Bravura Security

An IAM & PAM Industry Guide to Ransomware:

A Winning Defense with Zero Trust

E-BOOK

The State of the Market: Ransomware-as-a-Service

$20 billion. That's the cumulative cost of ransomware global attacks in 2020. It's a staggering number, more than double what it was in 2019.[1].[2]

Cyberattacks increased in number and complexity across the board but none more than ransomware, and industry analysts only expect them to continue to grow more so in the coming years.[2] The rise in these attacks has even produced a niche offering among hackers — ransomware as a service (RaaS) — essentially building an easy-to-implement service for hackers to use and quickly (but effectively) launch these attacks. But as advanced as the attacks may get, the avenues by which cyber criminals access systems remain surprisingly simple. They find easy exploits in dormant accounts, poorly managed passwords, and mismanaged privileges. And what these critical attack vulnerabilities all have in common is human error.

Every industry has its own identity access management challenges to consider while building defenses against these malicious attacks, however, compromised user identities are a popular attack vector for ransomware hackers. Identities (and all of the corresponding data) are most often the target of most ransomware attacks, but that doesn't mean they're only targeting people. Ransomware and malware which targets non-human accounts (such as service accounts) have become increasingly common.

Higher education, for example, has the personal data of its students and faculty to safeguard, but there are also research projects, donor initiatives, and so many other data sets to protect. For universities with medical campuses and hospitals, patient data raises the stakes even further.

Healthcare is another area that's been particularly impacted by ransomware, putting sensitive patient data (worth thousands of dollars, compared to $10-20 per record for consumer data) at risk without the proper safeguards in place.

This year, we've also seen the crippling impact ransomware can have in manufacturing and other supply chains (e.g., the Colonial pipeline). Analysts only expect ransomware attacks to increase in the coming years, and to combat these breaches, organizations need to get serious about strengthening their identity and privileged access management (IAM and PAM) solutions as they are essential defenses, and one of few ways of architecting a Zero Trust Architecture.

As part of a Zero Trust security model, a framework that doesn't trust any identity by default (inside or outside of the system), identity access management (IAM) and privileged access management (PAM) will further fortify your cybersecurity posture to minimize vulnerabilities and protect against breaches.

In this guide, we've outlined best practices to get your company on the right path to building a winning cyber defense against ransomware.

1. "2020 Was a Bad Year for Ransomware. 2021 Will Be Worse." Barron, January 2021, John Ford, Anthony Grenga
2. "Verizon 2021 Data Breach Investigations Report," Gabriel Basset, C. David Hylender, Philippe Langlois, Alexandre Pinto, Suzanne Widup

85% of breaches in 2021 involved the human element, with 61% coming from phishing and stolen credentials. It's clear: Even though the call is coming from inside the house, there's still a stranger on the line.[2]

Table of Contents

What is Zero Trust?

Ransomware strikes have surged over the past year from the rise of hard-to-trace cryptocurrencies, a remote-work boom, the ascent of organized criminal groups in the sector, and more. Across the world, network borders are becoming more blurred, and the dispersal of technology will continue to wreak havoc on traditional security models such as VPN, where the perimeter is everything.

Organizations should be deliberate about building proactive strategies to stay a step ahead. Zero Trust empowers your organization with the security and framework you need to combat the new ransomware-as-a-service paradigm. That may be reason enough to mature your operational security with Zero Trust, but there are many other marketplace-driven factors to encourage the change.

1. Government Mandated

The recent ransomware executive order signed by the U.S. President Joe Biden directs the government to put a Zero Trust Architecture in place with components such as encryption and multi-factor authentication. And the decree calls for the modernization of federal networks and improving data sharing between the U.S. government and the private sector.

The mandate also requires any supplier (or any supplier of a supplier) to the Federal Government to meet the qualification. So, if you want to do business as a federal agency or with one, your organization needs to start this Zero Trust journey. Moreover, the government is urging all companies to do the same through similar modernization efforts. The Zero Trust philosophy is growing across the marketplace.

