogether.

Only Silverfort can enforce MFA protection on the command-line interfaces (PsExec, Powershell, WMI, etc.) that ransomware payloads utilize to propagate.





RE-EVALUATE YOUR MFA:

Are You as Protected as You Should Be?



MFA CHALLENGE #1: RELYING ON AGENTS & PROXIES

The dependency of MFA on either agents or proxies creates an inherent coverage problem

Traditional MFA solutions rely on either installing agents on protected machines, or on placing a proxy in front of a group of machines in a network segment. Both approaches inherently entail coverage gaps.

Agents

As a rule of thumb agents can never be deployed across 100% of the machines in a given environment. The larger the environment is, the more chances that there will be machines out of the deployment scope. Additionally, there are always machines you cannot install agents on due to various reasons.

Proxies

Gaining full MFA coverage using proxies requires placing a proxy in front of each and every network segment without any blind spots. This makes it practically an impossible task whenever the network topology exceeds the most basic levels of size and complexity.

The end result in both cases is partial coverage that leaves critical resources exposed to attack with compromised credentials without MFA protection.





Re-Evaluate your MFA | 4

AGENTLESS AND PROXYLESS ARCHITECTURE TO PROTECT ALL RESOURCES

Unify MFA on both cloud and legacy identity providers.
Eliminate the need for agents or proxies.
Gain centralized protection for all resources.

Enforcing MFA from the backend of all identity providers rather than on the individual resource means that MFA is applied to any resource that authenticates to a directory, regardless if it is a SaaS application, on-prem server, legacy system or any other. Apart from the operational simplicity entailed in managing only one solution, this architecture eliminates the need for agents and proxies, enabling full MFA coverage across all network, on-prem, and cloud resources in the hybrid environment.

MFA VERIFICATION PROCESS



PROTECTION OF ALL ON-PREM AND CLOUD RESOURCES





Re-Evaluate your MFA | 9

CHOOSE THE SILVERFORT MFA PATH THAT ALIGNS BEST WITH YOUR NEEDS

Replace

Use Silverfort MFA as the single MFA provider in the protected environment to protect all your on-prem and cloud resources. This provides both comprehensive protection and operational simplicity with a single interface to manage and configure all access policies to your resources without agents or proxies.

Add

Keep your existing solutions in place and implement Silverfort for the resources that couldn't have been protected before. While not reducing operational complexity, this would deliver immediate coverage to all the resources that are currently exposed and ensure end-to-end MFA protection in your environment.

Extend

Choose one of your MFA solutions as the prime provider and use Silverfort to augment your chosen solution's protection to all the resources it doesn't natively support. The common choice would be the MFA solution that already protects your SaaS applications. With this model, Silverfort would integrate with the current MFA service to challenge your users with MFA, providing them with consistent user experience regardless of what resource they attempt to access.



MFA #1



MFA #2



MFA #1





Re-Evaluate your MFA | 11

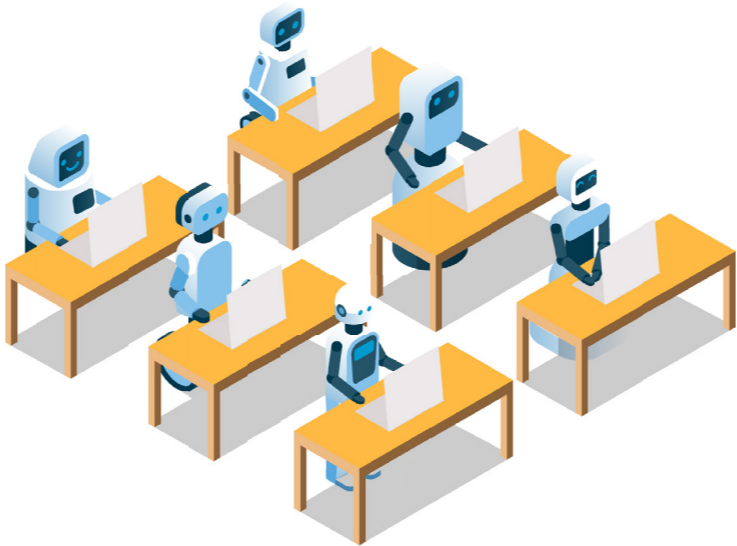
19



Intro - What are **Service Accounts**?

Service accounts, dedicated non-human accounts used by systems, applications, and services to interact with other systems, are an IT infrastructure basic. They perform scheduled actions automatically and repeatedly in the background, typically going totally unnoticed, and sometimes, forgotten about, by security administrators. There are countless service accounts in any given

organization and today, there are more than ever. The rise in Robotic Process Automation (RPA), or the use of AI to configure software "robots" to perform business tasks, that used to require the guidance of humans is increasing their popularity. Today, the number of these non-human accounts used by organizations, and the number of applications that rely on such accounts, is growing each day.



Since service accounts are scattered across the organization and used by various business applications (not by human users), they are typically forgotten about and left unsupervised. This means that nobody is tracking their use or validating that they aren't hijacked and used by malicious actors. What a great opportunity for adversaries!

Add to that the fact that domain level service accounts typically require elevated privileges and you make these accounts a prime target. Considering that too often, these accounts are over privileged - a result of the need to quickly implement business processes, makes them very valuable for hackers.

In the end, service accounts are left over-privileged and under-supervised.

You Can't Secure What You're **Not Aware of**

You might be sensing a problem here.

With hundreds or even thousands of these unsupervised, highly-privileged accounts running, they can become high-risk assets that, if left unchecked, may become a tool that enables threats to propagate throughout the network undetected. So these special accounts present an added set of risks, and in the process, create some very complicated challenges.