2. Insurance Requirements

Insurance companies are beginning to put security under the microscope. Carriers are asking questions about multi-factor authentication, password management, access to network infrastructure, and more. The answers to these questions are now affecting insurance policies and premiums. By delaying a Zero Trust-based digital transformation, your organization could be facing more than just ransomware dollars.

Zero Trust is a security approach that addresses new network realities by trusting no one.

The basic tenets of Zero Trust are:

- Trust nothing
- Secure everything
- Contextually authenticate requestors
- Contextually evaluate access requests
- Assess all requests
- Grant access by the Principle of Least Privilege (PoLP) or allowing users the minimum access privileges necessary to perform a specific job or task and nothing more

3. Mergers and Acquisitions

In the modern business climate, all companies and organizations face ratings on security readiness from organizations like BitSight and SecurityScorecard. Through continuous monitoring and verified data, these groups deliver actionable security benchmarks and cyber risk metrics. When organizations are involved in a merger and acquisition or a large-scale partnership with funds transfer, those deals are sometimes changed or killed based on the security ratings from these services.

Moreover, acquisitions are complicated. They come with a long list of to-dos: combining teams, technology, services, solutions, etc. With all of these action items to consider, cybersecurity often gets overlooked. However, as ransomware attacks continue to grow in intensity and frequency, your organization can't afford to neglect this essential protection. The cybersecurity combo of identity and access management, and privileged and access management, as part of a Zero Trust strategy, can lay an actionable foundation for process best practices to keep mergers and acquisitions smooth and secure.

4. Erosion of the Perimeter

Networks are evolving into dynamic landscapes where traditional security methods that focus on keeping attackers out of the network are no longer enough. Why? With your organization's growing network of users, devices, and applications, threats are now just as likely to come from within your perimeter. Internal threats account for 1 in 5 or 20% of breaches.[3] And even with external actors, they are most often using valid credentials: Phishing and use of stolen credentials account for 36% and 25% of breaches, respectively.[3]

The reality is that there are no longer any truly closed systems, and a cybersecurity methodology based on one entry point (the perimeter) is outdated. By implementing the tenets of Zero Trust, you can reduce your attack surface. Zero Trust mitigates risk from cyberattacks from multiple entry points across the internal and external.

3. "Verizon 2021 Data Breach Investigations Report," Gabriel Basset, C. David Hylender, Philippe Langlois, Alexandre Pinto, Suzanne Widup

How Zero Trust + IAM + PAM Can Protect You

Operating under the assumption that every user, request, and server remains untrusted until proven otherwise, a Zero Trust Architecture can dynamically and continually assess trust every time a user or device requests access to a resource. And a Zero Trust strategy that includes the dynamic components of identity access management and privileged access management can be foundational for the system, process, and operations design.

By implementing this dynamic cybersecurity strategy, you can reduce your attack surface within the perimeter and prevent ransomware hackers from utilizing valid stolen credentials to walk in and conduct reconnaissance on your confidential applications and data.

But Zero Trust is more than just a mode of cyberdefense; it delivers formidable business value. Beyond enhancing your security status, a Zero Trust strategy, empowered by identity access management and privileged access management, provides the foundational criteria for contemporary system process, design, and operations and creates a winning equation for modernization.

DEFEND YOUR DATA

Your data is valuable, and bad actors look to get their hands on one of your organization's most valuable assets. Once cybercriminals gain inside access, they can exfiltrate this sensitive data. And that can have significant consequences for your customers and organization.

For example:

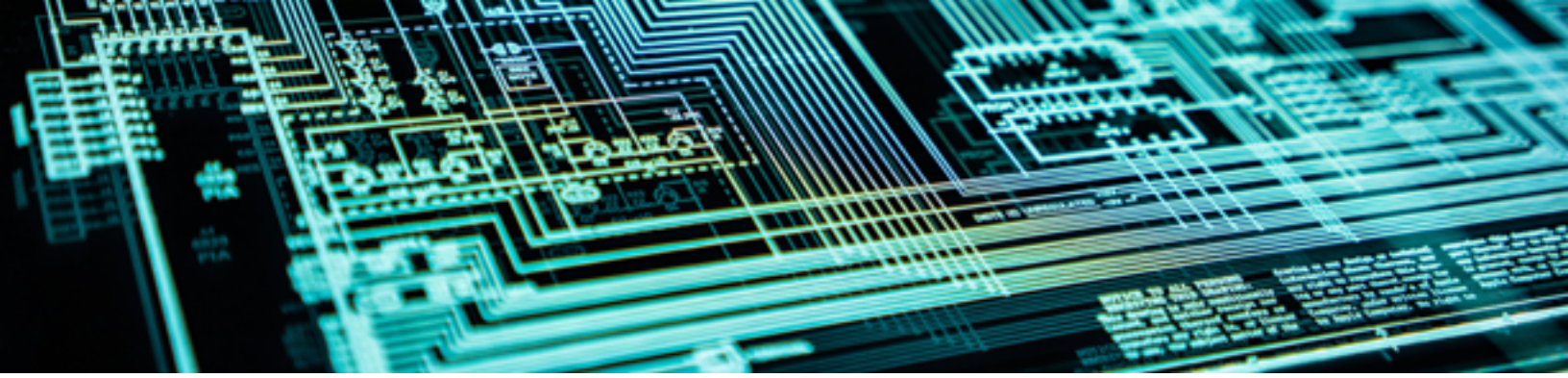
- Hijacked customer data can severely disrupt lives with stolen identities and access to financial accounts.
- Current regulations such as GDPR require your organization to notify users when a data breach occurs. This disclosure can potentially damage your organization's reputation with a loss of customer and stakeholder trust.
- Beyond the upfront lost revenue or ransomware demands, your organization could face costs from higher insurance premiums, incident response needs, security audits, and new cybersecurity measures. These repercussions can far outweigh the initial direct impact.

A Zero Trust Architecture secures your customer's data and safeguard's your business. By reducing the attack surface, you can keep cybercriminals at bay even in this new remote work and access paradigm.

Identity Access Management (IAM) is a framework of processes and policies that ensure that the right identities have the appropriate access to data, technology and network resources. A strong access and identity management solution promotes the principle of least privilege (PoLP). It contains four main components including Authentication, Authorization, and Centralization of Identities and Administration. In addition, top-tier technology will include intelligent automation and enforcement.

A Zero Trust Architecture secures your customer's data and safeguard's your business. By reducing the attack surface, you can keep cybercriminals at bay even in this new remote work and access paradigm.

Privileged Access Management (PAM) consists of cybersecurity strategies and technologies for applying control over the elevated ('privileged") access and permissions for users, accounts, processes, and systems across the IT environment. These systems provide a credential vault, access controls and workflow, and session management.



REDUCE COMPLEXITY

A Zero Trust strategy that includes identity and access management solution allows your organization to transfer mundane operational functions and free up valuable resources for more important endeavors. By reducing complexity your organization is able to remain focused on top priorities as you develop your Zero Trust strategy. And through a highly flexible solution such as Bravura Security Fabric, this process is further streamlined with the capacity to turn capabilities on, off, and scale up or down instantly as needed.

DELIVER EXCELLENT SECURITY AND END-USER EXPERIENCE

Previously, organizations needed to compromise between robust security and a great, constructive user experience, but Zero Trust solutions offer secure access and ease of use. Gone are the days of needing to remember dozens of passwords, replaced with straightforward, user-friendly multi-factor MFA and Federated single sign-on (SSO). Implementations such as these further enhance the user experience and improves productivity, allowing them to log in to every application they need and have access without re-authentication of each sign-on.

Identity access management and privilege access management solutions that leverage MFA deliver a higher level of security by requiring authentication using something known (e.g., login and password) and something owned (e.g., device and security key). Ransomware hackers can often learn or gain access to what a user knows but usually find it challenging to spoof owned devices challenging to spoof the “something owned.

Are Your Prepared for Your Zero Trust Journey?