Here is a look at some of the problems created by service accounts:



ADMINS CAN'T KEEP TRACK OF THEM

Service accounts are used for implementing much needed business processes, often in a haste. This leads to improper documentation of these accounts. Overtime, the lack of documentation and staff turnover leads to lack of awareness of the service accounts in use and their dependencies.



PASSWORDS CAN BE A PAIN

Service accounts are often left with the same initial password with which they were created. This is obviously a bad security practice - their passwords should be changed regularly. However, that's not always easy to do. Domain service accounts require passwords to be changed at both the domain and application level, which requires a ton of planning, creating additional complexity. In some cases, the passwords are hardcoded into the application code which means you need to change the application code itself.



THE FEAR OF UNEXPECTED DOWNTIME

Often, admins don't remember, or know, what dependencies service accounts have and there is a concern that if changes are implemented incorrectly, applications may break.

Sounds like a recipe for disaster, right?

Leaving service accounts unmanaged and improperly secured allows attackers to make their way deep inside networks, move laterally undetected, and get their hands-on critical data.



strattic

Ultimate Static WordPress Security

Strattic's static and headless approach to hosting and deploying WordPress eliminates virtually the entire attack surface used to attack WordPress sites.



Static, headless security for WordPress makes WordPress vulnerabilities irrelevant

Static websites deployed by Strattic offer the highest level of security by separating the live static website from the WordPress backend. This approach ensures that common web application attack vectors simply don't exist on the production, static replica of the WordPress site and become irrelevant.

The many layers of WordPress vulnerabilities

WordPress websites have a lot going on, with multiple layers where vulnerabilities can occur: starting from the operating system, moving up to the MySQL database and PHP, and of course in the dozens of third-party WordPress plugins installed in the average site, and the WordPress core itself.

Hackers use common and constantly changing methods of attack including Remote Code Executions, Remote and Local File Inclusions, SQL Injections, DDoS, Social Engineering, Session Hijacking, Man-in-the-Middle, XSS (Cross-site scripting), Brute Force and more.

And since more than 70% of WordPress sites are vulnerable to attack at any given time, and because WordPress is Open Source, vulnerabilities and bugs are publicized and known not only to site owners, but also to malicious actors who use this information to target WordPress sites and breach them.

These are the hard facts

- WordPress websites are a top target for hackers because of their massive user base and number of plugins.
- More than 70% of WordPress installations are vulnerable to hacker attacks.
- Hundreds of thousands of WordPress installations are hacked annually.
- Online threats have increased by as much as 6x their usual levels due to the global pandemic.
- 47% of all hacked websites were left with at least one backdoor, guaranteeing an imminent repeat attack.

The diagram is divided into two main sections: 'Traditional WP' and 'Strattic'.

Traditional WP: This section is labeled 'Attack Surface'. It shows a 'WP Database' at the top, connected by a double-headed arrow to a server stack below. The server stack is labeled 'Commonly Vulnerable' and contains 'Apache', 'PHP', 'WP', and 'WP Plugins'. Below the server stack, two icons represent an 'Attacker' and an 'End User', both with dashed arrows pointing to the server stack.

Strattic: This section is divided into two parts: 'Isolated' and 'Public Facing'.
 - **Isolated:** This part shows a 'WP Database' at the top, connected by a dashed arrow to a 'Fully Isolated' container. Inside the container is a stack of 'Apache', 'PHP', 'WP', and 'WP Plugins'. A red arrow labeled 'One Way Publishing' points from this container to the 'Public Facing' section.
 - **Public Facing:** This part shows a stack of 'HTML', 'CSS', and 'JS' files, labeled 'Static Files in S3 bucket'. A red arrow points from this stack to an 'Amazon CDN' oval. Below the CDN, two icons represent an 'Attacker' and an 'End User', both with dashed arrows pointing to the CDN.

strattic

Convert Your WordPress Site to Static in One Click

Boost your WordPress site with the security and speed of Strattic

Optimizing websites that run on WordPress can be time-consuming and frustrating. For website owners, it can be an ongoing battle to stay ahead of hacker bots, keep performance high, and scale for campaigns.

That's why we created Strattic, the all-in-one platform that instantly optimizes WordPress websites by converting them to static in one click, and delivering them on a headless architecture. By converting WordPress to static and headless, site owners get the best of all worlds: the power and usability of WordPress combined with the speed, security and scalability of a modern static architecture.

Marketing and Tech Teams Both Love Strattic

Marketers can continue to use WordPress as they always have, and benefit from the familiarity and extensibility of the world's most popular content management system.

Technologists know that the WordPress site is fully protected in a containerized environment, while the static production site is delivered quickly and securely via CDN.

Strattic's revolutionary hosting

- ✓ Removes 99.9% of vulnerabilities, including SQLi and XSS
- ✓ Can increase your website speed by up to 5000% (yes, really!)
- ✓ Leverages a global network of CDNs so your site is fast and available everywhere, always scaling to serve any amount of traffic
- ✓ Includes many built-in features that emulate standard WP dynamic functionality (search, forms, 301 redirects and more) so your site works perfectly as static

Discover the security, speed, and scalability of Strattic

"Migrating our WordPress websites from our previous hosting to Strattic immediately increased our site speed significantly. This contributed to lowering our bounce rate, increasing our conversion rates, and also helped improve our SEO."

Jonny Steel, Payoneer

Experience the Strattic difference for yourself. [Try Strattic free for 30 days.](#)

RESIDENT

HoneyBook

OCHA

Big Orange Heart.

Coralogix

Payoneer






Fast. Secure. Reliable.

Learn how to easily convert your WordPress sites to static websites.


Get the Guide



Fast. Secure. Reliable.

Learn how to easily convert your WordPress sites to static websites.

Get the Guide









Kiss website downtime goodbye!