Before executing your Zero Trust strategy to combat ransomware, you need to plan. Your organization should inventory its business processes and technical infrastructures. This prerequisite inventory will help you build your Zero Trust roadmap.

PREREQUISITE INVENTORY CHECKLIST

Network security audit

- [ ] Approved-use
- [ ] Communications
- [ ] Antivirus / end-point security
- [ ] Password
- [ ] Encryption
- [ ] Remote access policies

Inventory audit

- [ ] Identities
- [ ] Groups
- [ ] Applications
- [ ] Servers
- [ ] Workstations / desktops / laptops
- [ ] Virtual machines / containers
- [ ] Mobile devices
- [ ] Network appliances

For a deeper dive into inventory management including all of the identities you need to manage and resources that you will need to give access, check out our Planning Your Zero Trust Journey worksheet. Inventory now.

Next, after performing a prerequisite inventory and determining the foundation of what's in your network, your organization is ready to assemble its Zero Trust roadmap. This four-stage Zero Trust checklist will help you identify what stage your organization is in on a journey towards a ransomware-ready Zero Trust model.

ZERO TRUST ALIGNMENT CHECKLIST

Fragmented Identity

- [ ] Heavy dependence on the perimeter
- [ ] On-premise Active Directory
- [ ] No cloud integration
- [ ] Passwords wherever

Unified IAM

- [ ] SSO for all users
- [ ] Adaptive, MFA
- [ ] Cooperative policies across apps and servers
- [ ] Vaulting and randomization of privileged accounts

Contextual Access

- [ ] Automated joining, moving, and leaving processes
- [ ] Contextual requests and approvals
- [ ] Group Policy Management
- [ ] Safeguarding services, non-human accounts, and containers

Adaptive Access

- [ ] Risk-based access
- [ ] Systemic feedback / CDM
- [ ] Frictionless access
- [ ] Diminished emphasis on the perimeter
- [ ] Just-in-Time (JIT) access
- [ ] Centralized provisioning

Selling Zero Trust to Decision-makers

No two organizations are the same, but specific Zero Trust projects can play a considerable role in winning over organizational leadership with their smaller investment but outsized ROI.

If you don't have stakeholder buy-in, then you are dead in the water. To win over the mindshare of your IT leadership, focus on authentication first and "start small" with projects like password management, federated SSO, randomizing administrative accounts, and MFA.