Learn More



Kiss website downtime goodbye!

Learn More



**All the benefits
of Jamstack,
for WordPress.
In one click.**



1

**Migrate your
WordPress site
to Strattic.**



2

**Use WordPress as
usual to manage
content and
modify your site.**



3

**Click Strattic's
publish button
in the WP
admin.**





CyberProof®
A UST Company

FORRESTER INFOGRAPHIC

What are the key strengths and weaknesses of MDR providers?

LEARN MORE →

MDR vendor strengths and weaknesses

Competent teams, empathy during service delivery, and speed of detection were the three strengths customer references mentioned about their MDR providers. While the strengths directly outweighed weaknesses, customer references identified price, access to data, and limited visibility as areas for improvement.

CyberProof®
A UST Company

Las amenazas evolucionan constantemente

¿Puede tu SOC seguir el ritmo?

MÁS INFORMACIÓN →

CyberProof®
A UST Company

Protect Your Assets as you Migrate to the Cloud

by Ensuring your XDR Solution Features these Four "Fantastic" Superpowers

READ NOW →

CyberProof®
A UST Company

Learn more about CyberProof

Build a Smarter SOC with Us

Proactive Detection and Intelligent Automation

SPEAK WITH AN EXPERT →

CyberProof®
A UST Company

Versetzen Sie sich in die Lage eines Ransomware-Attackers

Laden Sie den Bericht herunter →

CyberProof®
A UST Company

Cloud-native XDR superpowers

Make sure your strategy includes all 4

LEARN MORE →

CyberProof®
A UST Company

eBook

Reduce cyber risk
across your estate
with MDR

DOWNLOAD NOW →

CyberProof®
A UST Company

Migrating to
cloud-native
threat detection
and response

CyberProof®
A UST Company

eBook

Secure the critical
areas of your estate
with MDR

DOWNLOAD NOW →

How the CyberProof Log
Collector can help

The CLC improves the flow and handling of data, aggregating
Microsoft Sentinel's predefined rules and capabilities to provide
customers with automated and consistently updated threat detection
capabilities. This new, cloud-native threat detection and response
solution is designed to help organizations secure their critical areas
of their estate. The CLC is a powerful tool that can help organizations
secure their critical areas of their estate. The CLC is a powerful tool
that can help organizations secure their critical areas of their estate.
The CLC also works with any programming language, including
Python, JavaScript, .NET, etc.

The CLC reduces costs by more than
40% due to the filtering of log data and
routing of less relevant data into a cost-
effective, cloud-native storage solution.

CyberProof®
A UST Company

We're hiring!

XSOAR Engineer

Location: Spain

LEARN MORE →



CyberProof®
A UST Company

How malicious actors
bypass geolocation bans

READ THE REPORT →

CyberProof®
A UST Company

CYBER THREAT INTELLIGENCE (CTI)
RESEARCH REPORT
A Deep Dive into Attacker-
Controlled Infrastructures

OCTOBER 2022

Identifying the
perceptions of
the threat actors
is a key to
understanding
their behavior.
This report
explores the
perceptions of
the threat actors
and how they
bypass geolocation
bans. The report
also includes
a list of the
top 100 malicious
IP addresses
and a list of the
top 100 malicious
domains.

CyberProof®
A UST Company

We're hiring!

XSOAR
Engineer

Location: Spain

LEARN MORE →




CyberProof®
A UST Company

We're hiring!

XSOAR Engineer

Location: Spain

LEARN MORE →



CyberProof®
A UST Company

How nation-state
actors bypass
geolocation bans

DOWNLOAD THE REPORT →

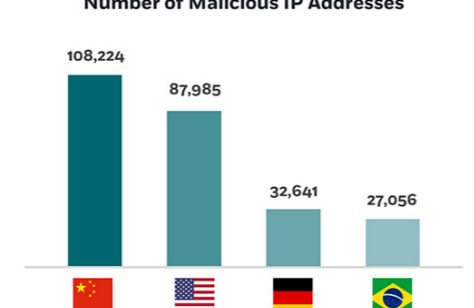
Number of Malicious IP Addresses

108,224

87,985

32,641


27,056



CyberProof®
A UST Company


Getting the most from your EDR
technology

WATCH ON-DEMAND →




EDR Lead,
CyberProof

ARIK DAY



Sr. Solutions architect,
CyberProof

NILS HAZA



Product Marketing Manager,
CyberProof

BEN CHANT

CyberProof®
A UST Company

January 12, 17:30-20:00

Join me!

I'm speaking at CyberProof's
Tel Aviv meet-up:
Securing the Future

Nir Aharon
DFIR & Threat Hunting, CyberProof



CyberProof®
AUST Company

CASE STUDY:

IT & OT security services
for a multinational
chemicals company

INDUSTRY: ENERGY

cyberproof.com

Client background

The client is a multinational specialty chemicals company that operates in many countries worldwide. It is focused on four business sectors: care chemicals (consumer and industrial); catalysis; natural resources (oil & mining, minerals); and plastics & coatings.

Client challenge

The client was looking for a strategic cyber security partner to provide comprehensive monitoring of security operations 24/7, accelerate the organization's detection and response capabilities, and help mitigate the business impact of potential cyber attacks. The client sought a hybrid delivery model aligned to their roadmap.

They wanted a partner that could work collaboratively with them and provide the full portfolio of security services – to measurably reduce risk and future-proof their defenses.

Our solution

The client chose CyberProof as its strategic cyber security partner for the next five years. CyberProof is running the client's next-generation SOC – and is providing an entire suite of cyber security services that are delivered from Spain, Israel, and India, covering:

- Security Monitoring and Response
 - Security Information and Event Management (SIEM) Operations
 - Digital Forensics and Incident Response (DFIR)
 - Threat Intelligence & Threat Hunting
 - Endpoint Detection & Response
- Vulnerability Management
 - Firewall Management
 - User & Entity Behavior Analytics (UEBA)
 - OT Security

Benefits

- Collaborative and transparent security service
- 360° portfolio to cover all security needs from IT to OT
- Competitive commercial model
- Proximity to client's SOC

CyberProof®
AUST Company

Cloud-scalable
Threat Detection and
Response services

Pre-integrated with Microsoft Sentinel
and Defender for Endpoint

cyberproof.com

CLOUD-SCALABLE THREAT DETECTION AND RESPONSE SERVICES

Security teams are struggling to reduce the time to detect and respond due to the complexity and volume of alerts being generated from multiple security technologies. Migrating to the cloud also brings an additional perimeter which requires constant vigilance for early signs of a cyber attack.

To help solve these challenges, CyberProof has partnered with Microsoft to provide cloud-scalable security monitoring, threat detection and response services across your IT estate.

Reducing alert fatigue and speeding up detection and response

Our proprietary service delivery platform, the CyberProof Defense Center (CDC) Platform, uses Automation, Orchestration and Collaboration features to:

- Provide a single view of security operations
- Speed up detection and response capabilities
- Facilitate real-time communication with our nation-state level analysts to help remediate incidents

Harnessing Microsoft Sentinel's cloud-native SIEM – without overhead

Microsoft Sentinel is pre-integrated with the CDC Platform, so customers can see value straight away by dramatically reducing the number of alerts while automating SOC tier 1 and 2 activities such as alert enrichment, escalation, investigation, containment and remediation.

Hunting and response with Microsoft Defender for Endpoint (MDE)

Our EDR engineers can set up, configure and manage MDE platforms on behalf of our clients. Our CDC platform integrates with MDE to act as a single interface for providing 24x7 advanced threat detection, hunting and response services.

KEY FEATURES

- 24x7 monitoring, alert triaging and investigation, freeing up your team to focus on high priority activities
- Machine Learning and Behavioral Analysis can reduce alert fatigue by up to 90%
- Large-scale collection and correlation of data from endpoint, cloud, network and identities for high-context alerts
- Increase your SOC team's efficiency by leveraging our CDC platform's automation and orchestration capabilities
- Agile development and optimization of Use Cases to continuously adapt to the latest threats
- Proactive threat hunting using IOC retrohunting, intelligence from our CTI team and behavioral analysis techniques

OUR SERVICES

- Security Event Monitoring
- Managed Detection and Response
- Managed Endpoint Detection and Response
- Advanced SOC Services
- Agile Use Case Management
- Security Platform Management

KEY OUTCOMES

Single View of Security Operations: The CDC is preintegrated with Microsoft Sentinel and Defender for Endpoint to provide a single pane of glass.

Shorter Detection & Response Time: Next-generation SOC capabilities drive operational efficiency and dramatically reduce the cost and time required to respond to security threats.

Dashboards & Reporting to Measure Risk: The CDC supports tailored risk scoring and operational dashboards & reporting – providing insights for internal and multi-layer customer stakeholders and for compliance purposes.

CLOUD-SCALABLE THREAT DETECTION AND RESPONSE SERVICES

SERVICES ARCHITECTURE

How we transition you to a smarter SOC

Discover & Plan

- Understand your business goals, security objectives and the maturity of your current SOC processes
- Identify and document a transformation plan to modernize your security's operational capabilities

Onboard & Enable

- Set up Microsoft Sentinel and Defender for Endpoint in line with a plan for people, process, and technology
- Connect to existing or new Microsoft solutions (Microsoft Defender for Cloud, Sentinel applications, etc.) and other cloud, on-prem, or hybrid environments

Migrate & Transition

- Connect Microsoft Sentinel and Defender for Endpoint to the CDC platform to have a single interface for managing security operations
- Configure custom detection rules, use cases and playbooks to automate Tier 1-2 tasks and speed up detection and response

Operate & Manage

- Provide continuous Security Event Monitoring, Threat Detection & Response services
- Monitor and enrich security alerts and triage issues – investigating incidents and supporting with remediation and recovery activities
- Create customized dashboards and reporting as well as actionable threat intelligence on targeted threats

Why CyberProof

- Recognized as "leader" by Forrester in the midsize managed security services market
- Our virtual analyst bot significantly reduces human effort
- Use Case Factory continuously improves your defenses
- Flexible, hybrid engagement model for a true partnership
- Our platform facilitates collaboration and provides transparency
- Have delivered the largest and most complex deployment of Microsoft Sentinel in the world

Case Studies

CyberProof®
AUST Company

Top Malware
Trends to Watch
in 2023

cyberproof.com

TOP MALWARE TRENDS TO WATCH IN 2023

2022's arrival was plagued by multiple events including the ongoing COVID-19 pandemic and the inception of the Russian-Ukrainian conflict. These events were coupled with a flurry of high-profile cyber-related threats – with widespread Log4Shell and Follina exploitations chief among them.

Threat actors keep up with current events and advancements in technology and leverage the opportunities they represent. Alongside more methodical and calculated approaches that attackers take, they also incorporate current events into campaigns and attack chains.

While many types of attackers fall under the ever-blossoming threat actor umbrella, this eBook, based on data collected by the CyberProof Cyber Threat Intelligence (CTI) team, seeks to take a focused snapshot of the malware-related threat landscape from January to July 2022. Its aim is to attempt to analyze malware usage and trends as observed through the lens of a CyberProof analyst whose objective is to provide threat intelligence solutions to enterprise clients.