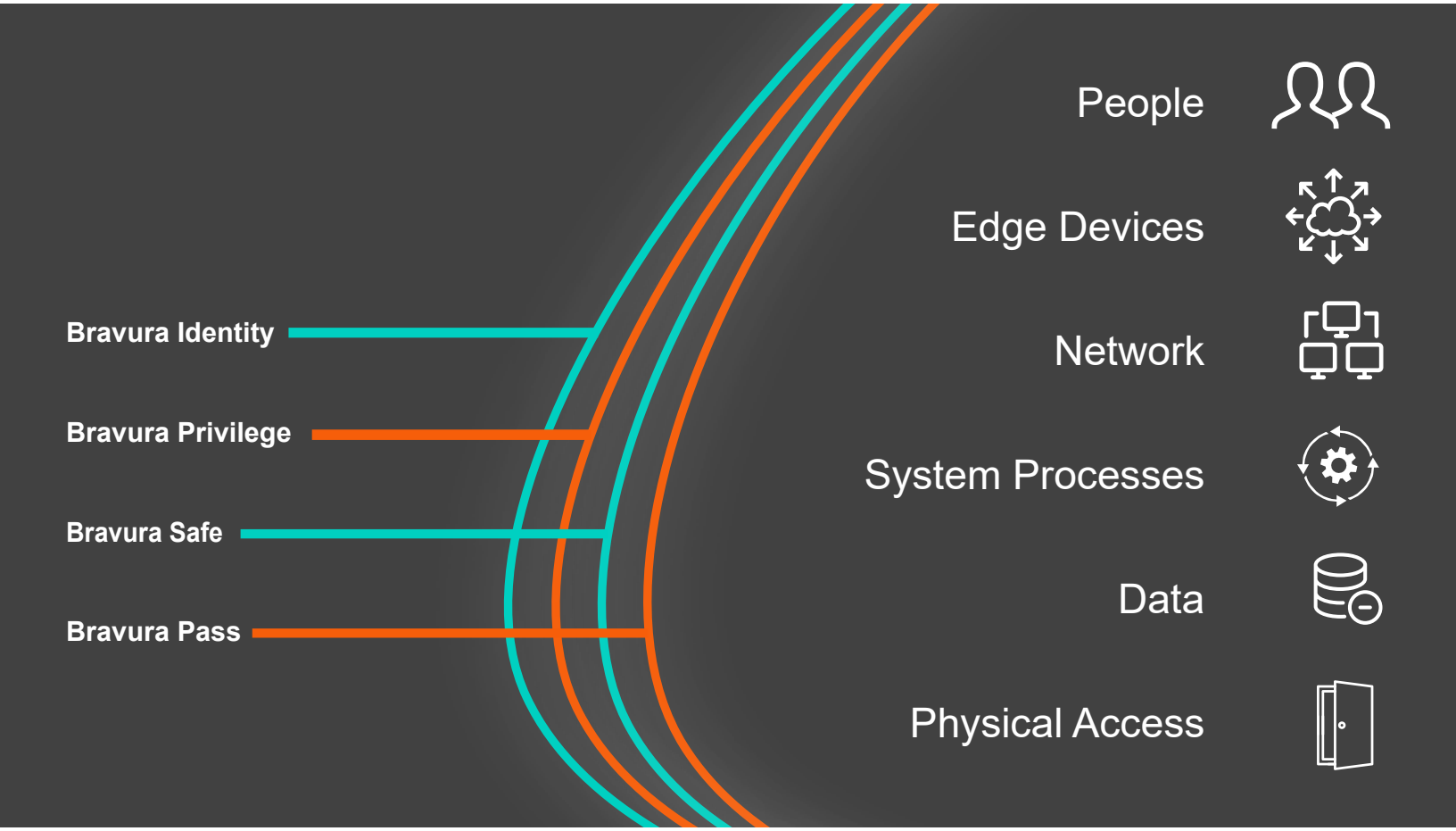
Many leaders need a path that resonates with them before they greenlight a Zero Trust modernization project. So, in a world of remote work, deperimeterization, and the growing threat of ransomware-as-a-service, it's easier for organizational leaders to see the benefits of these implementations early in the process. This work can help you overcome a common roadblock institutions often face in gaining decision-maker support.

Bring in a partner like global enterprise and security consulting firm, intiGrow, to help you build the foundation of your Zero Trust modernization. Assess the shape of your information security with intiGrow's pre-assessment offer. Evaluate Now.

The Ransomware Defense

Supercharge your ransomware resistance, identity access management, and Zero Trust strategy with the industry's only single platform for multi-factor, adaptive authentication, identity and access management, and privileged access management.

Bravura Security Fabric can secure your identities on-prem, in the cloud, and in hybrid IT models, all with the versatility of SaaS. This scalable capability comes with a team of experts to manage your service for you and ensure you have frequent updates and upgrades for cutting-edge protection.



Your organization will be ready to stop ransomware in its tracks with a Zero Trust-powered solution packed with future-ready technologies and architectures.

Next Steps

VISIT our solution webpage. > Visit Now

READ the Zero Trust Guide. > Read Now

We Are Bravura Security

A recognized market leader, we deliver access governance and identity administration solutions to organizations globally, including many Fortune 500 companies. By leveraging decades of experience, we provide the industry's only single platform identity and privileged access solution to simplify implementation as your IAM and PAM roadmaps evolve.

Bravura Security, Inc.

Corporate Headquarters
1401 - 1st Street S.E., Suite 500
Calgary, Alberta, Canada T2G 2J3
bravurasecurity.com

Contact Information
1.403.233.0740
Sales Toll Free: 1.877.386.0372 / 1.877.495.0459
sales@BravuraSecurity.com