Alongside more methodical and calculated approaches, attackers also incorporate current events into campaigns and attack chains.

cyberproof.com

TOP MALWARE TRENDS TO WATCH IN 2023

MITRE tactics

The MITRE techniques that were used were related to the following tactics:

- 21% of MITRE techniques used were related to Execution
- 16% pertain to Privilege Escalation
- 16% are related to Defense Evasion

TOP TACTICS RELATED TO THE MITRE TECHNIQUES THAT WERE USED

A comparative analysis of data collected in previous years highlights an interesting trend:

In comparison to data collected by external sources in 2020, there was a large uptick in Scheduled Task usage, alongside a decrease in the volume of malware attacks using Process Injection, in the first half of 2022.

Interestingly, PowerShell exploitation has remained relatively consistent and is constantly being observed in attacks.

cyberproof.com

TOP MALWARE TRENDS TO WATCH IN 2023

Unraveling the adversaries' motivation – User Execution

Now that we've laid out the top MITRE techniques used this year, we can attempt to understand why they were the most popular.

First, let's explore why malware was used most often for execution purposes. This notion is supported by several pieces of evidence:

WIPER MALWARE

Harnessed by threat actors hellbent on data destruction – is the most prominent type of malware utilized in the Russia-Ukraine conflict.

APT GROUPS

Advanced Persistent Threat (APT) groups have had the most individual malware strains attributed to their use. Seeing as these groups are acting to achieve a larger goal, their endgame usually culminates in user execution.

UNATTRIBUTED ATTACKS

Completely unattributed attacks – the "average Joes" of malware attacks – are most likely to have no ulterior motives save for user execution.

eBooks

29

CyberProof

A UST Company

12

Questions for Security Leaders in 2023

Based on Forrester's latest privacy report

DATA COVERAGE REPORT

The State Of Privacy And Cybersecurity, 2022

November 8, 2022

By Scott Branson, Head of Data, Privacy & Security, CyberProof, with Benoit van der Kamp, Director of Privacy, CyberProof

Executive Summary

Summary

Executive Summary



Infographics

CyberProof

A UST Company

Cyber Defenders Playbook 2023

Real-life examples that will empower your security teams

SCENARIO 1 | BLACKCAT RANSOMWARE INCIDENT

5

Scenario 1

BlackCat ransomware incident

Most of the incidents described in this report were written from the perspective of the Security Operations Center (SOC) team and illustrate effective collaboration of teams having different types of expertise. This incident, however, was written from the perspective of the DFIR team and it focuses on demonstrating "Best Practices" regarding incident management.

Teams involved

| Team | Description |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| CTI | <ul style="list-style-type: none">Insights and EnrichmentOSINT and WEBINTIOC Collection & Analysis |
| Threat hunting | <ul style="list-style-type: none">Identify Additional Infected AssetsLeverage IOA to Locate Infection |
| L1 analysts | <ul style="list-style-type: none">Initial Response & TriageMonitor Security Perimeters and CDC Alerts |
| DFIR | <ul style="list-style-type: none">In-depth InvestigationResolve Key Investigation Questions |
| Managed EDR | <ul style="list-style-type: none">Add IOA as Behavior Rules |
| Vulnerability Management | <ul style="list-style-type: none">Patch Relevant Vulnerabilities |

L1 initial response & triage

CyberProof's Security Operations Center (SOC) received hundreds of alerts in a short period of time regarding the detection of a BlackCat ransomware attack on one of CyberProof's clients. The L1 team started to investigate the suspicious alerts: CyberProof's managed EDR was able to prevent the execution of two malicious files, but the L1 team escalated the severity to a critical level after they realized that large numbers of assets were encrypted.

SCENARIO 1 | BLACKCAT RANSOMWARE INCIDENT

6

(This problem was due to legacy EDR agents, which were managed by another vendor and had not been updated to their latest security version.) The team received additional alerts regarding behavior across the environment, which was indicative of infection.

Based on the above, the L1 team confirmed with the L2 team that the client was faced with an active ransomware infection – and escalated the incident to the DFIR teams.

Managing incident response

As soon as the incident was confirmed as representing an active intrusion, the DFIR team assigned the incident an Incident Manager. The Incident Manager role:

- Leads the investigation and the collaboration to respond quickly and efficiently to the incident; must have a broad view of all tasks related to the incident.
- Maintains full involvement in the actual investigation – understanding the "Big Picture," governing incident handling, validating the forensic evidence, and agreeing on its context within the investigation.
- Is present in all meetings with the client's stakeholders, and provides an incident timeline, updates and description of tasks conducted by CyberProof.
- Communicates confirmed forensic information to the client's stakeholders involved in the incident.
- Focuses on multiple tracks to quickly resolve open questions, assigning different analysts to solve specific questions.

Figure 1: Managing incident response

SCENARIO 1 | BLACKCAT RANSOMWARE INCIDENT

9

Track 3: Containment

The Threat Hunting and Managed EDR (MEDR) teams participated in containment processes with the aim of identifying non-contained, infected hosts and installing managed EDR agents on all environments. Their work involved the following steps:

- By leveraging what had already been learned about the behavior of the attack, the threat hunting team queried and found more than five infected endpoints that had not been contained, due to an inactive EDR agent. CyberProof reached out to the client's IT team and together, the endpoints were isolated.
- CyberProof's MEDR team assisted the client with EDR deployment on legacy assets, guiding the deployment process and providing recommendations for configuration.
- After the incident was contained, the threat hunting team conducted proactive queries to identify lateral movement (such as RDP connections or SMB shares) and to detect activity disruption of EDR or other security products. No additional artifacts were found.

Our recommendations:

- Deploy EDR on all environments.
- Don't fully trust security products to contain all infections.
 - Learn the behavior of an attack (all IOCs, all IOAs, all used tools, all MITRE techniques) and hunt for it throughout the rest of the environment. This helps identify additional infected endpoints and validates the environment's integrity.
 - During an incident, make sure the threat actor did not tamper with security products.
- EDR is not the only tool for containment. You can also:
 - Use GPO to deploy a local Firewall policy.
 - Use the Firewall to create an isolated VLAN to contain all infected endpoints.
 - Disable RDP connections or SMB shares during incidents.
 - Remove the ability for departments to communicate during live incidents.

SCENARIO 1 | BLACKCAT RANSOMWARE INCIDENT

11

Our recommendations:

- In situations involving engagement with threat actors, don't trust the data they show you. Validate the authenticity of the "stolen" files.
- Conduct an investigation of data exfiltration since the time of initial access.
- Monitor the dark web for any mentions of data leakage on regular basis.

Track 6: C2 architecture to support the attack

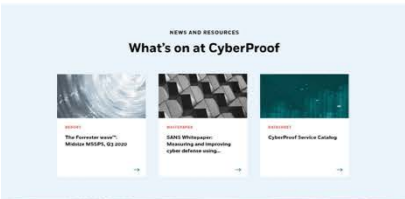
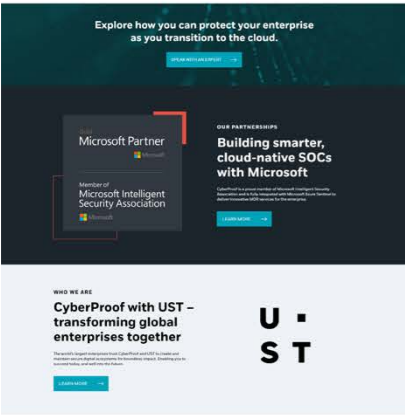
The CTI team investigated the C2 architecture with the aim of providing leads for the investigation. Their work involved the following steps:

Figure 2: C2 architecture to support the attack

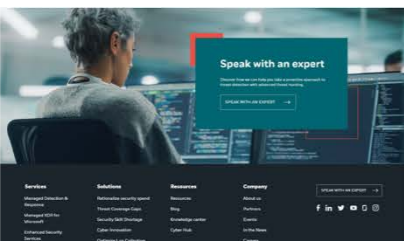
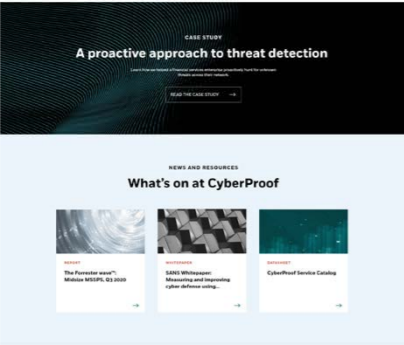
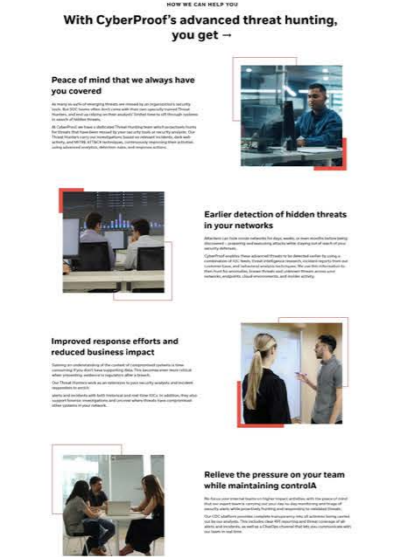
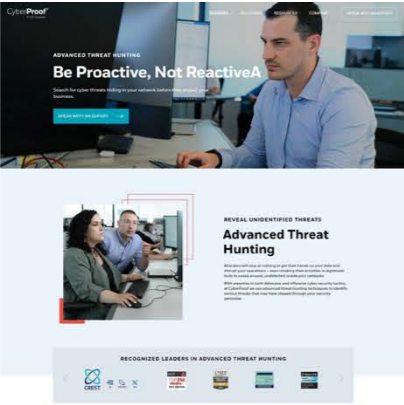
- The CTI team identified that the ransomware's C2 domain had been registered via private registrant 4 days before the attack was initiated on the environment. A day before the attack, the threat actors deployed HTTP services and opened ports 80 and 8081 in the malicious C2 address.
- Two days after the mass encryption, the threat actor removed all services in the malicious C2 address. It seems that the threat actor attempted to destroy evidence of the C2 architecture.

Playbooks

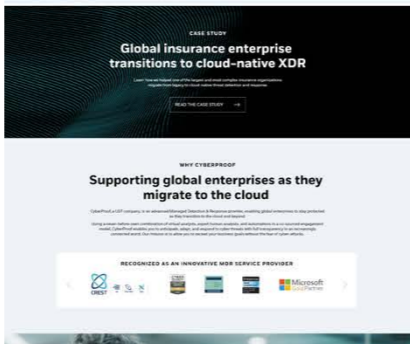
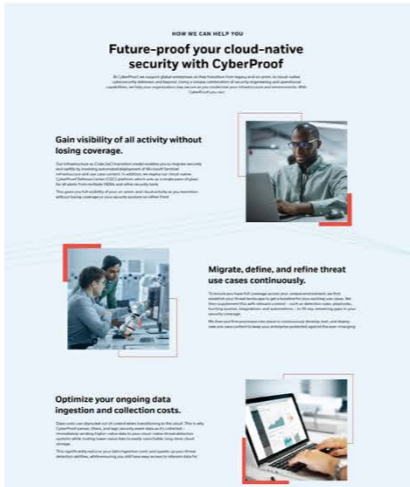
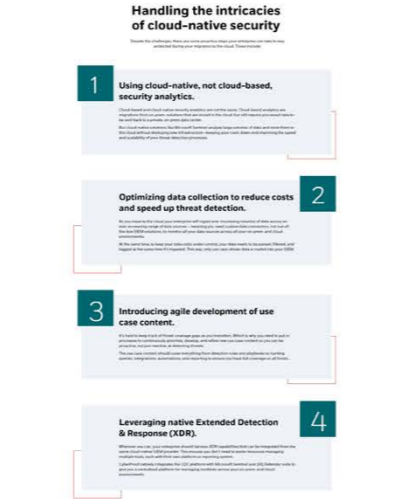
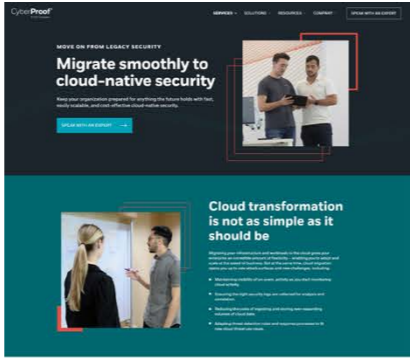
Homepage



Service Page Template



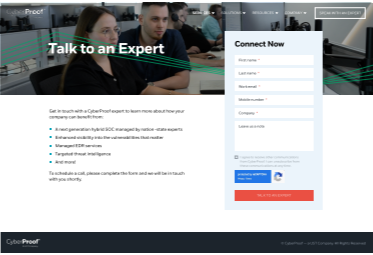
Solution Page Template



Case Study Page Template



Contact Us

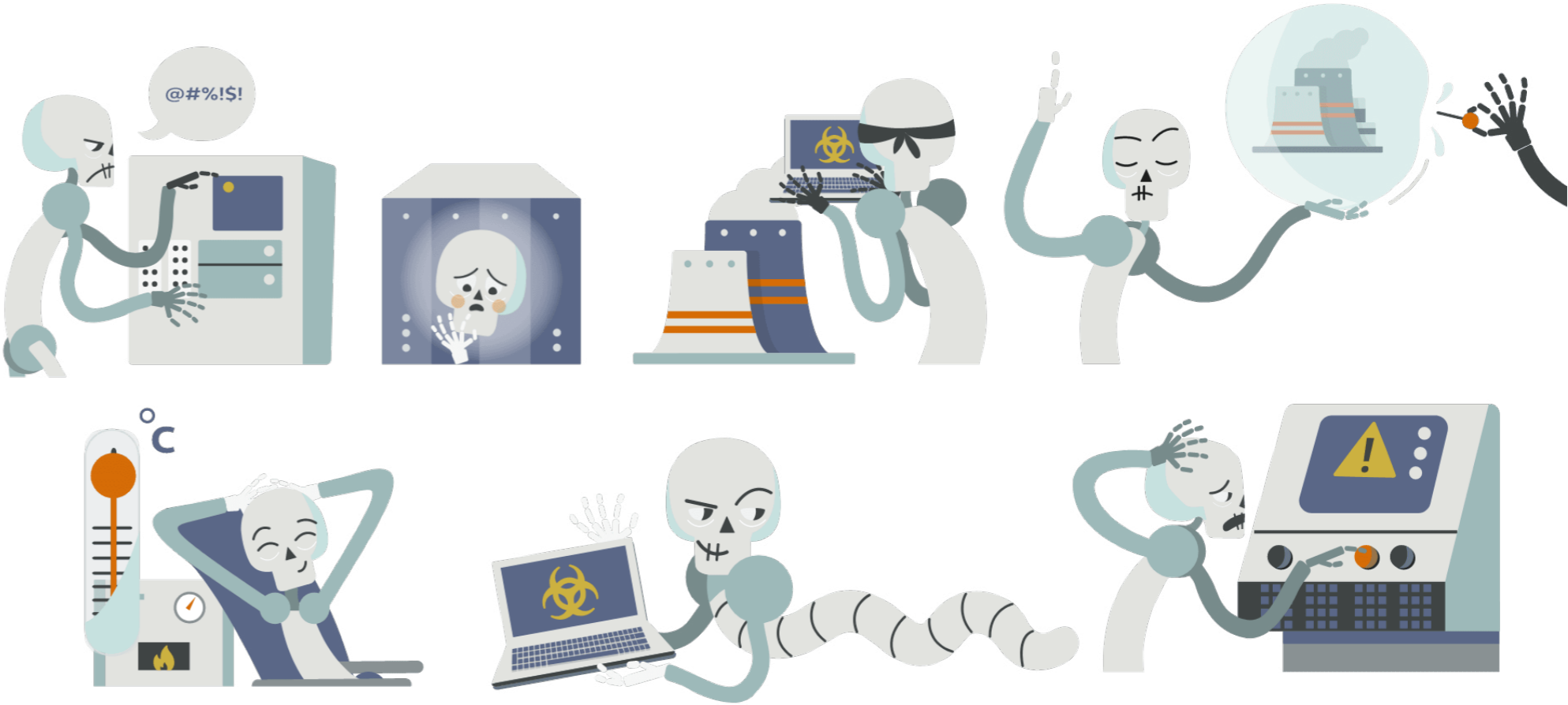
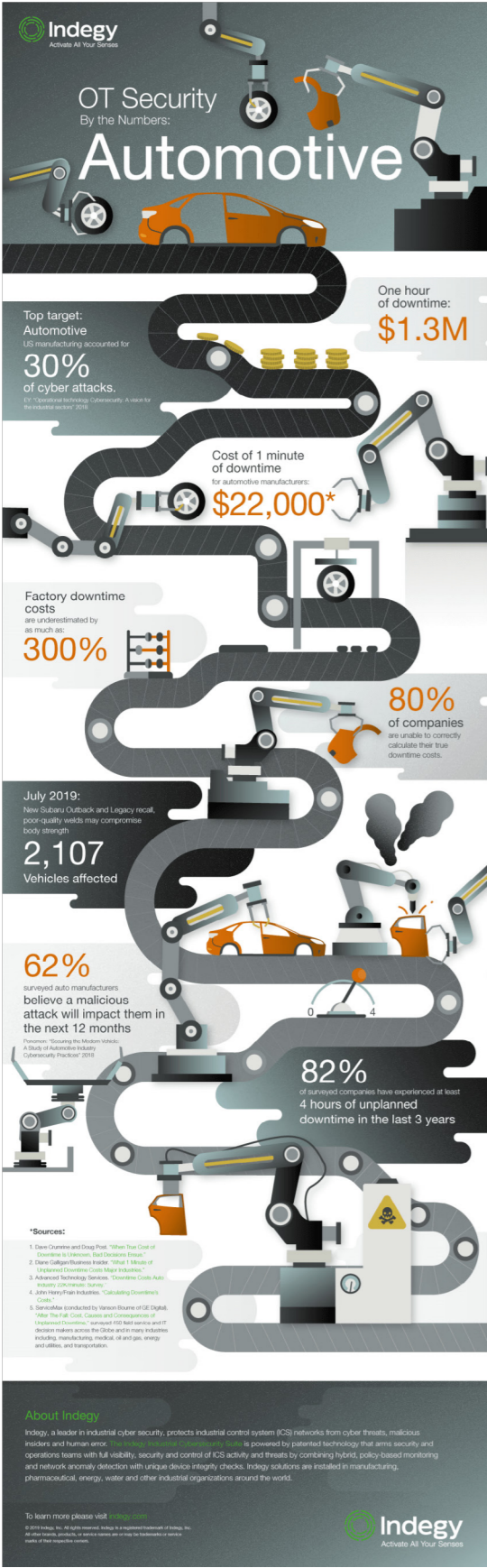















Products & TechnologySolutionsPartnersResourcesCompanyRequest a Demo


Indegy Device Integrity

Take an active role in securing your industrial environment with Indegy's patented technology

Request a Demo

Assembly Line 7
15.10.10.78
Type: Robot Controller
Family: Fanuc
Traffic: 129.8 MB
Firmware: 4


Substation Relay Control
10.10.10.50
Type: RTU
Family: SEL
Traffic: 234.4 MB
Firmware: 2.4



Indegy Industrial Cybersecurity Suite

Experience what complete visibility, security and control of your industrial environment can do for your organization


Request a Demo



ICS Cybersecurity Architecture

Resilient end-to-end solution architecture that helps ensure complete situational awareness with maximum flexibility for your entire ICS-based infrastructure


Request a Demo



Managed Security Monitoring Service

Through our worldwide partner network gain unparalleled security monitoring resources to proactively safeguard your OT environment, identify risks and swiftly respond to potential threats


Request a Demo



Industrial Cybersecurity for Power & Utilities

Securing the journey towards more efficient and resilient electric and water utilities


Request a Demo



Indegy Enterprise Manager

Single pane of glass for centralized visibility and management of your multi-site Indegy Industrial Cybersecurity Suite deployment


Request a Demo



ICS Asset Inventory Management

Enjoy the benefits of a complete, detailed and automated asset inventory for your ICS environment

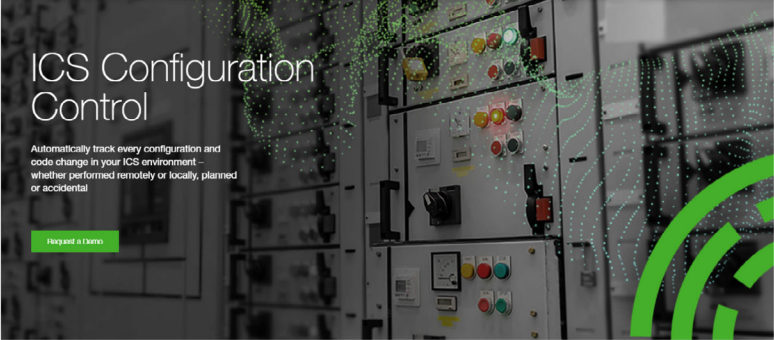
Request a Demo



ICS Configuration Control

Automatically track every configuration and code change in your ICS environment - whether performed remotely or locally, planned or accidental


Request a Demo



Industrious Partners

Industrial Security Expertise. Transformative Results.

Become a Partner



37



START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Cynet Ransomware Prevention

Cynet provides the most thorough ransomware protection available: Multiple layers of detection, Immediate response actions, all backed by a 24/7 MDR team

Request a Demo →

START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Cynet Centralized Log Management

Quickly uncover hidden threats with full visibility into your log data

Request a Demo →

START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Cynet Deception

Easily configure decoy files, users, hosts, and networks to expose malicious actors who have gained access to your environment

Request a Demo →

START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Security & IT Operations

Cynet includes the IT & Security Operations tools you need to reduce your attack surface, shorten incident response times, and improve your company's overall security posture.

Request a Demo →

START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Cynet Network Detection and Response (NDR)

Cynet network detection and response layer discovers and eliminates otherwise invisible threats

Request a Demo →

START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Cynet Next-Gen Antivirus (NGAV)

Cynet Next-Gen Antivirus automatically stops ransomware, fileless malware and zero-day exploits

Request a Demo →

START FREE TRIALBLOGUNDER ATTACK?LOGIN

cynet

XDR PLATFORMSERVICESPARTNERSRESOURCESCOMPANYREQUEST A DEMO

Cynet User Behavior Analytics Rules (UBA)

Cynet UBA security layer monitors user behavior to spot and isolate compromised accounts

Request a Demo →



Thanks